Discrete Structures Notes

Hashan Punchihewa

https://hashanp.xyz

Contents

1 Discrete Structures **1**
- 1.1 Sets . . . 1
- 1.2 Functions . . . 3
- 1.3 Peano Arithmetic . . . 5
- 1.4 Computable Functions . . . 6
- 1.5 Countability . . . 7
- 1.6 Orderings . . . 10
- 1.7 Induction . . . 12
- 1.8 Additional Implicative Logic★ . . . 13

Chapter 1

Discrete Structures

1.1 Sets

Definition 1.1.1 ***(Sets)***

A set is a collection of unique objects. Objects in a set are unordered. Sets are denoted by curly brackets e.g. $\{1, 2, 3\}$*. Since elements in a set are unique and unordered, that set is equivalent to* $\{2, 3, 1\}$ *and* $\{2, 2, 1, 3\}$*. To denote that an element* x *belongs to a set* A*,* $x \in A$ *is used. Alternatively* $x \notin A$ *is used to denote that* x *does not belong to* A*. Set builder notation can also be used to denote sets,* $\{x \in A \mid P(x)\}$*, describes a set containing the elements of* A *that satisfy the predicate* P*. The empty set is denoted as* $\varnothing$*.*

Definition 1.1.2 ***(Russell's paradox)***

The reason set builder notation has $x \in A$*, rather than* x*, is because then it would be possible to construct the set* $A = \{X \mid X \text{ is a set } \wedge X \notin X\}$*. Observe that if* $A \in A$*, then* $A \notin A$*, and if* $A \notin A$*, then* $A \in A$*, leading to a contradiction. By adding the* $x \in A$*, restriction this inconsistency can be avoided.*

Definition 1.1.3 ***(Subsets)***

$A \subseteq B$ *means* $\forall a \in A\ (x \in B)$*, i.e. every element of* A *is contained in* B*.* $A = B$*, means* $A \subseteq B$ *and* $B \subseteq A$*. The property of being a subset is transitive i.e. if* $A \subseteq B$ *and* $B \subseteq C$*, then* $A \subseteq C$*.*

Definition 1.1.4 ***(Set operations)***

1. *(Set union)* $A \cup B = \{x \mid x \in A \vee x \in B\}$*.*
2. *(Set intersection)* $A \cap B = \{x \mid x \in A \wedge x \in B\}$*.*
3. *(Set difference)* $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$*.*
4. *(Symmetric set difference)* $A \triangle B = (A \setminus B) \cup (B \setminus A)$*.*
5. *Two sets* A *and* B *are disjoint if* $A \cap B = \varnothing$*.*

Proposition 1.1.1

1. *(Commutativity)* $A \cup B = B \cup A$
2. *(Commutativity)* $A \cap B = B \cap A$
3. *(Commutativity)* $A \triangle B = B \triangle A$
4. *(Associativity)* $A \cup (B \cup C) = (A \cup B) \cup C$
5. *(Associativity)* $A \cap (B \cap C) = (A \cap B) \cap C$
6. *(Idempotence)* $A \cup A = A$
7. *(Idempotence)* $A \cap A = A$
8. *(De Morgan's law)* $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
9. *(De Morgan's law)* $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$
10. *(Absorption)* $A \cap (A \cup B) = A$
11. *(Absorption)* $A \cup (A \cap B) = A$

Definition 1.1.5

- *An n-tuple over sets $A_1 \dots A_n$ is an ordered sequence of elements $a_1, \dots a_n$, such that $a_i \in A_i$.*
- *A 2-tuple is called an (ordered) pair.*
- *The n-ary product of n-sets, denoted as $A_1 \times \dots \times A_n$ is the set of all possible n-tuples over the sets.*

Definition 1.1.6

- *If A is a finite set, then $|A|$ is the number of distinct elements in A.*
- *$\mathcal{P}(A)$ for a set A is the set of all subsets of A.*

Proposition 1.1.2

1. *If A and B are sets, then $A \cup B$ can be written as the union of disjoint sets, $(A \cap B) \cup (A \setminus B) \cup (B \setminus A)$.*
2. *If A and B are disjoint, then $|A \cup B| = |A| + |B|$.*
3. $|A \cup B| = |A| + |B| - |A \cap B|$.
4. *For a finite set A, $|\mathcal{P}(A)| = 2^{|A|}$.*
5. $|A_1 \dots A_n| = |A_1| \dots |A_n|$

Definition 1.1.7 ***(Relation)***

- *A relation R on the sets A and B is a subset of $A \times B$.*
- *If $\langle a, b \rangle \in R$ this can be denoted as aRb.*

- *If $A = B$, i.e. $R \subseteq A^2$, then R is a binary relation.*
- *A binary relation is symmetric if $aRb \implies bRa$.*
- *A binary relation is transitive if $aRb \wedge bRc \implies aRc$.*
- *A binary relation is reflexive if $\forall a \in A\ (aRa)$.*
- *For a relation R on the sets A and B has an inverse relation $R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}$.*
- *For a relation R on the sets A and B has a complement relation $\bar{R} = \{(a, b) \in A \times B \mid (a, b) \notin R\}$.*
- *The identity relation, id_A for a set A is $\{(a, b) \in A^2 \mid a = b\}$.*
- *Composition of relations over $R \in A \times B$ and $S \in B \times C$, $R \circ S$, is defined as $\{(a, c) \in A \times C \mid \exists b \in B\ (aRb \wedge bRc)\}$.*

Proposition 1.1.3

- *R is a reflexive relation on a set A if and only if $\mathrm{id}_A \subseteq R$.*
- *R is symmetric relation on a set A if and only if $R = R^{-1}$.*
- *R is transitive relation on a set A if and only if $R \circ R \subseteq R$.*

Definition 1.1.8

- *If R is a relation $R^{n+1} = R^n \circ R$, and $R^1 = R$.*
- *The transitive closure of R, $R^+ = \bigcup_{i \geq 1} R^i$*

Definition 1.1.9

- *If a binary relation R is symmetric, reflexive and transitive it is an equivalence relation.*
- *An equivalence class of $a \in A$, under R, where R is an equivalence relation on A, denoted as $[a]_R = \{b \in A \mid bRa\}$.*
- *The quotient set of A is the set of equivalences classes under some equivalence relation R: $\{[a]_R \mid a \in A\}$.*
- *A partition of a set of A is a set of non-empty disjoint subsets, whose union is A.*
- *A quotient set of a set A forms a partition of A.*
- *Pigeonhole principle: If n objects are partitioned in k subsets where $0 \leq k \leq n$, then one subset must have at least 2 elements.*

1.2 Functions

Definition 1.2.1

- *A function f is a relation on sets A, B, such that $\forall(a_1, b_1), (a_2, b_2) \in (A \times B)$ $(a_1 = a_2 \implies b_1 = b_2)$, denoted as $f : A \to B$.*
- *A is the domain of the function and B is the co-domain.*
- *$f(a)$ is used to denote the unique b, if there exists such a b, where $(a, b) \in f$.*
- *A function is total if $\forall b \in B \; \exists a \; (a, b) \in f$.*
- *A function that isn't total is partial.*
- *If $X \subseteq A$, then the image set of the function under X, $f[X] = \{b \in B \mid \exists a \in X \; (a, b) \in f\}$*
- *The image of a function is the image set under the domain.*
- *Two functions are considered equal if they contain the same elements, as well as have the same domain and co-domain.*

Proposition 1.2.1

- *If A and B are finite sets, with $|A| = m$ and $|B| = n$, then there are n^m total functions and $(n + 1)^m$ partial functions of the form $A \to B$.*

Definition 1.2.2

- *A function is surjective if the image of a function is the same as its co-domain.*
- *A function is injective if $\forall(a_0, b_0), (a_1, b_1) \in f \; (b_0 = b_1 \implies a_0 = a_1)$.*
- *A function is bijective if it is surjective and injective.*

Proposition 1.2.2

- *If there is a surjection between A and B, then $|A| \geq |B|$.*
- *If there is an injection between A and B, then $|A| \leq |B|$.*
- *If there is a bijection between A and B, then $|A| = |B|$.*
- *(Cantor-Berstein Theorem) If there is an injection from A to B, and from B to A, then there exists a bijection between A and B.*
- *(Dual Cantor-Berstein Theorem) If there is a surjection from A to B, and from B to A, then there exists a bijection between A and B.*

Definition 1.2.3

- *For any set A, there is an identity function $\mathrm{id}_A : A \to A$, such that $\mathrm{id}(x) = x$.*
- *For a bijective function $f : A \to B$, there is an inverse function $f^{-1} : B \to A$, such that $f^{-1} = \{(b, a) \in (B \times A) \mid (a, b) \in f$.*

- *The characteristic function for a set $B \subseteq A$, is defined as follows:*

$$\chi_B(x) = \begin{cases} 1, & x \in B \\ 0, & \textit{otherwise} \end{cases}$$

- *For two functions $f : A \to B$, and $g : B \to C$, there exists $g \circ f : A \to C$, such that $(g \circ f)(x) = g(f(x))$.*

Proposition 1.2.3

- *For a bijective function f, f^{-1} is also bijective, such that $(f^{-1})^{-1} = f$.*
- *Function composition is associative.*

1.3 Peano Arithmetic

Definition 1.3.1

The set of natural numbers, $\mathbb{N}$ are defined as follows:

1. $0 \in \mathbb{N}$
2. $\forall x \in \mathbb{N}, Sx \in \mathbb{N}$
3. $\forall x \in \mathbb{N}, Sx \neq 0$
4. $\forall x, y \in \mathbb{N}, Sx = Sy \implies x = y$
5. *Let V be a set that contains 0 and for all $n \in \mathbb{N}$, such that $n \in V$, then $Sn \in V$, then $\mathbb{N} \subseteq V$.*

The fifth condition, essentially states that $\mathbb{N}$ is the smallest set that satisfies the above properties.

Definition 1.3.2

- *The smaller than by 1 relation, $<_1$ is defined as: $\{\langle n, Sn\rangle, n \in \mathbb{N}\}$.*
- *The smaller than relation, $<$ is defined as the transitive closure over $<_1$.*

Definition 1.3.3

Addition and multiplication are defined as follows:

- $\text{Add}(0, n) = 0$
- $\text{Add}(Sx, n) = \text{Succ}(\text{Add}(x, n))$
- $\text{Mul}(0, n) = 0$
- $\text{Mul}(Sx, n) = \text{Add}(\text{Mul}(x, n), n)$

Definition 1.3.4

- *From our definition of natural numbers, we can define the integers:*

$$\mathbb{Z} = \mathbb{N} \cup \{-n \mid n \in \mathbb{N}\}$$

- *Equality can be defined as follows:*

$$=_{\mathbb{Z}} = \{\langle n, n\rangle \mid n \in \mathbb{N}\} \cup \{\langle -n, -n\rangle \mid n \in \mathbb{N}\} \cup \{\langle 0, -0\rangle, \langle -0, 0\rangle\}$$

Definition 1.3.5

- *The rationals can be defined as follows:*

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{N} \setminus \{0\})$$

- *Equality can be defined as follows:*

$$=_{\mathbb{Q}} = \{\langle\langle a_0, b_0\rangle, \langle a_1, b_1\rangle\rangle \in \mathbb{Q} \mid a_0 b_1 = a_0 b_0\}$$

1.4 Computable Functions

The primitive recursive functions, $\mathcal{F}_{pr}$ are a set of functions of $\mathbb{N}^k \to \mathbb{N}$, where $k \in \mathbb{N}$ and $k \geq 1$, that are made from the following:

- $\text{Zero}(x) = 0$
- $\text{Succ}(x) = x + 1$
- $\text{Proj}^i_n(x_1, \ldots, x_n) = x_i \ (1 \leq i \leq n)$
- $\text{Comp}(h, f_1, \ldots, f_n)(x_1, \ldots, x_k) = h(f_1(x_1, \ldots, x_k), \ldots, f_n(x_1, \ldots, x_k))$
- $\text{Recursion}(f, g)(0, x_1, \ldots, x_k) = f(x_1, \ldots, x_k)$
- $\text{Recursion}(f, g)(Sy, x_1, \ldots, x_k) = g(y, \text{Recursion}(f, g)(y, x_1, \ldots, x_k), x_1, \ldots, x_k)$

Add is built recursively, where $f = \text{Proj}^1_1$ and $g = \text{Succ} \circ \text{Proj}^2_3$. So:

-
$$\text{Add}(0, x) = \text{Recursion}(f, g)(0, x) = f(x) = \text{Proj}^1_1(x) = x$$

-
$$\begin{aligned} \text{Add}(Sy, x) &= g(y, \text{Recursion}(f, g)(y, x), x_1) && (1.1)\\ &= \text{Succ}(\text{Proj}^2_3(y, \text{Add}(y, x), x_1)) && (1.2)\\ &= \text{Succ}(\text{Add}(y, x)) && (1.3)\\ &= \text{Add}(y, x) + 1 && (1.4) \end{aligned}$$

However, primitive recursive functions do not represent all computable functions, namely the Ackermann function is a total function that is not primitive recursive.

Definition 1.4.1

The Ackermann function is defined as follows:

$$\mathrm{Ack}(n,m) = \begin{cases} m+1 & (n=0) \\ \mathrm{Ack}(n-1,1) & (n>0 \wedge m=0) \\ \mathrm{Ack}(n-1,\mathrm{Ack}(n,m-1)) & (n>0 \wedge m>0) \end{cases}$$

To sole this, the definition of a partial recursive function was introduced.

Definition 1.4.2

The set of partial recursive function, $\mathcal{F}_{rec}$ is the set of primitive recursive functions, adding minimisation. I.e. if $f : \mathbb{N}^{n+1} \to \mathbb{N}$, then $h : \mathbb{N}^n \to \mathbb{N}$ is defined as:

$$h(x_1,\ldots,x_n) = \mu y(f(y,x_1,\ldots,x_n)=0)$$

This means it returns the smallest y, for which the expression $f(y,x_1,\ldots,x_n)=0$.

1.5 Countability

Definition 1.5.1 ***(Countability)***

1. *If A and B are two sets $A \approx B$, is there exists a bijection between A and B.*
2. *A set A is countable if it is finite or $A \approx \mathbb{N}$.*
3. *A set is uncountable if it is not countable.*

Proposition 1.5.1

1. *$\approx$ is an equivalence relation.*
2. *$\mathbb{N}$ is countable.*
3. *$\mathbb{Z}$ is countable.*
4. *If two sets A and B are countable, then $A \times B$ is countable.*
5. *$\mathbb{Q}$ is countable.*
6. *$\mathbb{R}$ is uncountable.*
7. *For any set A, $A \not\approx \mathcal{P}(A)$.*
8. *$\mathcal{P}(A)$, where A is a countable infinite set, is uncountable.*
9. *The union of countably many countable set is countable.*

Proof:

1. Not proven here.
2. Consider the function $\mathrm{id}_{\mathbb{N}}$.
3. Consider the function $f : \mathbb{Z} \to \mathbb{N}$:
   - $f(2n) = n$
   - $f(2n+1) = -(n+1)$
4. The cases where either both of or one of A and B are finite are trivial. Consider the case where A and B are both infinite, then the elements of A and B can be numbered $A_0, \ldots$ and $B_0, \ldots$ respectively. Then arrange the items of A and B as such:

$$\begin{array}{lll} (A_0, B_0) & (A_1, B_0) & \ldots \\ (A_0, B_1) & (A_1, B_1) & \ldots \\ \vdots & \vdots & \ddots \end{array}$$

   Then go through the items diagonally. Consider the sum of any item in the grid (A_i, B_j), $i + j$, then notice the sum of all the elements in a diagonal are the same. So first iterate through the diagonal whose sum is 0, then whose sum is 1, etc.

   Alternatively, this is the same as going through the elements column by column in the following arrangement:

$$\begin{array}{llll} (A_0, B_0) & (A_0, B_1) & (A_0, B_2) & \ldots \\ & (A_1, B_0) & (A_1, B_1) & \ldots \\ & & (A_2, B_0) & \ldots \\ & & & \ddots \end{array}$$

5. By the previous proposition, it is known that $\mathbb{N}^2$ is countable. Therefore, there is a surjection from $\mathbb{N}$ to $\mathbb{Q}$. It is also possible to construct a surjection from $\mathbb{Q}$ to $\mathbb{N}$, as follows:

$$f\left(\frac{a}{b}\right) = a \text{ where } \frac{a}{b} \text{ is in its simplest form}$$

   So by the Dual Cantor-Berstein Theorem, there exists a bijection between $\mathbb{N}$ and $\mathbb{Q}$.

6. Suppose $\mathbb{R}$ was countable. This means the numbers of $\mathbb{R}$ can be numbered $\mathbb{R}_0, \ldots$. Let $\mathbb{R}_n^j$ denote the jth digit of $\mathbb{R}_n$ in binary after the radix (technically not a decimal point, since this is binary not decimal). Then construct a binary number $g = 0.g^0g^1g^2g^3\ldots$, where $g_{2n} = 1 - \mathbb{R}_n^{2n}$ and $g_{2n+1} = \mathbb{R}_n^{2n}$. Observe that if g must be the nth number for some $n = k$. Suppose $g_{2k} = 1$, then $1 - \mathbb{R}_k^{2k} = 0$, so $g_{2k} = 0$. This leads to a contradiction. The same applies assuming $g_{2k} = 0$. The problem is certain numbers have two representations for instance 1 can be represented as $1.000\ldots$ or $0.111\ldots$. These dyadic rationals are of the form $n/2^k$. They can either end with an infinite number of 0s (0-tail) or 1s (1-tail). So, could g be an alternative representation of

a number already in our bijection. No, since it does not end with a 0-tail or 1-tail, since it contains pairs of either 01 or 10.

7. Suppose there were such a bijection. Then define the set: $B = \{a \in A \mid a \notin f(a)\}$. There must exist $b \in A$ such that $f(b) = B$. Now if $f(b) = B$, then if $b \in B$, $b \notin B$, i.e. a contradiction. The same applies if $b \notin B$.
8. The result follows the previous proposition.
9. Number these $V_0, \ldots$. Let $\tilde{V} = \bigcup_{i=0}^{\infty} V_i$. Assume that at least one set is infinite, and make this one V_0. (If there is not a single infinite set, then the proof is straightforward). Also since the elements in the sets are countable, number the element $V_i^0, \ldots$. If there are a finite number of sets, or a finite number of elements in a given set, simply 'wrap around'. To do this, I shall use the Dual Cantor-Berstein Theorem and construct surjections from $\mathbb{N}$ to $\tilde{V}$. Then I shall construct one the other way around. To construct a surjection from $\mathbb{N}$ to $\tilde{V}$, called $h_1(x)$ notice that $\mathbb{N}^2$ is countable, so there is a bijection from $\mathbb{N} \to \mathbb{N}^2$, $h_0(x)$. Let our surjection $h_1(x)$, be that if $h_0(x) = (a, b)$, then let $h_1(x) = V_a^b$. Now to construct a surjection from $\tilde{V}$ to $\mathbb{N}$, $h_2(x)$, let V_a, be the smallest a for which $x \in V_a$, the let $h_2(x) = b$ for the smallest b such that $V_a^b = x$. The only problem, is that the first set may not be infinite, prevent a surjection, which is why that requirement was added at the beginning.

Definition 1.5.2 *A set $A \subseteq B$ is a null set in B, if A can be covered by the union of countably many intervals whose total length can be arbitrarily small.*

Proposition 1.5.2 *$\mathbb{Q}$ is a null set in $\mathbb{R}$.*

Proof: Since $\mathbb{Q}$ is countable the elements can be listed $q_0, \ldots$. Then for some $\delta > 0$, an interval can be cast around each rational $(q_i - \delta * 2^{-i}, q_i + \delta * 2^{-i})$. Then A can be covered by:

$$\bigcup_{i=0}^{\infty} (q_i - \delta * 2^{-i}, q_i + \delta * 2^{-i})$$

Observe:

$$\left|\bigcup_{i=0}^{\infty}(q_i - \delta * 2^{-i}, q_i + \delta * 2^{-i})\right| \leq \sum_{i=0}^{\infty}\left|(q_i - \delta * 2^{-i}, q_i + \delta * 2^{-i})\right| \tag{1.5}$$

$$= \sum_{i=0}^{\infty} 2^{-i}\delta + 2^{-i}\delta \tag{1.6}$$

$$= \sum_{i=0}^{\infty} 2^{-i+1}\delta \tag{1.7}$$

$$= \delta\sum_{i=0}^{\infty} 2^{-i+1} \tag{1.8}$$

$$= 2\delta\sum_{i=0}^{\infty} 2^{-i} \tag{1.9}$$

$$= 2\delta\sum_{i=0}^{\infty} \left(\frac{1}{2}\right)^{i} \tag{1.10}$$

$$= 4\delta \qquad \text{Sum to infinity for geometric series} \tag{1.11}$$

1.6 Orderings

Definition 1.6.1 ***(Orders)***

For a binary relation R on a set A.

1. *R is anti-symmetric if aRb and bRa imply $a = b$.*
2. *R is irreflexive if it is not the case that aRa for any a.*
3. *R is a pre-order if it is reflexive and transitive.*
4. *R is a partial order if it is reflexive, transitive and anti-symmetric.*
5. *R is a strict partial order if it is irreflexive and transitive.*
6. *R is a total order if it is a partial order and it is the case that $\forall(a, b) \in A^2\ (aRb \vee bRa)$.*
7. *R is a well-founded partial order if there is no infinite decreasing sequence of elements i.e. for every sequence $a_1 \leq a_2 \leq a_3 \leq \ldots$, there exists some $m \in \mathbb{N}$, such that $\forall n \in \mathbb{N}\ (n \geq m \implies a_n = a_m)$.*

Definition 1.6.2

If A is a set with some partial order R, and $a \in A$, then:

- *a is minimal, if $\forall b \in A\ (bRa \implies b = a)$.*

- *a is least, if* $\forall b \in A\ (aRb)$.
- *a is maximal, if* $\forall b \in A\ (aRb \implies b = a)$.
- *a is greatest, if* $\forall b \in A(bRa)$.

Proposition 1.6.1

1. *If a is the least element, then it is the minimal element.*
2. *If a is the least element, then it is unique.*
3. *If a is the greatest element, this it is the maximal element.*
4. *If a is the greatest element, then it is unique.*
5. *If A is finite with a partial order $\leq$, then there must be a minimal element and a maximal element.*

Definition 1.6.3

- *For a set A with partial order R, if aRb, then a is a predecessor of b, and b is a successor of a.*
- *If aRb, and $\nexists c \in A(aRc \wedge cRb)$, then a is an immediate predecessor of b, and b.*
- *A Hasse diagram shows all the elements of A, and a line drawn between two elements, if one is the immediate predecessor of another, where predecessor is below the successor.*

Definition 1.6.4

If A and B are sets with partial orders $\leq_A$, $\leq_B$, then here are two partial orders on $A \times B$:

- *Product order:* $\langle a_1, b_1\rangle \leq \langle a_2, b_2\rangle$ *if* $(a_1 \leq_A a_2) \wedge (b_1 \leq_B b_2)$
- *Lexiographical order:* $\langle a_1, b_1\rangle \leq \langle a_2, b_2\rangle$ *if* $(a_1 \leq_A a_2) \vee ((a_1 = a_2) \wedge (b_1 \leq_B b_2))$

Proposition 1.6.2

If two sets with partial orders are well-founded, then so is the lexicographical order formed from the two sets.

Proof: Suppose you have $\langle a_1, b_1\rangle \geq \langle a_2, b_2\rangle \geq \ldots$, then you have $a_1 \geq a_2 \geq \ldots$, so eventually you get to a point $m_a \in \ldots$ such that $\forall n \in N\ \ (n \geq m_a \implies a_{m_a} = a_n)$. This means after this point $b_m \geq b_{m+1} \geq \ldots$, and so you get to a point $m_b \in \ldots$ such that $\forall n \in N\ \ (n \geq m_b \implies b_{m_b} = b_n$. Hence the lexicographical ordering is also well-founded.

Proposition 1.6.3 *The Ackermann function terminates:*

Proof: Evaluating the Ackermann function, takes one down a well-founded partial order ($\mathbb{N}^2$). The first case, clearly terminates. The second case, goes down a well-founded partial order since $\langle n, m\rangle > \langle n-1, 1\rangle$. The third case also goes down a well-founded partial order, since $\langle n, m-1\rangle$ goes down a well-founded partial order, and regardless of the value k which $\mathrm{Ack}(n, m-1)$ returns, $\langle n, m\rangle > \langle n-1, k\rangle$.

1.7 Induction

Proposition 1.7.1 *Suppose $P(x)$ is a unary predicate and $P(0)$ and $\forall k \in \mathbb{N}\ (P(k) \to P(Sk))$ holds. Then $\forall n \in \mathbb{N}\ P(n)$.*

Proof: Let $V = \{x \in \mathbb{N} \mid P(x)\}$. Since $P(0)$, $0 \in V$. Also if $k \in V$, then $P(k)$, so $P(Sk)$, so $Sk \in V$, so $(k \in V) \to (Sk \in V)$. Then by Peano's axiom of induction, $\mathbb{N} \subseteq V$, i.e. $\forall n \in \mathbb{N}\ (n \in V)$, so $\forall n \in \mathbb{N}\ P(n)$.

Proposition 1.7.2 *Suppose $P(x)$ is a unary predicate and $P(0)$ and $\forall k \in \mathbb{N}\ (\forall k' \in \mathbb{N}\ (k' \leq k \to P(k'))) \to P(Sk)$.*

Proof: Let $P'(x)$ be a unary predicate, $P'(x) = \forall x' \in \mathbb{N}((x' \leq x) \to P(x'))$. Since $P(0)$, then $P'(0)$ holds. Similarly, if $\forall k \in \mathbb{N}\ (\forall k' \in \mathbb{N}\ (k' \leq k \to P(k'))) \to P(Sk)$, this means $\forall k \in \mathbb{N}\ P'(x) \to P(Sx)$ i.e. $\forall k \in \mathbb{N}\ P'(x) \to P'(Sx)$. Since $P'(0)$ and $\forall k \in \mathbb{N}\ P'(x) \to P'(Sx)$, $\forall n \in \mathbb{N}\ P'(n)$, so $\forall n \in \mathbb{N}\ P(n)$.

Definition 1.7.1 *A set V is structurally defined if given by a base case consisting of a finite number of constants, and an inductive case consisting of a finite number of contexts, which given a finite number of elements in V produce a new element in V.*

Definition 1.7.2 *A set V can be structurally defined with a grammar that might look like this:*

$$\begin{aligned} \langle \textit{expr} \rangle &::= \langle \textit{num} \rangle \quad | \quad \langle \textit{num} \rangle \langle \textit{op} \rangle \langle \textit{num} \rangle \\ \langle \textit{num} \rangle &::= 0 \quad | \quad 1 \\ \langle \textit{op} \rangle &::= + \quad | \quad - \end{aligned}$$

Proposition 1.7.3 *To show a unary predicate $P(x)$ for a set V defined inductively, it is enough to show $P(x)$ holds for all constants, and that assuming $P(x)$ holds for the necessary number of elements, then $P(x)$ holds for elements defined from contexts using those elements, that you've assumed $P(x)$ holds for.*

Formulae in implicative logic, IL are defined through the grammar:

$$\langle I \rangle ::= \top \mid \bot \mid (\langle I \rangle \to \langle I \rangle)$$

Observe the following:

- To write $\neg A$ for some A it is possible to write $A \to \bot$.
- To write $A \vee B$ for some A and B, it is possible to write $\neg A \to B$, since $A \to B$ is equivalent to $\neg A \vee B$. This is since, we have already seen how to write $\neg A$ in implicative logic.
- De Morgan laws can, therefore be used to write $\wedge$ in terms of $\neg$ and $\vee$.
- $\leftrightarrow$ can easily be written using $\to$ and $\wedge$.

- Therefore, all logical formulae can be converted into implicative logic.

Definition 1.7.3

The set of proofs in IL*,* $prf(\mathsf{IL})$ *is defined as follows:*

- $\Gamma \cup \{A\} \in prf(\mathsf{IL})$*, for all* A*.*
- *If* $\Gamma \cup \{A\} \vdash B \in prf(\mathsf{IL})$*, then* $\Gamma \vdash (A \to B) \in prf(\mathsf{IL})$
- *If* $\Gamma \vdash (A \to B), \Gamma \vdash A \in prf(\mathsf{IL})$*, then* $\Gamma \vdash B \in prf(\mathsf{IL})$

This forms the basis for natural deduction in implicative logic which consists of the following rules: axioms, implication introduction and implication elimination.

Axioms are of the form:

$$(\text{Ax})\ \frac{}{\Gamma \cup \{A\} \vdash A}$$

Implication introduction is of the form:

$$(\to\text{I})\ \frac{\Gamma \cup \{A\} \vdash B}{\Gamma \vdash A \to B}$$

Implication elimination is of the form:

$$(\to\text{E})\ \frac{\Gamma \vdash A \to B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

Here is an example of showing $((A \to B) \to (A \to C))$ from $(B \to C)$: In this example, I let $\Gamma = \{(A \to B), A, (B \to C)\}$:

$$\dfrac{\dfrac{\dfrac{(\text{Ax})\ \dfrac{}{\Gamma \vdash (B \to C)} \quad \dfrac{(\text{Ax})\ \dfrac{}{\Gamma \vdash (A \to B)} \quad (\text{Ax})\ \dfrac{}{\Gamma \vdash A}}{\Gamma \vdash B}\ (\to\text{E})}{\Gamma \vdash C}\ (\to\text{E})}{\{(A \to B), (B \to C)\} \vdash (A \to C)}\ (\to\text{I})}{\{(B \to C)\} \vdash ((A \to B) \to (A \to C))}\ (\to\text{I})$$

Proposition 1.7.4 ***(Weakening)***

If $\Gamma \vdash A$ *and* $\Gamma \subseteq \Gamma'$*, then* $\Gamma' \vdash A$*.*

1.8 Additional Implicative Logic★

Definition 1.8.1

- *The size of a formula in* IL *is given by:*

$$\begin{aligned} size(\top) &= 1 \\ size(\bot) &= 1 \\ size(A \to B) &= size(A) + size(B) \end{aligned}$$

- *Intuitively, a cut is where from* $\Gamma \vdash A$ *and* $\Gamma, A \vdash B$*, you conclude* $\Gamma \vdash B$*, rather than proving directly* $\Gamma \vdash B$*. In natural deduction for implicative logic, a cut is an instance of the following in a proof:*

$$\begin{array}{c} (\to I) \\ (\to E) \end{array} \dfrac{\dfrac{\boxed{D_1}}{\Gamma \cup \{A\} \vdash B}}{\Gamma \vdash A \to B} \quad \dfrac{\boxed{D_2}}{\Gamma \vdash A}}{\Gamma \vdash B}$$

- *The size of a cut, is the size of* $A \to B$*.*

Proposition 1.8.1

- *If* $A \to B$ *is the largest cut in a proof, then there exists a proof which introduces cuts at most smaller than the size of* $A \to B$*.*
- *For every proof there exists a cut-free version of the proof.*

Proof:

- This is shown on induction of the structure of proofs on D_1:
  - If D_1 is an axiom of the form $\Gamma \cup \{A\} \vdash A$, then this can be replaced by the derivation $\Gamma \vdash A$, i.e. D_2.
  - If D_1 is an axiom of the form $\Gamma \cup \{A\} \cup \{C\} \vdash C$ (where $C \neq A$), then this can be replaced with $\Gamma \cup \{C\} \vdash C$.
  - If D_1 is an implication introduction of the form:

$$(\to \text{I}) \dfrac{\dfrac{\boxed{D_3}}{\Gamma \cup \{A\} \cup \{C\} \vdash D}}{\Gamma \cup \{A\} \vdash (C \to D)}$$

    Notice, that we can transform this to, where D_3' is the algorithm recursively applied to D_3:

$$(\to \text{I}) \dfrac{\dfrac{\boxed{D_3'}}{\Gamma \cup \{C\} \vdash D}}{\Gamma \vdash (C \to D)}$$

– If D_1 is an implication elimination of the form:

$$(\rightarrow\text{E})\ \frac{\dfrac{\boxed{D_3}}{\Gamma \cup \{A\} \vdash C \rightarrow D} \quad \dfrac{\boxed{D_4}}{\Gamma \cup \{A\} \vdash C}}{\Gamma \cup \{A\} \vdash D}$$

You can recursively, apply the rules to D_3 and D_4 to get:

$$(\rightarrow\text{E})\ \frac{\dfrac{\boxed{D_3'}}{\Gamma \vdash C \rightarrow D} \quad \dfrac{\boxed{D_4'}}{\Gamma \vdash C}}{\Gamma \vdash D}$$

If D_3' ends with implication introduction, this is either because D_3 ends with implication introduction or D_2 ends with implication introduction, and $A = (C \rightarrow D)$. In the latter case, the cut already exists in D_3 so must be smaller than the size of $A \rightarrow B$. In the former case, this means D_2 ends in implication introduction. This is not a problem since $C \rightarrow D$ is smaller than $A \rightarrow B = (C \rightarrow D) \rightarrow B$.

Following these rules for replacing D_1, gives you D_1' and you can replace the cut with:

$$\frac{\boxed{D_1'}}{\Gamma \vdash B}$$

- To get a cut-free version of a proof, apply the above algorithm till there are eventually no cuts. This will eventually terminate. This is as the maximum size of any cut is s, and there are only n cuts with size s. Applying the algorithm to each of the n size s cuts, will not introduce any more cuts of size s or higher. Thus after n applications there are only cuts of at most size $s - 1$. Then reapply this algorithm recursively, and eventually there will be no cuts.