①

Proofs

Statement 1 'The product of two odd integers is odd'

- ↳ What is a statement? => sentence which is either true or false but not both
- ↳ What are the integers?
  - ↳ What are the odd integers
- ↳ What is the product of two integers

· Statement could be written : if m, n are odd integers then so is m · n

Predicate: Statement whose truth depends on the value of one or more variables

Theorem : Very important true statement

Proposition : Less important but nonetheless interesting true statement.

Lemma : True statement used in proving other true statements.

Corollary : True statement that is a simple deduction from a theorem or proposition

Conjecture : Statement believed to be true, but for which we have no proof.

Proof : Logical explanation of why a statement is true; a method for establishing truth.

Logic A study of methods and principle used to distinguish bad reasoning from good.

Definition: An explanation of the mathematical meaning of a word (or phrase).

{generally defined in terms of properties}

Axiom: Basic assumption about a mathematical situation. Axioms can be considered facts that do not need to be proved or they can be used in definitions.

Proposition: $\forall$ integers m and n, if m and n are odd, then so ~~are~~ is $m \cdot n$

Def: A integer is said to be odd if it is of the form $2i+1$ for some integer i.

Let m and n be arbitrary odd integers $\Leftrightarrow m = 2i+1$ for some i

$\Leftrightarrow n = 2j+1$ for some j

where $i, j \in \mathbb{Z}$

RTP: $m \cdot n = 2k+1$ for integer k

$$m \cdot n = (2i+1)(2j+1)$$
$$= 4ij + 2i + 2j + 1$$
$$= 2(2ij + i + j) + 1$$

Since $2ij + i + j$ is an integer, we are done.

A statement is simple (or atomic) when it can be broken into other statements. It is composite when it is built by using several statements (simple or composite) connected by logical expressions

Implication : if... then...

↳ Proof strategy to prove goal of $P \Rightarrow Q$ is to assume P is true and to prove Q logically follows

Contrapositive

Contrapositive of $P \Rightarrow Q$ is not $Q \Rightarrow$ not P

Then same strategy as above.

DEF

<u>Rational</u> : of form $\frac{m}{n}$ for integers m and n

<u>Positive</u> : greater than 0
Negative : less than 0
Nonnegative : greater than equal to 0
Nonpositive : less than or equal to 0

<u>Natural</u>: nonnegative number

LOGICAL DEDUCTION - MODUS PONENS

From statements P and $P \Rightarrow Q$, the statement Q follows.
* ∴ to use an assumption of the form $P \Rightarrow Q$, first work at establishing P.
. Then by Modus Ponens, one can conclude Q and so further assume it.

Theorem

Let P_1, P_2, P_3 be statements. If $P_1 \Rightarrow P_2$ and $P_2 \Rightarrow P_3$ then $P_1 \Rightarrow P_3$

Assume $P_1 \overset{1}{\Rightarrow} P_2$ and $P_2 \overset{2}{\Rightarrow} P_3$
<u>RTP</u>: $P_1 \Rightarrow P_3$:
  <u>Assume</u> : P_1 3
  <u>RTP</u> : P_3
    From (MP) ~~P_1~~ 3 and 1 we have P_2 (4)
    From (MP) 2 and 4 we have P_3
    Therefore, we are done.

<u>IN PRACTISE</u>: $P_1 \Rightarrow P_2 \Rightarrow \dots \Rightarrow P_n$
then we have $P_1 \Rightarrow P_n$

formally
$$\begin{array}{l} P_1 \Rightarrow P_2 \\ P_2 \Rightarrow P_3 \\ \vdots \\ P_{n-1} \Rightarrow P_n \\ \hline P_1 \Rightarrow P_n \end{array}$$

Bi-implication ($\Leftrightarrow$)

$P \Leftrightarrow Q$ is P is equivalent to Q
P if and only if (iff) Q

↳ Proof Pattern for $P \Leftrightarrow Q$
↳ (1) Write $\Rightarrow$ and give proof of $P \Rightarrow Q$
↳ (2) Write $\Leftarrow$ and give proof of $Q \Rightarrow P$

Divisibility and Congruence

DEF Let d and n be integers. We say that d divides n and write $d \mid n$ whenever there exists an integer k s.t. $n = k \cdot d$

N.B. '$\mid$' and 'divides' are not an operation on integers. They are predicates (a property a pair of integers may or may not have between themselves.

{ we can write a, b (as integers) and fixed integer m as $a \equiv b \bmod m$ when $m \mid (a-b)$ }

Universal Quantifications

Universal Statements are of the form 'for all individuals x of the universe of discourse, the property P(x) holds'

$$\forall x \cdot P(x) \quad (\Leftrightarrow \forall y \cdot P(y) \quad - \quad \alpha \text{ equivalence})$$

↳ Proof Strategy
↳ let x stand for a fresh arbitrary individual and prove P(x) for that individual.
GENERIC AND UNCONSTRAINED

Universal Instantiation

To use an assumption of the form $\forall x \cdot P(x)$, you can plug in any value for x to conclude that $P(a)$ is true and so further assume it.

PROPOSITION

Fix a positive integer m. For integers a, b, we have that $a \equiv b \bmod m$ iff $\forall n \in \mathbb{Z}^+$ we have $na \equiv nb \bmod mn$

Let m be a positive integer,
Let a and be be arbitrary integers
RTP: $a \equiv b \bmod m \Leftrightarrow (\forall n \in \mathbb{Z}^+ .\ na \equiv nb \bmod mn)$

$\Rightarrow$ Assume $a \equiv b \bmod m \Leftrightarrow a-b = km$ for integer k

So $na - nb = n(a-b) = nkm$

$na \equiv nb \bmod mn$

$\Leftarrow$ Assume $\forall n \in \mathbb{Z}^+$ $na \equiv nb \bmod m$

RTP: $a \equiv b \bmod m$

By $\boxed{\text{Universal Instantiation}}$, we have $1 \cdot a \equiv 1 \cdot b \bmod (1 \times m)$

that is $a \equiv b \bmod m$

Equality Axioms

① Every individual is equal to itself: $\forall x .\ x = x$

② For any pair of equal individuals, if the property holds to one of them then it holds for the other

$$\forall x .\ \forall y .\ x = y \Rightarrow (P(x) \Rightarrow P(y))$$

$$\left\{ \begin{array}{l} ③\ \forall x .\ \forall y .\ x = y \Rightarrow y = x. \\ ④\ \forall x .\ \forall y .\ \forall z .\ x = y \Rightarrow (y = z \Rightarrow x = z) \end{array} \right\}$$

Conjunction

Conjunctive statements are of the form 'P and Q' or $P \wedge Q$

Proof Pattern

↳① Proove P

↳② Prove Q.

Existential Quantification

Existential statements are statements of the form: 'there exists an individual x in the university of discourse for which the property $P(x)$ holds.

i.e. $\exists x . P(x)$

Proof Strategy ($\exists x . P(x)$)

↳ ① find a witness for the existential statement; that is, a value of x, say w, for which $P(x)$ will be true

↳ ② Show $P(w)$ is true.

Prop For every positive integer k, there exist natural numbers i and j such that $4 \cdot k = i^2 - j^2$

$$\forall \text{ pos int } k \; \exists \text{ nat } i . \exists \text{ nat } j . \; 4k = i^2 - j^2$$

Let k be an arbitrary pos int.

RTP: $\exists \text{nat } i . \exists \text{nat } j . \; 4k = i^2 - j^2$

Consider witness $w = \cancel{2}k+1$

Consider witness $v = \cancel{2}k-1$

We check $4k = w^2 - v^2$

$$= \cancel{2}(k+1)^2 - (k-1)^2$$

$$\cancel{5k} = k^2 + 2k + 1 - (k^2 - 2k + 1)$$

$$= k^2 + 2k + 1 - k^2 + 2k - 1$$

$$= \underline{\underline{4k}}$$

So we are done

To use an assumption of the form $\exists x . P(x)$, introduce a new variable x_0 into the proof to stand for some individual for which the property $P(x)$ holds. This means you can now assume $P(x_0)$ holds

Unique Existence

The notation $\exists! x . P(x)$ stands for 'the unique existence of an x for which the property $P(x)$ holds.

This can be expressed hence:

1. $\exists x . P(x) \wedge (\forall y . \forall z . (P(y) \wedge P(z)) \Rightarrow y = z)$

MOST USED

2. $\exists x . (P(x) \wedge \forall y . P(y) \Rightarrow y = x)$
3. $\exists x . \cancel{P(x)} . \forall y . P(y) \Leftrightarrow y = x$

Dijunctions

Disjunctive statements are of the form 'P or Q' – $P \vee Q$

Proof Strategy $(P \vee Q)$

→ ① Try to prove P (if you succeed, then you are done); or

→ ② Try to prove Q (if you succeed, then you are done); or

→ ③ Break proof into cases; proving in each case, either P or Q.

PROP $\forall n \in \mathbb{Z} . n^2 \equiv 0 \bmod 4 \vee n^2 \equiv 1 \bmod 4$

Break into cases ① n is even

② n is odd.

① Assume n is even $\Leftrightarrow n = 2m$ for int m

$$n^2 = 4m^2 = 4(m^2)$$
$$\equiv 0 \bmod 4$$

② Assume n is odd $\Leftrightarrow n = 2k + 1$ for int k

$$n^2 = 4k^2 + 4k + 1$$
$$= 4(k^2 + k) + 1$$
$$\equiv 1 \bmod 4.$$

Another proof strategy for $P \vee Q$:

→ Assume not P and prove Q or assume not Q and prove P. (this can sometimes be helpful)

(8)

Using a disjunctive assumption

To use a disjunctive hypothesis $\{ (P_1 \vee P_2) \Rightarrow Q \}$ to establish a goal, consider two cases, using P_1 to establish Q and then using P_2 to establish Q.

Binomial Theorem : for all natural numbers n:

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

↳ Corollary: $\forall n \in \mathbb{N}, (z+1)^n = \sum_{i=0}^{n} \binom{n}{i} z^i$

↳ Corollary : $2^n = \sum_{i=0}^{n} \binom{n}{i}$

The Freshman's Dream : $\forall m, n \in \mathbb{N} \, \forall p \in \mathbb{P} \Rightarrow (m+n)^p \equiv m^p + n^p \mod p$

By Binomial Theorem: $(m+n)^p - m^p - n^p = p \cdot \Big(\underbrace{\sum_{i=1}^{p-1} \binom{p-1}{i} m^{p-i} n^{p-i}}_{A} \Big)$

Since A is a natural number this is $\equiv 0 \mod p$, hence we are done.

! Fermat's Little Theorem !

$\forall i \in \mathbb{N}, \forall p \in \mathbb{P} \cdot (i^p \equiv i \mod p) \wedge (i^{p-1} \equiv 1 \pmod p)$ where i ~~p see~~ is not sop
$p \nmid i$

Negation

Statements of the form 'not P' - $\neg P$

Logical Equivalences :

$\neg (P \Rightarrow Q) \Leftrightarrow P \wedge \neg Q$

$\neg (P \Leftrightarrow Q) \Leftrightarrow P \Leftrightarrow \neg Q$

$\neg (\forall x \cdot Px) \Leftrightarrow \exists x \cdot \neg P(x)$

$\neg (P \wedge Q) \Leftrightarrow (\neg P) \vee (\neg Q)$

$\neg (\exists x \cdot P(x)) \Leftrightarrow \forall x \cdot \neg P(x)$

$\neg (P \vee Q) \Leftrightarrow (\neg P) \wedge (\neg Q)$

$\neg(\neg Q) \Leftrightarrow Q$ (in classical logic)

By definition: $\neg Q \Leftrightarrow (Q \Rightarrow \text{false})$

Theorem $(P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)$

For statements P, Q
Assume $P \Rightarrow Q$ (2)
Assume $\neg Q \Leftrightarrow (Q \Rightarrow \text{false})$ (4)
RTP $\neg P \Leftrightarrow (P \Rightarrow \text{false})$
Assume P (1):
By (1) and (2) we have Q (3)
By (3) and (4) we have false and we are done.

Proof By Contradiction

To prove P by contradiction is effectively showing $\neg P \Rightarrow \text{false}$.

⇓ relies upon accepting $\neg(\neg Q) = Q$

Proof Pattern

- Write: "We use proof by contradiction"
- Deduce a logical contradiction
- "This is a contradiction. Therefore, ... must be true"

Theorem $\sqrt{2}$ is irrational

Prove by contradiction, that assume $\sqrt{2} = \frac{p}{q}$ st p and q ~~are~~ share no factors (in most simple form)

$$\sqrt{2} = \frac{p}{q}$$

$$2q^2 = p^2$$

By previous proof if $2 | p^2$, $2 | p$ $\therefore p = 2h$ for int h.

$$2q^2 = 4h^2$$
$$q^2 = 2h^2 \quad \therefore \quad 2 | q$$

$\therefore$ p and q share a factor of 2. Therefore we have a contradiction and $\sqrt{2}$ is irrational.

Numbers

Natural Numbers ($\mathbb{N}$): Number generated from zero by successive increment.
↳ Has basic operations of Addition and Multiplication

Additive Structure: $(\mathbb{N}, 0, +)$
↳ Satisfys Monoid laws: $\underset{\uparrow \text{ identity}}{0+n = n = n+0}$, $\underset{\uparrow \text{ ~~commutativity~~ associativity}}{(l+m)+n = l+(m+n)}$

↳ Commutativity laws: $m+n = n+m$

↳ Is a commutative monoid

Multaplicative Structure satisfys the same conditions $(\mathbb{N}, 1, \cdot)$

Monoid: Algebraic structures with
- elements
- a neutral element
- a binary operation, say m st $m(e,x) = x = m(x,e)$
  $m(m(x,y),z) = m(x,m(y,z))$

· A monoid is commutative if $m(x,y) = m(y,x)$

Additive and Multiplicative structures interact nicely in that it satisfies the Distributive Law
↳ $l\cdot(m+n) = l\cdot m + l\cdot n$

- This makes the overall structure $(\mathbb{N}, 0, +, 1, \cdot)$ into a commutative semiring
  ↳ Semiring is structure consisting of:
  - elements
  - commutative monoid structure 1
  - monoid structure 2
  - Satisfys the distributive law

  (is commutative if 2 is also commutative)

Cancellation : A binary operation satisfies cancellation on the left whenever : $\boxed{x * y = x * z \Rightarrow y = z}$

Inverses : An item x is said to have an inverse y when $x * y = e$ where e is the neutral element.

Prop Inverses, wherever they exist, are unique in a monoid $(e, *)$

Suppose x has inverses y and $z \Leftrightarrow x * y = e,\ y * x = e$
$x * z = e,\ z * x = e$

$\Rightarrow y = y * x * y = y * x * z = e * z = z$
$y = z$ therefore inverse is unique

Extending the system of natural numbers to (i) admit all additive inverses
(ii) admit multiplicative inverses for non zero numbers.

(i) This leads to the integers
↳ $\mathbb{Z}$: $\ldots, -n, \ldots, -1, 0, 1, \ldots, n, \ldots$
↳ This is a commutative ring

(ii) This leads to the rationals ($\mathbb{Q}$)
↳ This is a field

A group is a monoid in which every element has an inverse
A ring is a semiring $((0,+),(1,\cdot))$ where $(0,+)$ is a group. It is commutative if $(1,\cdot)$ is ~~as well~~. a group as well.
A field is a ring where every non-zero element has a multiplicative inverse.

Division Theorem : For every $m \in \mathbb{N}$ and $n \in \mathbb{N}, n > 0$ $\exists! p, q \in \mathbb{Z}$ s.t
$q \geq 0,\ 0 \leq r < n$ and $m = \underset{\text{quotient}}{q}n + \underset{\text{remainder}}{r}$

(12)

Unqueness

Suppose q, r are st. $m = qn + r \quad q \geq 0, \ 0 \leq r < n$

q', r' are st $m = q'n + r' \quad q' \geq 0, \ 0 \leq r' < n$

$$qn + r = q'n + r'$$

Assume $r \geq r'$

$$r - r' = q'n - qn = n(q' - q)$$

$$r - r' < n \Rightarrow q' - q = 0$$

$$q = q' \Rightarrow qn + r = qn + r'$$

By cancellation $r = r'$

$\therefore$ Unique

```
fun divalg(m,n) =
    let fun diviter(q,r) = if r<n then (q,r)
                           else diviter (q+1,r-n)
   in  diviter (0,m)
   end;
```

Theorem: For $m \in \mathbb{N}$, $n \in \mathbb{N}$, $n > 0$, the evaluation of divalg (m,n) terminates outputting pair of natural numbers (q_0, r_0) st $r_0 < n$ and $m = q_0 n + r_0$

~~Lemma~~ The evaluation of divalg (m,n) diverge iff so does the evaluation of diviter $(0,m)$ within this call. This is in turn ~~g~~ the case iff $m - i \cdot n \geq n$ for all natural numbers. Since this latter statement is absurd, the evaluation of divalg (m,n) terminals

For all calls of diviter (q,r) one has $0 \leq q \wedge 0 \leq r \wedge m = qn + r$

because ↳ For first call with $(0,m)$: $0 \leq 0 \wedge 0 \leq m \wedge m = 0 \cdot n + m$

↳ For subsequent calls with $(q+1, r-n)$, these are done when

$$0 \leq q \wedge n \leq r \wedge m = qn + r$$

so that

$$0 \leq q+1 \wedge 0 \leq r - n \wedge m = (q+1)n + (r-n)$$

Therefore since in the last call (q_0, r_0) satisfies $r_0 < n$ we are done.

Modular Arithmetic: For every positive integer m, the integers modulo m are: $\mathbb{Z}_m: 0, 1 \ldots m-1$

$$k +_m l = [k+l]_m = rem(k+l, m)$$
$$k \cdot_m l = [k \cdot l]_m = rem(k \cdot l, m)$$

N.B. $(k +_m l) +_m p = k +_m (l +_m p)$
i.e. $rem(rem(k+l, m)+p, m) = rem(k + rem(l+p, m), m)$

Sets: Set is a well-defined, ordered collection of mathematical objects, called (or members) of the set.
↳ The set membership predicate '$\in$' is central to set and allows us to say $x \in A$ which returns true if x is an element of set A and false, otherwise.

Set Comprehension
↳ Define a set by means of a property that precisely characterise all elements of the set
↳ Notation: $\{x \in A \mid P(x)\}$, $\{x \in A : P(x)\}$

Greatest Common Division
↳ Given a natural number n, the set of its divisors is defined by: $D(n) = \{d \in \mathbb{N} : d \mid n\}$
↳ N.B. set of divisors is hard. GCD is easier.
↳ Common Divisors of pairs
↳ $CD(m,n) = \{d \in \mathbb{N} : d \mid m \wedge d \mid n\}$

Lemma $(m, m' \in \mathbb{N}.\ n \in \mathbb{Z}^+$ st $m \equiv m' \pmod n) \Rightarrow (CD(m,n) = CD(m',n))$

$m \equiv m' \pmod n \Leftrightarrow m - m' = in$ for some int
Let d be arbitrary
$(d \mid m \wedge d \mid n) \Rightarrow (d \mid m' \wedge d \mid n)$

Assume $d | m \wedge d | n$

RTP $d | m' \Leftrightarrow d | m - in$ | RTP $d | n$

True by lemma that if $d | a \wedge d | b \Rightarrow d | pa + qb$ | By assumption

~~Key Lemma~~ Euclid's Algorithm

```
fun gcd (m, n) =
    let val (q, r) = divalg (m, n)
    in
        if r = 0 then n
        else gcd (n, r)
```

Lemma 58

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

Theorem Euclid's Algorithm terminates on all pairs of positive integers and, ~~for such~~ ~~such common division of~~ is the GCD such that:

(i) $gcd(m,n) | m \wedge gcd(m,n) | m$

(ii) $\forall d \in \mathbb{Z}^+$ st $d | m \wedge d | n \Rightarrow d | gcd(m,n)$

By Lemma 58, $CD(m,n) = D(gcd(m,n))$ which is equivalent (1) and (2) and so we are done

Fundamental Properties of gcds.

$\forall l, m, n \in \mathbb{Z}^+$

- Commutativity: $gcd(m,n) = gcd(n,m)$
- Associativity: $gcd(l, gcd(m,n)) = gcd(gcd(l,m), n)$
- Linearity: $gcd(lm, ln) = l \cdot gcd(m,n)$

To show $gcd(m,n) = gcd(n,m)$

- $gcd(m,n)$ contains $gcd(n,m)$, that is:

  (i) $gcd(n,m) | m \wedge gcd(n,m) | n$

  (ii) $\forall d . \; d | m \wedge d | n \Rightarrow d | gcd(n,m)$

4

Since it therefore satisfies the same properties of $gcd(m,n)$, it is clear that $gcd(m,n) = gcd(n,m)$

Theorem $gcd(lm, ln) = l\,gcd(m,n)$
Let l, m, n be pos ints

RTP $gcd(lm, ln) = l\,gcd(m,n)$
↳ case 1: $n | m$
↳ $l \cdot gcd(m,n) = l \cdot n$
$gcd(lm, ln) = ln$ } so we are done

↳ case 2:
↳ $l \cdot gcd(m,n) = l \cdot gcd(n, rem(m,n))$
↳ $gcd(lm, ln) = gcd(ln, rem(lm, ln))$
$= gcd(ln, l \cdot rem(m,n))$

This property is maintained throughout the computation and so the output of $gcd(lm, ln) = l \cdot gcd(m,n)$ $\boxtimes$

Euclid's Theorem → For positive integers k, m and n, if $k | mn$ and $gcd(k,m) = 1$ then $k | n$

Let k, m, n be pos ints.
Assume $\underbrace{k | mn}_{(2)}$ and $\underbrace{gcd(k,m) = 1}_{(1)}$

RTP $k | n$
(1) ⇒ $n \cdot gcd(k,m) = n$
$\quad\quad ||$
$gcd(nk, nm)$
$gcd(nk, ki) = k \cdot gcd(n,i)$

(2) ⇒ $mn = ki$ for integer i

$n = k \cdot gcd(n,i)$
Since $gcd(n,i)$ is an integer, $k | n$ and so we are done

$\boxtimes$

Corollary

For positive integers m and n and prime p, if $p \mid mn$ then $p \mid m$ or $p \mid n$

↳ The second part of Fermat's Little follows from this ($i^{p-1} \equiv 1 \pmod{p}$) where $p \nmid i$

By the first part of Fermat's Little Theorem:

$$i^{p} - i = 0 \bmod p$$
$$\iff p \mid i\,(i^{p-1} - 1)$$

Therefore it follows that $p \mid i^{p-1} - 1$ by Euclid's Theorem $\iff$ $i^{p-1} \equiv 1 \bmod p$ where $p \nmid i$

For prime p, every non-zero element of $\mathbb{Z}_p$ has $[i^{p-2}]_p$ as multiplicative inverse. Hence $\mathbb{Z}_p$ is a field $\iff$ a set in which addition, subtraction, multiplication and division.

Extended Euclid's Algorithm

$\gcd(34, 13) =$	$34 = 2\times 13 + 8$	$8 = 34 - 2\times 13$
$= \gcd(13, 8) =$	$13 = 1\times 8 + 5$	$5 = 13 - 1\times 8$
$= \gcd(8, 5) =$	$8 = 1\times 5 + 3$	$3 = 8 - 1\times 5$
$= \gcd(5, 3) =$	$5 = 1\times 3 + 2$	$2 = 5 - 1\times 3$
$= \gcd(3, 2)$	$3 = 1\times 2 + 1$	$1 = 3 - 1\times 2$
$= \gcd(2, 1)$	$2 = 2\times 1 + 0$	can be rewritten
$= 1$		

~~$2 = 8 - (3 - 1\times 2)\times 3$~~
~~$= 5 - 3\times 3 - 3\times 2$~~

$8 = 34 - 2\times 13$

$5 = 13 - 1\times 8$
$= 13 - 1\,(34 - 2\times 13)$
$= 13 - 34 + 2\times 13$
$= 3\times 13 - 1\times 34$

$3 = 8 - 1\times 5$
$= (34 - 2\times 13) - (3\times 13 - 1\times 34)$
$= 2\times 34 - 5\times 13$

$2 = (3\times 13 - 1\times 34) - (2\times 34 - 5\times 13)$
$= 8\times 13 - 3\times 34$

$1 = (2\times 34 - 5\times 13) - (8\times 13 - 3\times 34)$
$= 5\times 34 - 13\times 13$

(18)

This shows that gcd(m,n) is a linear combination of m and n.

↳ ~~[illegible]~~ An integer i is said to be a linear combination of a pair of integers m and n when:

$\exists s,t \in \mathbb{Z}$ st $(s\ t)\cdot\begin{pmatrix}m\\n\end{pmatrix} = i$

↑ coefficients of the linear combination

$sm + tn = i$

~~Multiplicative inverses in modular arithmetic~~

Theorems ① gcd(m,n) is a linear combination of m and n

② A pair $\underbrace{lc1(m,n) \text{ and } lc2(m,n)}_{\text{coefficients}}$ can be efficiently computed

Propositions (i) $(1\ 0)\begin{pmatrix}m\\n\end{pmatrix} = m \wedge (0\ 1)\begin{pmatrix}m\\n\end{pmatrix} = n$

(ii) $\forall s_1, t_1, r_1$ and s_2, t_2, r_2

$(s_1\ t_1)\begin{pmatrix}m\\n\end{pmatrix} = r_1 \wedge (s_2\ t_2)\begin{pmatrix}m\\n\end{pmatrix} = r_2$

$\Downarrow$

$(s_1+s_2\ \ t_1+t_2)\begin{pmatrix}m\\n\end{pmatrix} = r_1 + r_2$

(iii) $\forall k \in \mathbb{Z}$ and s, t, r

$(s\ t)\begin{pmatrix}m\\n\end{pmatrix} = r \Rightarrow (ks\ kt)\begin{pmatrix}m\\n\end{pmatrix} = kr$

(iv) $\forall$ distinct ints m, n

$lc_1(m,n) = lc_2(n,m)$

Theorem $\forall m,n \in \mathbb{Z}^+$, gcd$(m,n)$ is the least positive linear combination of m and n.

Let m and n be arbitrary positive integers

By previous proof gcd(m,n) is a linear combination of m and n

Furthermore, since it is positive, it is the least such.

Multiplicative Inverses

For all $m, n \in \mathbb{Z}^+$, ① $n \cdot lc_1(m,n) \equiv \gcd(m,n) \bmod m$

② whenever $\gcd(m,n) = 1$

$[lc_2(m,n)]_m$ is the multaplicative inverse of $[n]_m$ in $\mathbb{Z}_m$

Diffie-Helman Cryptographic Method.

A $\qquad\qquad$ c, p $\qquad\qquad$ B

$a \rightsquigarrow [c^a]_p = \alpha \qquad \xleftarrow{\beta} \qquad \xrightarrow{\alpha} \qquad [c^b]_p = \beta \leftarrow\!\!\!\rightsquigarrow b$

$\cancel{\alpha}\beta \downarrow \lambda = [\beta^a]_p \qquad\qquad \alpha \downarrow \lambda = [\alpha^\beta]_p$

Someone intercepting cannot recreate λ

$$[[c^a]_p{}^b]_p = [c^{ab}]_p = [[c^b]_p{}^a]_p$$

Key Exchange

Lemma $p \in \mathbb{P}$ and $e \in \mathbb{Z}^+$ with $\gcd(p-1, e) = 1$

$d = [lc_2(p-1, e)]_{p-1}$

Then, $\forall h \in \mathbb{Z}$

$(h^e)^d \equiv h \bmod p$

Let p be a prime and e a pos int

Assume $\gcd(p-1, e) = 1$

(20)

$$\left\{ \begin{array}{l} \text{Let } l_1 = l_{c_1}(p-1, e) \\ \quad l_2 = l_{c_2}(p-1, e) \end{array} \right\}$$

$p-1 \cdot l_1 + e \cdot l_2 = 1$ for some l_1, l_2

$$\left[\begin{array}{l} \text{If } r = im + jn \\ \quad = (i + ln)m + (j - lm)n \quad (\forall \text{ int } l) \quad (*) \end{array} \right]$$

As $(p-1)l_1 + el_2 = 1$

By $(*)$ it follows that

$(p-1)l_3 + e[l_2]_{p-1} = 1$ for a non-positive int l

So $ed = 1 + (p-1)l'$ for some natural l'

So $(h^e)^d = h^{ed} = h^{1+(p-1)l'}$

$= h(h^{p-1})^{l'}$

By fermat's little

$\equiv h \cdot 1^{l'} \pmod p \equiv h \bmod p.$

A	(P)	B
(e_A, d_A)		(e_B, d_B)
$0 \le h < p$		
$[h^{e_A}]_p = m_1 \longrightarrow$		m_1
m_2		$\longleftarrow m_2 = [m_1^{e_B}]_p$
$[m_2^{d_A}]_p = m_3 \longrightarrow$		m_3
		$m_4 = h = [m_3^{d_B}]_p$

?

21

Principle of Induction (from basis l)

If $P(m)$ is a statement for m ranging over the set of Natural Numbers $\mathbb{N}$.

If: → the statement $P(0)$ holds (BASE CASE) $P(l)$

→ the statement

$\forall n \in \mathbb{N}.\ (P(n) \Rightarrow P(n+1))$ also holds (INDUCTIVE STEP)

$\forall n (\geq l) \in \mathbb{N}$

then $\forall m \in \mathbb{N}.\ P(m)$ also holds

$\forall m (\geq l) \in \mathbb{N},\ P(m)$

Example: Binomial Theorem $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

Proceed by induction

Base case: Show $(x+y)^0 \stackrel{?}{=} \sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k$

$(x+y)^0 = 1$ and $\sum_{k=0}^{0} \binom{0}{k} x^{0-k} y^k = 1$

So we are done.

Note: the $\sum_{k=0}^{n}$ is defined by induction on $n \in \mathbb{N}$

↳ Base case $\sum_{k=0}^{0} f(k) = f(0)$

↳ Inductive Step: $\sum_{k=0}^{n+1} = \left(\sum_{k=0}^{n} f(k)\right) + f(n+1)$

Inductive Step $\forall n \in \mathbb{N}\ \ P(n) \Rightarrow P(n+1)$

Assume $n \in \mathbb{N}$, Assume $P(n)$, that is:

$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$

RTP

$(x+y)^{n+1} \stackrel{?}{=} \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$

Expand left side

$$(x+y)^{n+1} = (x+y) \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$$
$$= \sum_{k=0}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^{k+1}$$

Expand right side $\sum_{k=0}^{n+1} \binom{n+1}{k} x^{(n+1)-k} y^k$

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1} \quad (*)$$

$$\sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k$$

$$= x^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} x^{n+1-k} y^k + y^{n+1}$$

$$= x^{n+1} + y^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1}\right) \cdot x^{n-k+1} \cdot y^k$$
$$= x^{n+1} + y^{n+1} \quad \sum_{k=1}^{n} \binom{n}{k} x^{n-k+1} + \sum_{k=1}^{n} \binom{n}{k-1} x^{n+1-k} y^k$$
$$= \sum_{k=0}^{n} \binom{n}{k} x^{n+1-k} y^k + \sum_{j=0}^{n} x^{j-k} y^{j+1}$$
$$= (x+y) \left(\sum_{k=0}^{n} x^{n-k} y^k \right)$$
$$= (x+y)(x+y)^n$$
$$= \underline{(x+y)^{n+1}}$$

<u>Principle of Strong Induction</u>

P(m) statement for $m \in \mathbb{N}, m \geq l$

If: $\rightarrow P(l)$

$\hookrightarrow \forall n \geq l$ in $\mathbb{N}$ $((\forall k \in [l \dots n] . P(k)) \Rightarrow P(n+1))$ hold

then

$\hookrightarrow \forall m \geq l$ in $\mathbb{N} . P(m)$ holds

<u>Fundamental Theory of Arithmetic</u>

Every positive integer greater than ~~2~~ or equal to 2 is a prime or product of prime

By strong induction

<u>Base Case</u> : True <u>for 2</u>

(2B)

<u>Inductive Step</u>

Let $n \geq 2$ st for all $2 \leq h \leq n$, h prime or product of primes

<u>RTP</u>: $(n+1$ prime$)$ or product of primes

↳ case (1) $n+1$, then we are done
↳ case (2) $n+1$ not prime say $n+1 = pq$

Inductive hypothesis holds for p and q that is they are prime or product of primes
So pq is a product of primes and we are done.

(2) For every $n \in \mathbb{Z}^+$ there is a unique finite ordered sequence of primes $(p_1 \leq \cdots \leq p_l)$ with $l \in \mathbb{N}$ st

$$n = \Pi(p_1 \cdots p_l)$$

Idea is: $1 = \Pi()$

$n \geq 2$ so $n = \Pi(p) = p$ n is prime

or

$n = \Pi(p_1, \ldots, p_l)$ n is a product of prime

<u>RTP</u> $\Pi(p_1, \ldots, p_l) = \Pi(q_1, \ldots, q_k)$
for p_i and q_j primes

Prove by induction on length of the sequence.

$P(l) = \forall p_1, \ldots, p_l$ ordered pairs
$\forall k \in \mathbb{N} \cdot \forall q_1 \cdots q_k$ ordered pairs
$\Pi(p_1 - p_l) = \Pi(q_1 - q_k)$
$\Rightarrow l = k \wedge p_i = q_i$
$\forall i = 1, \ldots, l$

Euclid's Infinitude of Primes

Theorem The set of primes is infinite

Suppose the set of primes is finite, and let $p_1, p_2 \cdots p_n$ be all the primes

Consider $q = (p_1 \times p_2 \cdots p_n) + 1$

Since q is not in the list of primes there is some prime p_i such that $p_i \mid q$

Also $p_i \mid (p_1 p_2 \cdots p_n)$ $\therefore$ So $p_i \mid q - (p_1 p_2 \cdots p_n)$

$\Leftrightarrow p_i \mid 1$ which is a contradiction

And so we are done.

Sets

Abstract Set: A 'bag of dots' (with no set shape)

Extensionality Axiom: Two sets are equal if they have the same elements

↳ $\forall_{\text{sets}}\, A, B \cdot A = B \Leftrightarrow (\forall x \cdot x \in A \Leftrightarrow x \in B)$

Membership Relation: This is the most important structure of a set it describes

↳ $x \in A \Leftrightarrow$ [x is an element in A]

Subsets and Supersets: A is a subset of B, denoted by $A \subseteq B$, whenever:

$\forall x \cdot x \in A \Rightarrow x \in B$

Also B is a superset of A.

Reflexivity: $\forall_{\text{sets}}\, A,\ A \subseteq A$

Transitivity: $\forall_{\text{sets}}\, A, B, C,\ (A \subseteq B \wedge B \subseteq C) \Rightarrow A \subseteq C$

Antisymmetry: $\forall_{\text{sets}}\, A, B\ (A \subseteq B \wedge B \subseteq A) \Leftrightarrow A = B$

↳ expression of the extensionality axiom

Seperation Principle: For any set A and definable property P, there is a set containing precisely those elements of A for which the property holds.

By definition: $a \in \{x \in A \mid P(x)\} \subseteq A \Leftrightarrow (a \in A \wedge P(a))$

Russel's Paradox: The seperation principle does not allow us to consider the class of those R such ~~that~~ that $R \notin R$ as a set

~~Empty Set~~ $R = \{x \mid x \notin x\}$

By def: $\forall x. \; x \in R \iff x \notin x$

By univ instantiation

$$R \in R \iff R \notin R$$

Gives an inconsistency

Universal Set: Set containing all objects and elements

Empty Set: set whose existence is postulated by the seperation principle for a set A and property false

↳ denoted as $\emptyset$ or $\{\}$

↳ $\forall x . x \notin \emptyset$

OR

↳ $\neg(\exists x. \; x \in \emptyset)$

Cardinality: Size of a set. If this is a natural number, the set is 'finite'

↳ $\#S$ or $|S|$

Powerset Axiom

For any set, there is a set consisting of all its subset

↳ $\mathcal{P}(U)$

↳ $\forall X . X \in \mathcal{P}(U) \iff X \subseteq U$

	$\mathcal{P}(U)$	$\#$
$U = \emptyset$	$\{\emptyset\}$	1
$U = \{1\}$	$\{\emptyset, \{1\}\}$	2
$U = \{1,2\}$	$\{\emptyset, \{1\}, \{2\}, \{1,2\}\}$	4

$$\#\mathcal{P}(U) = 2^{\# U}$$

<u>Hasse Diagrams</u> : Links a set of sets connecting items with a difference of a single item in the set.

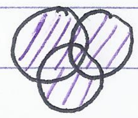
<u>Prop</u> $\forall$ finite sets U $\quad \#\mathcal{P}(U) = 2^{\#U}$

Let U be a set ~~sets~~ with n elements say $u_1, u_2 \ldots u_n$.
We need to count~~ed~~ the subsets of U

Every subset ~~can~~ $S \subseteq U$ can be encoded as a sequence of 0s and 1s of length n with 0 in position i if $u_i \notin S$ and 1 otherwise

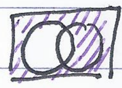
So $\#\mathcal{P}(U) =$ number of possible sequences $= \underline{\underline{2^n}}$

<u>Venn Diagrams</u> ↳ union.



↳ intersection

↳ Complement



<u>Powerset Boolean Algebra</u>

↳ $(\mathcal{P}(U), \emptyset, U, \underbrace{\cup}_{\vee}, \underbrace{\cap}_{\wedge}, \underbrace{(\cdot)^c}_{\neg})$

$\forall A, B \in \mathcal{P}(U)$

↳ $A \cup B = \{x \in U \mid x \in A \vee x \in B\} \in \mathcal{P}(U)$

↳ $A \cap B = \{x \in U \mid x \in A \wedge x \in B\} \in \mathcal{P}(U)$

↳ $A^c = \{x \in U \mid x \notin A\} \in \mathcal{P}(U)$

Union and intersection are associative, commutative and idempotent.

↓

$f(f(x)) = f(x)$

~~The~~ $\emptyset$ is a neutral element for $\cup$ and the universal set $(\mho)$ is a neutral element for $\cap$

{neutrall element = identity element}

In the opposite way $\emptyset$ is the annihalator for $\cap$ and $\mho$ is the annihilator for $\cup$

With regards to each other, $\cup$ and $\cap$ are distributive and absorptive

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$
$$\boxed{A \cup (A \cap B) = A = A \cap (A \cup B) \quad \{(A \cup A) \cap (A \cup B)\}}$$

$\forall x : x \in A \cup (A \cap B) \Rightarrow x \in A$

Let x be arbitrary. Assume $x \in A \cup (A \cap B)$

$\iff (x \in A) \cup (x \in A \cap B)$

<u>RTP</u> $x \in A$

<u>By case</u>: ① $x \in A$ we are done

② If $x \in A \cap B \iff x \in A \wedge x \in B$

so $x \in A$ and we are done

The complementation function $(\cdot)^c$ satisfies complementation laws

$$A \cup (A)^c = \mho$$
$$A \cap A^c = \emptyset$$

Prop

① $\forall X \in \mathcal{P}(U).\ A \cup B \subseteq X \iff (A \subseteq X \land B \subseteq X)$

② $\forall X \in \mathcal{P}(U).\ X \subseteq A \cap B \iff (X \subseteq A \land X \subseteq B)$

① Assume $A \cup B \subseteq X$

$\Rightarrow$ RTP $A \subseteq X$, ~~RTP $B \subseteq X$~~

Know $A \subseteq A \cup B$, $B \subseteq A \cup B$

By assumption

$A \cup B \subseteq X$

By transitivity of $\subseteq$ we are done

$\Leftarrow$ Assume $A \subseteq X \land B \subseteq X$

RTP $A \cup B \subseteq X \iff (\forall x \cdot x \in A \cup B \Rightarrow x \in X)$

Let x be arbitrary assume $x \in A \cup B \iff x \in A \lor x \in B$

RTP: $x \in X$

By cases: ① $x \in A \Rightarrow x \in X$ because $A \subseteq X$ by assumption

② $x \in B \Rightarrow x \in X$ because $B \subseteq X$ by assumption

② Let $X \in \mathcal{P}(U)$

$\Rightarrow$ Assume $X \subseteq A \cap B$. Then since $A \cap B \subseteq A$ and $A \cap B \subseteq B$, by transitivity of $\subseteq$ both that $X \subseteq A$ and $X \subseteq B$

$\Leftarrow$ Assume $X \subseteq A \land X \subseteq B$

RTP $\forall u \in U.\ u \in X \Rightarrow (u \in A \land u \in B)$

Assume $u \in X$

By assumption $u \in A$ and $u \in B$ since $X \subseteq A$ and $X \subseteq B$

Corrolaries : $\mho$ be a set and $A, B, C \in \wp(\mho)$

① $C = A \cup B \iff [A \subseteq C \wedge B \subseteq C] \wedge [\forall X \in \wp(\mho).$
$(A \subseteq X \wedge B \subseteq X) \Rightarrow (C \subseteq X)]$

② $C = A \cap B \iff [C \subseteq A \wedge \cancel{B} C \subseteq B] \wedge$
$[\forall X \in \wp(\mho) . (X \subseteq A \wedge X \subseteq B) \Rightarrow X \subseteq C]$

Sets and Logic

$\wp(\mho) = \{false, true\}$
$\emptyset = false$
$\mho = true$
$\cup = \vee$
$\cap = \wedge$
$(\cdot)^c = \neg$

Pairing Axiom : For every a and b, there is a set with a and b as its only elements.
$\{a, b\}$

↳ defined by : $\forall x . x \in \{a, b\} \iff (x = a \vee x = b)$

Singleton : ~~set to~~ The ~~set~~ set $\{a, a\}$ is abbreviated ~~to~~ as $\{a\}$

Ordered Pairing : For every pair a and b, the set $\{\{a\}, \{a, b\}\}$ is abbreviated as $\langle a, b \rangle$ and referred to as an ordered pair

↳ $\boxed{\langle a, b \rangle = \langle a', b' \rangle \iff (a = a' \wedge b = b')}$

$\Rightarrow$ Assume $\langle a, b \rangle = \langle a', b' \rangle$ that is
$\{\{a\}, \{a, b\}\} = \{\{a'\}, \{a', b'\}\}$

(31)

RTP $a = a' \wedge b = b'$

Case $a = b$ then $\{\{a\}\} = \{\{a'\}, \{a', b'\}\}$

So $\{a\} = \{a'\}$

and $\{a\} = \{a', b'\}$

$a = a \wedge b = a = a' = b'$

Case $a \neq b$

$\{a'\} = \{a\} \vee \{a'\} = \{a, b\}$

case ① $\{a'\} = \{a\}$ $a' = a$

case ② $a' = a = b$ which is a contradiction.

$\therefore$ $a' = a$

Then $(a, b) = (a', b') = (a, b')$

$\therefore$ $b' = b$

And so we are done

Products

Product of two sets $(A \times B)$ is the set:

$$A \times B = \{x \mid \exists a \in A, b \in B \,.\, x = (a, b)\}$$

where $\forall a_1, a_2 \in A,\ b_1, b_2 \in B$

$$(a_1, b_1) = (a_2, b_2) \iff (a_1 = a_2 \wedge b_1 = b_2)$$

$$\therefore\ \forall x \in A \times B\ \exists! a \in A \,.\, \exists! b \in B \,.\, x = (a, b)$$

For a fixed natural number n and sets $A_1, \dots, A_n$, we have:

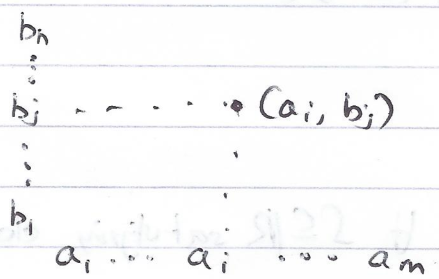
$$\prod_{i=1}^{n} A_i = A_1 \times \dots \times A_n$$
$$= \{x \mid \exists a_1 \in A_1, \dots, a_n \in A_n \,.\, x = (a_1, \dots, a_n)\}$$

where $\forall a_1, a_1' \in A_1, \dots, a_n, a_n' \in A_n$

$$(a_1, \dots, a_n) = (a_1', \dots, a_n') \iff (a_1 = a_1', \dots, a_n = a_n')$$

Proposition $\forall$ finite sets A and B: $\#(A \times B) = \#A\,\#B$.

Suppose $A = \{a_1, \dots, a_m\}$
$B = \{b_1, \dots, b_n\}$



$$A \times B = \{(a_i, b_j) \mid i = 1, \dots, m \ \ j = 1, \dots, n\}$$
$$\#(A \times B) = mn = \#A\,\#B$$

Big Unions

Let U be a set. For a collection of sets $F \in \mathcal{P}(\mathcal{P}(U))$, we let the big union is:

$$\bigcup F = \{x \in U \mid \exists A \in F \,.\, x \in A\} \in \mathcal{P}(U)$$

Hence:

$\bigcup(\emptyset) = \emptyset$

$\bigcup\{A\} = A$

$\bigcup\{A_1, A_2\} = A_1 \cup A_2$

$A\{A_1, A_2, A_3\} = A_1 \cup A_2 \cup A_3$

Big Intersection

$$\bigcap F = \{x \in U \mid \forall A \in F.\ x \in A\}$$

$F = \{\ldots, A, A', \ldots B \ldots\}$
$\bigcap F = \{\ldots \cap A \cap A' \cap \ldots \cap B \cap \ldots\}$

Theorem: Let $F = \{S \subseteq \mathbb{R} \mid (0 \in S) \wedge (\forall x \in \mathbb{R}\ x \in S \Rightarrow (x+1) \in S\}$
Then (i) $\mathbb{N} \in F$, (ii) $\mathbb{N} \subseteq \bigcap F$, (iii) $\bigcap F = \mathbb{N}$

This collects all subsets of $\mathbb{R}$ (?) satisfying the closure property
↳ 0 is in the subsets.
↳ $\forall x \in S \Rightarrow (x+1) \in S$

(i) ~~Proof by induction~~ $0 \in F$ by definition
and given $x \in F$, $(x+1) \in F$
$\Rightarrow \bigcap F \subseteq \mathbb{N}$
$\therefore \mathbb{N} \in F$.

(ii) We show that $\mathbb{N} \subseteq S\ \forall\ S \subseteq \mathbb{R}$ satisfying closure property
↳ Then prove $\forall n \in \mathbb{N}\ n \in S\ \forall S \in F$ by induction on n

Union Axiom: Every collection of sets has a union
↳ $x \in \bigcup F \Leftrightarrow \exists X \in F.\ x \in X$

For nonempty F, $\bigcap F = \{x \in \bigcup F \mid \forall X \in F.\ x \in X\}$
since $\forall x.\ x \in \bigcap F \Leftrightarrow (\forall X \in F.\ x \in X)$

Tagging: Construction $\{l\} \times A = \{(l, a) \mid a \in A\}$
provides copies of A, as tagged by labels l.

Disjoint Unions

$A \uplus B = (\{1\} \times A) \cup (\{2\} \times B)$

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

Proposition $A \cap B = \emptyset \Rightarrow \#(A \cup B) = \#A + \#B$

$A = \{a_1, \dots, a_m\}, \quad B = \{b_1, \dots, b_n\}$

$A \cup B = \{\underbrace{a_1, \dots, a_m}_{\#A = m}, \underbrace{b_1, \dots, b_n}_{\#B = n}\}$

$\#(A \cup B) = \#A + \#B$

Corrolary: $\#(A \uplus B) = \#A + \#B$

Isomorphism : $A \cong B$ or $\#A = \#B$

Equivalence Relations : Relation E on a set A is an equivalence relation when:

① Reflexive
↳ $\forall x \in A \cdot x E x$

② Symmetric
↳ $\forall x, y \in A \cdot x E y \Rightarrow y E x$

③ Transitive
↳ $\forall x, y, z \in A \; (x E y \wedge y E z) \Rightarrow x E z$

↳ The set of all equivalence relations on A is denoted $EqRel(A)$

Partitions : Partition P of a set A is a set of non-empty subsets of A (that is $P \subseteq \mathcal{P}(A)$ and $\emptyset \notin P$), whose elements are referred to as blocks:

① $\bigcup P = A$

② Blocks are pairwise disjoint
↳ $\forall b_1, b_2 \in P, \; b_1 \neq b_2 \Rightarrow b_1 \cap b_2 = \emptyset$

↳ Set of all partitions is $Part(A)$

Examples of Relations

① Empty Relation : $\phi : A \nrightarrow B$ $\quad (a \,\phi\, b \Leftrightarrow \text{false})$

② Full Relation : $(A \times B) : A \nrightarrow B$ $\quad (a\,(A\times B)\,b \Leftrightarrow \text{true})$

③ Identity (or equality) relation

$$id_A = \{(a,a) \mid a \in A\} : A \nrightarrow A \quad (a \; id_A \; a' \Leftrightarrow a = a')$$

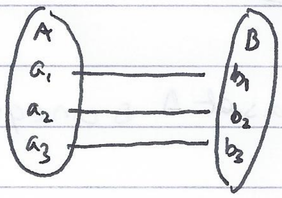
④ Integer square root.

↳ $R_2 = \{(m,n) \mid m = n^2\} : \mathbb{N} \nrightarrow \mathbb{Z} \quad (m R_2 n \Leftrightarrow m = n^2)$

Relation : Relation from A to B is a set consisting of pairs with first component in A and second component in B

$$R : A \nrightarrow B \Rightarrow R \subseteq A \times B \quad (aRb \text{ for } (a,b) \in R)$$

Internal Diagrams



$R = \{(a_1, b_1), (a_2, b_2), (a_3, b_3)\}$

Relational Extensionality

↳ $R = S : A \nrightarrow B$

$\forall a \in A . \forall b \in B . \; aRb \Leftrightarrow aSb$

Relational Composition : Composition of two relations $R : A \nrightarrow B$, $S : B \nrightarrow C$

↳ $S \circ R : A \nrightarrow C$

$a(S \circ R)c \Leftrightarrow \exists b \in B . \; aRb \wedge bSc$

↳ Relational composition is associative and has identity relation as neutral element

↳ Associativity : $\forall R : A \nrightarrow B, \; S : B \nrightarrow C$
$T : C \nrightarrow D$

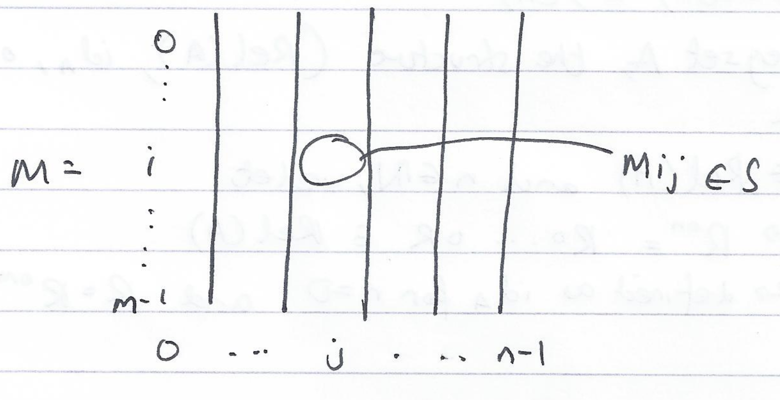
↳ $(T \circ S) \circ R = T \circ (S \circ R)$

↳ Neutral Element : $\forall R : A \nrightarrow B$

↳ $R \circ id_A = R = id_B \circ R$

Relations and Matrices

$\forall m,n \in \mathbb{Z}$ an $(m \times n)$-matrix M over a semiring $(S, 0, \oplus, 1, \odot)$ is given by entries $M_{i,j} \in S$ for $0 \leq i < m$ and $0 \leq j < n$



Identity matrix: $(n \times n)$-matrix I_n:

$$(I_n)_{i,j} = \begin{cases} 1 \text{ if } i = j \\ 0 \text{ if } i \neq j \end{cases}$$

Multiplication of an $(l \times m)$ matrix L with an $(m \times n)$ matrix M is an $(l \times n)$ matrix $M \cdot L$ with

$$(M \cdot L)_{i,j} = (M_{0,j}) \odot (L_{i,0}) \oplus \cdots \oplus (M_{m-1,j} \odot L_{i,m-1})$$
$$= \bigoplus_{k=0}^{m-1} M_{k,j} \odot L_{i,k}$$

↳ Matrix multiplication is associative with identity matrix as neutral element.

Null matrix $Z_{m,n}$ has entries: $(Z_{m,n})_{i,j} = 0$

Addition of two $(m \times n)$ matrices M and L is the $(m \times n)$-matrix $(M+L)$ with entries:

$$(M+L)_{i,j} = M_{i,j} \oplus L_{i,j}$$

Relation R ~~from~~ $[m] \nrightarrow [n]$ can be seen as $(m \times n)$ matrix $mat(R)$ over commutative semirings of Booleans:

$(\{false, true\}, false, true, \vee, \wedge)$

$(mat(R))_{i,j} = [(i,j) \in R]$

$(i,j) \in rel(M) \iff M_{i,j}$

Directed Graphs

↳ Directed Graph (A,R) consists of a set A and a relation R on A (a relation from A to A)

↳ $Rel(A) \subseteq \mathcal{P}(A)$

↳ For every set A, the structure $(Rel(A), id_A, \circ)$ is a monoid

↳ For $R \in Rel(A)$ and $n \in \mathbb{N}$, we let:

↳ $R^{\circ n} = R \circ \ldots \circ R \in Rel(A)$

↳ defined as id_A for $n=0$ and $R \circ R^{\circ m}$ for $n=m+1$.

Paths

↳ Let (A,R) be a directed graph. For $s, t \in A$, a path of length $n \in \mathbb{N}$ in R with source s and target t, is a tuple $(a_0, \ldots, a_n) \in A^{n+1}$

↳ $s R^{\circ n} t$ iff there exists a path of length n in R with source s and target t.

↳ Can be proved by induction

↳ ~~Let~~ $R \in Rel(A)$

$R^{\circ *} = \bigcup \{R^{\circ n} \in Rel(A) \mid n \in \mathbb{N}\} = \bigcup_{n \in \mathbb{N}} R^{\circ n}$

$s R^{\circ *} t$ iff there exists a path with source s and target t in R.

↳ $(n \times n)$-matrix $M = mat(R)$ of a finite directed graph $([n], R)$ for n as a positive integer is called its adjacency matrix

↳ $M^* = mat(R^{\circ *})$

$$\begin{cases} M_0 = I_n \\ M_{k+1} = I_n + (M \cdot M_k) \end{cases}$$

↳ Gives an algorithm for finding if there is path in finite directed graphs

<u>Preordes</u> : $(P, \sqsubseteq)$ consists of a set P and a relation $\sqsubseteq$ on P satisfying two axioms:

↳ Reflexivity

↳ $\forall x \in P \cdot x \sqsubseteq x$

↳ Transitivity

↳ $\forall x, y, z \in P \cdot (x \sqsubseteq y \wedge y \sqsubseteq z) \Rightarrow x \sqsubseteq z$

<u>Example</u> : • $(\mathbb{R}, \leq)$, $(\mathbb{R}, \geq)$

• $(\mathcal{P}(A), \subseteq)$, $(\mathcal{P}(A), \supseteq)$

• $(\mathbb{Z}, |)$ {preorder that is not a partial order}

↳ For $R \subseteq A \times A$

$$\mathcal{F}_R = \{Q \subseteq A \times A \mid \overbrace{R \subseteq Q \wedge Q \text{ is a preorder}}^{\text{closure property}}\}$$

Then (i) $R^{\circ *} \in \mathcal{F}_R$ and (ii) $R^{\circ *} \subseteq \bigcap \mathcal{F}_R$

$\Rightarrow R^{\circ *} = \bigcap \mathcal{F}_R$

↳ $\mathcal{F}_R$ is the family of all the preordes on A that contain R.

(i) $R^{\circ *} \in \mathcal{F}_R$

↳ $R \subseteq R^{\circ *} = \bigcup_{n \in \mathbb{N}} R^{\circ n}$

↳ $R^{\circ *}$ is a preorder

↳ $x R^{\circ *} x \quad \forall x$

↳ $x R^{\circ *} y \wedge y R^{\circ *} z \Rightarrow x R^{\circ *} z$

↳ uses the characteristic of $R^{\circ *}$ as describing paths in R

<u>Partial Functions</u> : Relation $R: A \nrightarrow B$ is functional and a partial when it is:

↳ $\forall a \in A \, \forall b_1, b_2 \in B \, . \, a R b_1 \wedge a R b_2 \Rightarrow b_1 = b_2$

↳ One thing in domain maps to one item in range

↳ If $f \subseteq A \times B$ is a partial function, $a \in A$:

$f(a)\downarrow$ if $\exists b \in B \cdot a f b$ (There is an output for a)

$f(a)\uparrow$ if $\forall b \in B \;\; \neg(a f b)$ (no output)

↳ The identity relation is a partial function and composition of partial functions is a partial function

$$f = g : A \overset{\text{notation for partial function}}{\rightharpoonup} B$$
$$\iff \forall a \in A \cdot (f(a)\downarrow \iff g(a)\downarrow) \wedge f(a) = g(a)$$

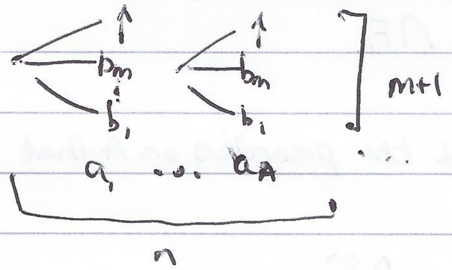
↳ The number of relations between finite sets.

$$\#A = n \qquad \#B = m$$
$$\#Rel(A,B) = \#\mathcal{P}(A \times B)$$
$$= 2^{\#(A \times B)}$$
$$= \underline{2^{\#A\#B}}$$

Proposition: For all finite sets A and B: $\#(A \rightharpoonup B) = (\#B + 1)^{\#A}$

$$A = \{a_1, \dots, a_n\}$$
$$B = \{b_1, \dots, b_m\}$$

$A \rightharpoonup B \iff \{f \in Rel(A,B) \mid f \text{ is a partial function}\}$



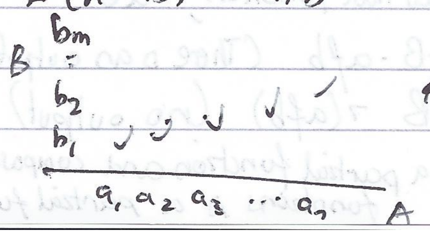
$$\therefore \#(A \rightharpoonup B) = (m+1)^n = (\#B+1)^{\#A}$$

<u>Total Function</u>: Partial function is total and is referred to as a total function when its domain of definition coincides with its source

$$\forall f \in Rel(A,B)$$
$$f \in \underbrace{(A \Rightarrow B)}_{A \Rightarrow B \text{ is the set of all functions from } A \text{ to } B.} \iff \forall a \in A \ \exists! b \in B . afb$$

$$\therefore (A \Rightarrow B) \subseteq (A \rightharpoonup B) \subseteq Rel(A,B)$$

Propositions: $\#(A \Rightarrow B) = \#B^{\#A}$



each a has m choices for output

$$\therefore m \times m \times m \dots$$
$$m^n = \#B^{\#A}$$

↳ The identity partial function is a function and the composition of functions gives a function

<u>Bijection</u>: A function $f: A \to B$ is a bijection whenever it has a (two sided) inverse, i.e there exists a $g: B \to A$ s.t.

$$g \circ f = id_A \quad \wedge \quad f \circ g = id_B$$

↳ Inverses, if they exist, are unique.

↳ $f \circ g = id_B \iff \forall b \in B \;\; f \cdot g(b) = b$

↳ $g \circ f = id_A \iff \forall a \in A \;\; g(f(a)) = a$

↳ Retraction for f is left inverse

↳ $g \cdot f = id_A$

↳ Section is right

↳ $f \circ g = id_B$

↳ $\# Bij(A,B) = \begin{cases} 0 \text{ if } \#A \neq \# B \\ n! \text{ if } \#A = \#B = n \end{cases}$

$A = \{a_1, \dots, a_m\}, B = \{b_1, \dots, b_n\}$

if $n < m$, there can be no bijection since no possible inverse

Bijection precisely when:

$$\begin{array}{cccc} a_1, & a_2 & \dots & a_m \\ \downarrow & \downarrow & \downarrow & \downarrow \\ b_{i_1}, & b_{i_2}, & b_{i_3} & \dots b_{i_n} \end{array}$$

These are a permutation of the combinations, therefore $m! = n!$ of these.

↳ The identity function is a bijection and the composition of bijection gives a bijection

$$Bij(A,B) \subseteq (A \Rightarrow B) \subseteq (A \rightharpoonup B) \subseteq Rel(A,B)$$

Theorem For every set A: $EqRel(A) \cong Part(A)$.

① Define a mapping that to every equivalence relation $E \subseteq A \times A$ associates with a partition $\Pi(E)$ of A.

$E \longmapsto A/E = \{b \subseteq A \mid \exists a \in A .\ b = [a]_E\}$

$[a]_E = \{x \in A \mid x E a\}$

(Quotient of a under E)

must prove E is an equivalence relation, A/E is a partition

② Prove the mapping gives function $EqRel(A) \to Part(A)$

③ Prove mapping $P \mapsto \equiv_P$ where $x \equiv_P y \Leftrightarrow \exists b \in P . x \in b \land y \in b$

gives $Part(A) \to EqRel(A)$

④ Prove functions are inverses of one another (See proof in notes)

Calculus of Bijections

↳ $A \cong A$, $A \cong B \Rightarrow B \cong A$

↳ $(A \cong B \land B \cong C) \Rightarrow A \cong C$

↳ If $A \cong X \land B \cong Y$

↳ $\mathcal{P}(A) \cong \mathcal{P}(X)$, $A \times B \cong Y \times X$, $A \uplus B \cong X \uplus Y$

$Rel(A, B) \cong Rel(X, Y)$, $(A \rightharpoonup B) \cong (X \rightharpoonup Y)$

$(A \Rightarrow B) \cong (X \Rightarrow Y)$, $Bij(X, Y)$

Characteristic (indicator) functions

$\mathcal{P}(A) \cong (A \Rightarrow [2])$

$\chi : \mathcal{P}(A) \to (A \Rightarrow [2])$

$\chi_S(a) = \begin{cases} 1 & a \in S \\ 0 & a \notin S \end{cases} \quad \forall a \in A \ (S \subseteq A)$

$\varphi : (A \Rightarrow [2]) \to \mathcal{P}(A)$

$\varphi(f) = \{x \in A \mid f(x) = 1\}$

Finite Cardinality : Set is finite if $A \cong [n]$ for some $n \in \mathbb{N}$ when we can say $\#A = n$.

<u>Infinity Axiom</u>: There is an infinite set, containing $\emptyset$ and closed under successor

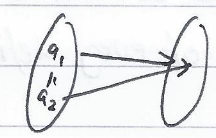
<u>Surjection and Injection</u>: For a function $f: A \to B$, the following are equivalent

① f is bijective

② $(\forall b \in B. \exists a \in A \; f(a) = b) \land$
(SURJECTIVE)
$(\forall a_1, a_2 \in A. \; f(a_1) = f(a_2) \Rightarrow a_1 = a_2)$
(INJECTIVE)

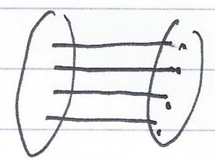
③ $\forall b \in B. \exists! a \in A. \; f(a) = b$

<u>Injection</u>:
$f: a \rightarrowtail B$



: $\forall a_1, a_2 \in A \; f(a_1) = f(a_2) \Rightarrow a_1 = a_2$

<u>Surjection</u>: $\forall b \in B \; \exists! a \in A \; f(a) = b$
$f: a \twoheadrightarrow b$



<u>Enumerability</u>

↳ Enumerable set A when there exists a surjection $\mathbb{N} \twoheadrightarrow A$ (enumeration)

↳ Countable set is either empty or enumerable

<u>Countability</u>

↳ $\mathbb{N}$, $\mathbb{Z}$ and $\mathbb{Q}$ are countable sets (1)

↳ Product and disjoint union of countable sets is countable (2)

↳ Every finite set is countable

↳ Every subset of a countable set is countable

<u>Fixed-Point of function</u>: $f: X \to X$ is an element $x \in X$ st $f(x) = x$

Theorem

Lawvere's Fixed Point Argument: For sets A and X, if $A \twoheadrightarrow (A \Rightarrow X)$ then every function $X \to X$ has a fixed-point and therefore X is a singleton

$E: A \twoheadrightarrow (A \Rightarrow X)$

$f: X \to X$

Define $A \xrightarrow[\varphi]{} X \quad : \quad a \to f(Eaa)$

There is $\alpha \in A$ s.t. $E(\alpha) = f \Rightarrow E(\alpha)(\alpha) = f(\alpha)$

$\therefore E\alpha\alpha$ is a fixed point of f

Axiom of Choice: Every surjection has a section

Replacement Axiom: The direct image of every definable functional property on a set, is a set

~~Set~~

~~Set theke~~

Formal Languages and Automata

Alphabets: Specified by giving a finite set Σ, whose elements are called symols - effectively any finite set.

String: String of length n over an alphabet Σ is an ordered n-tuple of elements of Σ, written without punctuation.
↳ Σ^* denotes set of all strings over Σ of any finite length.
↳ If $\Sigma = \phi$, then $\Sigma^* = \{\varepsilon\}$ - empty string

Concatenation of strings: Concatenation of two strings u and v is uv, obtained by joining the strings end-to-end. This generalises to concatenation of three or more strings.

Formal Language: An subset of Σ^*, given an alphabet Σ

Inductive Definition
↳ Axioms: $\overline{a}$ means a is in the subset we are defining
↳ Rules: $\dfrac{h_1, h_2 \dots h_n}{c}$ means if $h_1, h_2 \dots h_n$ are in the subset, so is c.

Derivations: Given a set of axioms and rules for inductively defining a subset of a given set U, a derivation that a particular element $u \in U$ is in the subset is by definition:
↳ Finite rooted tree with vertexes as elements of U:
↳ Root is u
↳ Each vertex is a conclusion of rule whose hypothesis is a child
↳ Leaves are axioms

Inductively defined subsets: Given axioms and rules subset consists all elements for which there is a derivation with conclusion that element.

Reflexive - Transitive Closure

↳ Given a binary relation $R \subseteq X \times X$ on a set X, its reflexive - transitive closure R^* is the smallest binary relation on X which contains R which is reflexive and transitive $(\forall x. \in x, (x,x) \in R^*)$

$\therefore$

$$\frac{}{(x,y)} \text{ for } (x,y) \in R \qquad \frac{}{(x,x)} \; \forall x \in X$$

$$\frac{(x,y) \quad (y,z)}{(x,z)} \; \forall x,y,z \in X$$

Rule Induction

↳ Subset $I \subseteq U$ is inductively defined by a collection of axioms and rules. I is closed under them and is the least such subset iff:

↳ if $S \subseteq U$ is also $\underbrace{\text{closed under axioms and rules}}$ then $I \subseteq S$

↳ ① For every axiom $\frac{}{a}$ $a \in S$

↳ ② For every rule $\frac{h_1 h_2 \ldots h_n}{c}$ if $h_1, h_2, \ldots h_n \in S \Rightarrow c \in S$

$\bigcap (\forall S \subseteq U \text{ (} S \text{ closed under } R\text{)})$ is closed under R

set of axioms and rules

Theorem: The subset $I \subseteq U$ inductively defined is closed under axioms and rules and is least such subset: if $S \subseteq U$ is also closed under the axioms and rules $I \subseteq S$

Closure

↳ ① I is closed under each axiom $\frac{}{a}$ since we can construct a derivation witnessing $a \in I$ - simply a tree with one node containing a.

↳ ② I is closed under each rule $r = \frac{h_1 h_2 \ldots h_n}{c}$ because if $h_1 h_2 \ldots h_n \in I$ we have n derivations from axioms to each h_i and so we make these the n children to our rule r to form a big tree. This a derivation witnessing $c \in I$

Proof: must show: (S closed under axioms and rules) $\Rightarrow I \subseteq S$

That is the least subset, in that any other subset that is closed under the axioms and rules contains I

Let $P(n) \triangleq$ all derivations of height n, having their conclusion in S. Therefore, need to show: ① $P(0)$

② $\forall (h \leq n) P(h) \Rightarrow P(n+1)$

① Trivially true since conclusion is an axiom - S is closed under axioms

② Assume $\forall (h \leq n) P(h)$ and that say D is a derivation of height $n+1$ with conclusion s. But derivations for c_i all have heights $\leq n$

So in S by assumption $\Rightarrow c \in S$

$\therefore \forall (h \leq n) P(h) \Rightarrow P(n+1)$

$\therefore$ ~~For~~ Every element in I is in S ~~[illegible]~~. Therefore I is the least subset closed under specified axioms and rules

Rule Induction: Given a property $P(u)$ of elements of U, to prove $\forall u \in I \; P(u)$ we show:

↳ $P(a)$ holds for every axiom $\overline{a}$

↳ Induction steps: $P(h_1) \,\&\, P(h_2) \,\&\, \ldots \,\&\, P(h_n) \Rightarrow P(c)$ holds for every rule $\dfrac{h_1 \, h_2 \ldots h_n}{c}$

Collatz Conjecture: Can consider the following problem: $f(n) = \begin{cases} 1 & \text{if } n = 0, 1 \\ f(n/2) & \text{if } n > 1, n \text{ even} \\ f(3n+1) & \text{if } n > 1, n \text{ odd} \end{cases}$

using $\dfrac{}{0}$, $\dfrac{}{1}$, $\dfrac{k}{2k}$, $\dfrac{3(2k+1)+1}{2k+1}$ $\quad k \geq 1$

and see if this is equal to the whole of $\mathbb{N}$, in order to see if $f(n)$ is a total function $f: \mathbb{N} \to \mathbb{N}$

Regular Expressions

Concrete Syntax: → strings of symbols (these can be commands - eg 'let')

↳ Can include symbols to disambiguate the semantics (whitespace)

Abstract Syntax: Finite rooted tree

↳ Verticies with n children are labelled by operators expecting n arguments (n-ary operators) - leaves are labelled with nullary operators

↳ Label of root gives outermost form of the whole phrase

↳ A regular expression defines a pattern of symbols (therefore a language)

↳ Concrete Syntax over a given alphabet Σ. Define $\Sigma^{\#} = \{\epsilon, \phi, |, *, (,)\}$

$U = \{\Sigma \cup \Sigma^{\#}\}^*$

axioms: $\overline{a}$, $\overline{\epsilon}$, $\overline{\phi}$

rules: $\dfrac{r}{(r)}$ $\dfrac{r \quad s}{r|s}$ $\dfrac{r \quad s}{rs}$ $\dfrac{r}{r*}$

(where $a \in \Sigma$ and $r, s \in U$)

↳ Abstract Syntax

↳ Signature over alphabet Σ consists of:

↳ ① Binary operators – Union, Concat

↳ ② Unary operator – $*$

↳ ③ Nullary operators – Null, Empty, Sym_a ($\forall a \in \Sigma$)

↳ Relating Concrete and abstract syntax ($\sim$ is an inductively defined relation)

many-many relation

↳ $\overline{a \sim Sym_a}$, $\overline{\epsilon \sim Null}$, $\overline{\phi \sim Empty}$

↳ $\dfrac{r \sim R}{(r) \sim R}$, $\dfrac{r \sim R \quad s \sim S}{r|s \sim Union(R,S)}$

↳ $\dfrac{r \sim R \quad s \sim S}{rs \sim Concat(R,S)}$, $\dfrac{r \sim R}{r* \sim Star(R)}$

↳ <u>Parsing</u>: Producing abstract syntax trees from concrete syntax

↳ Pretty Printing: Producing concrete syntax from abstract syntax trees

↳ Operator Precedence : Star > Concat > Union

↳ Associativity

↳ Concat and Union are left associative

↳ $abc = (ab)c$

↳ $a|b|c = (a|b)|c$

Matching : Each regular expression r over an alphabet Σ determines a language $L(r) \subseteq \Sigma^*$. The strings u in $L(r)$ are those that match r, where:

↳ ① u matches the regular expression a (where $a \in \Sigma$) iff $u = a$

↳ ② u matches the regular expression ε iff u is null string

↳ ③ No string matches $\emptyset$

↳ ④ u matches $r|s$ iff it matches r or s

↳ ⑤ u matches rs iff it can be expressed as vw with v matching r and w matching s.

↳ ⑥ u matches r^* iff either $u = \varepsilon$ or u matches r, or u can be expressed as concatenation of two or more strings, each of which matches r.

↳ Inductive definition of matching: $U = \Sigma^* \times \{\text{regular expressions over } \Sigma\}$

$$\frac{}{(a,a)} \qquad \frac{}{(\varepsilon,\varepsilon)} \qquad \frac{}{(\varepsilon, r^*)}$$

$$\frac{(u,r)}{(u,r|s)} \qquad \frac{(u,s)}{(u,r|s)} \qquad \frac{(v,r)\ (w,s)}{(vw, rs)} \qquad \frac{(u,r)\ (v,r^*)}{(uv, r^*)}$$

Finite Automaton → ① Set of states $\{q_0, q_1, \dots q_n\}$

↳ ② Input alphabet $\{a, b\}$

↳ ③ Transitions

↳ ④ Start state

↳ ⑤ Accepting state(s)

↳ Language accepted by a finite automaton

↳ Set of strings represented by path from start state to accepting state $= L(M)$

↳ $q \xrightarrow{u}{}^* q'$ means there is an automaton where there is a path between q and q' whose labels form u

<u>Non-Deterministic Finite Automaton</u> (NFA) : 5 Tuple $M(Q, \Sigma, \Delta, s, f)$

↳ Q is finite set of states

↳ Σ finite set of symbols (alphabet of input)

↳ Δ is subset $Q \times \Sigma \times Q$ (transition relation)

↳ s is an element of Q (start state)

↳ F is subset of Q - accepting states.

↳ Non-deterministic as can have one symbol go to multiple states.

<u>Deterministic Finite Automaton</u> : NFA with property that $\forall q \in Q$ $a \in \Sigma_M$ $\exists! q' \in Q \cdot q \xrightarrow{a} q'$

↳ δ is a next state function

↳ We can introduce an ϵ-transition which effectively introduce non-determinism by themselves (NFA$^{\epsilon}$)

Language accepted by NFA : → If there is a path from start to an accepting state, then the string of non-ϵ labels is in Σ^*

↳ The set of accepted strings is $L(M)$

↳ $q \overset{u}{\Rightarrow} q'$ means path from q to q' whose non ϵ labels form $u \in \Sigma^*$

↳ In a DFA, it is an NFA (with a transition mapping Δ being a next-state function δ)

↳ NFA is an NFA$^{\epsilon}$ (with empty ϵ-transition relation)

$L(DFA) \subseteq L(NFA) \subseteq L(NFA^{\epsilon})$

↳ An NFA accepts if there is a path, while in a DFA, the path is determined one symbol at a time

Subset Construction

↳ Given an NFA$^\varepsilon$ M with states Q, we can construct a DFA PM whose states are a subset of Q

↳ Start state of M is set containing start state of M and any states which are reachable by ε-transitions from that state.

↳ Accepting states are any subset containing accepting state.

↳ Alphabet is the same.

Theorem: For each NFA$^\varepsilon$ $M = (Q, \Sigma, \Delta, s, F, T)$, there is a DFA $PM = (\mathcal{P}(Q), \Sigma, \delta, s', F')$ accepting the same strings as M. $(L(PM) = L(M))$

Consider a string $a_1 a_2 \dots a_n \in L(M)$

$s \xRightarrow{a_1} q_1 \xRightarrow{a_2} \dots \xRightarrow{a_n} F$ in M $\quad \therefore L(M) \subseteq L(PM)$

$s' \xrightarrow{a_1} S_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} F'$ in PM

Consider string $a_1 a_2 \dots a_n \in L(PM)$

$S' \xrightarrow{a_1} S_1 \xrightarrow{a_2} \dots \xrightarrow{a_n} S_n \in F'$ in PM

$\therefore L(PM) \subseteq L(M)$

$q_0 \xRightarrow{a_1} q_1 \xRightarrow{a_2} \dots \xRightarrow{a_n} q_n \in F$ in M

$\therefore L(M) = L(PM)$

Kleene's Theorem: a language is regular iff it is equal to $L(M)$ the set of strings accepted by some deterministic finite automaton M.

↳ (a) For any regular expression r, the set $L(r)$ of strings matching r is a ~~rela~~ regular language.

↳ (b) Every regular language is the form $L(r)$ for some regular expression r.

↳ The first part requires us to demonstrate that for any regular expression r, we can construct a DFA, M with $L(M) = L(r)$. Do this by proving for any r, we can construct an NFA$^\varepsilon$ M' with $L(M') = L(r)$ and rely on the subset construction theorem to give us a DFA.

For any regular expression r we can build an NFA$^{\varepsilon}$ M such that $L(r) = L(M)$. Do induction on the depth of abstract syntax trees.

↳ Base Case: Trivially $\{a\}$, $\{\varepsilon\}$ and ϕ are regular language

↳ ① Induction step for $r_1 | r_2$: given NFA$^{\varepsilon}$ M_1 and M_2, we create:

$$L(\text{Union}(M_1, M_2)) = \{u \mid u \in L(M_1) \vee u \in L(M_2)\}$$

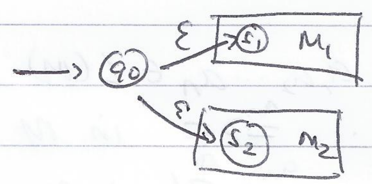
↳ ② Induction step for $r_1 r_2$:

$$L(\text{Concat}(M_1, M_2)) = \{u_1 u_2 \mid u_1 \in L(M_1) \wedge u_2 \in L(M_2)\}$$

↳ ③ Induction step for r^*

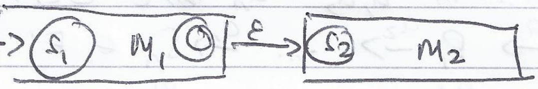
$$L(\text{Star}(M)) = \{u_1 u_2 \ldots u_n \mid n \geq 0 \wedge u_i \in L(M)\}$$

① Union:

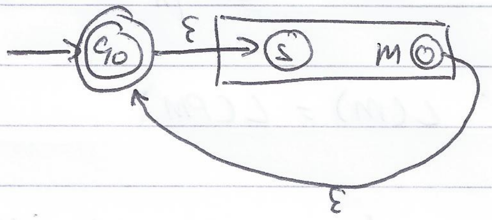


It is clear that this new M accepts any states that either M_1 or M_2 accepts and clearly does not accept any other states

② Concat



③ Star(M)



N.B only accepting state of Star(M) is q_0

Algorithm, given a string u and regular expression r, tells you whether u matches r is: → ① Construct NFA$^{\varepsilon}$ M st $L(M) = L(r)$

↳ ② Get DFA PM equivalent to M through subset construction

↳ ③ Carry out the sequence of transitions corresponding to u from the start state to some state Q (since PM is deterministic, unique transition sequence)

↳ ④ Check if Q is accepting

Exponential Blow-up:

↳ If NFA^{ε} has n states, DFA has 2^n states since member of powerset.

↳ Minimise sets by:

↳ ① Removing non-reachable set.

↳ ② Merging sets iff

↳ (a) Both accepting or both non-accepting

↳ (b) Transition functions are the same

↳ ③ Updating transition functions to take account of merged states

↳ Then repeat.

Lemma: Given an NFA $M = (Q, \Sigma, \Delta, s, F)$, for each subset $S \subseteq Q$ and each pair of states $q, q' \in Q$ $\exists$ reg expression $r^S_{q,q'}$ satisfying

$$L(r^S_{q,q'}) = \{u \in \Sigma^* \mid q \xrightarrow{u}{}^{*} q' \text{ in } M \text{ without intermediate state of the sequence of transitions in } S\}$$

Base case $S = \phi$

Inductive step:

Given states $q, q' \in M$, if $q \xrightarrow{a} q'$ holds for just $a = a_1, a_2 \dots a_n$ then:

$$r^{\phi}_{q,q'} \triangleq \begin{cases} a = a_1 \mid a_2 \mid \dots \mid a_n & \text{if } q \neq q' \\ a = a_1 \mid a_2 \mid \dots \mid a_n \mid \varepsilon & \text{if } q = q' \end{cases}$$

↳ S has $n+1$ elements

↳ Pick some $q_0 \in S$ and consider $S^- = S \setminus \{q_0\}$

↳ Can apply induction hypothesis to S^-, since S^- has n elements

$\therefore$ RTP can express $r^S_{q,q'}$ in terms of only things dependent on S^-

Two possibilities : ① May be able to get from q to q' without going through q_0.

② Go from q to q_0 ~~to~~, stay for arbitrary number of tries then to q'.

$$\therefore \; r^{S}_{q,q'} = r^{S^-}_{q,q'} \mid \left(r^{S^-}_{q,q_0} [r^{S^-}_{q_0 q_0}]^* \, r^{S^-}_{q_0,q'} \right)$$

<u>Other useful patterns</u> : NOT(M)

↳ Given $DFA(M) = (Q, \Sigma, \delta, s, F)$

↳ $Q' = Q$

↳ $\Sigma' = \Sigma$

↳ $\delta' = \delta$

↳ $s' = s$

↳ $F' = \{q \in Q \mid q \notin F\}$

∴ Regular languages are closed under complementation

Regular Languages closed under intersection :

↳ Theorem: If L_1, L_2 are regular languages over Σ, then $L_1 \cap L_2 = \{u \in \Sigma^* \mid u \in L_1 \wedge u \in L_2\}$ is also regular

$$L_1 \cap L_2 = \Sigma^* \setminus ((\Sigma^* \setminus L_1) \cup (\Sigma^* \setminus L_2))$$

↳ So if $L_1 = L(M_1)$ and $L_2 = L(M_2)$

$L_1 \cap L_2 = L(Not(PM))$ where PM is $DFA \equiv M$.

and M is NFE^{ε} Union $(Not(M_1), Not(M_2))$

↳ Corrolary: Given regular expressions r_1 and r_2, there is a regular expression $(r_1 \& r_2)$ ~~which~~ st a string matches iff it matches r_1 and r_2

Finding Equivalent Regular Expressions : Two regular expressions r and s are said to be equivalent if $L(r) = L(s)$, that is, they ~~determ~~ determine exactly the same set of strings via matching.

$L(r) = L(s)$ iff : ① $L(r) \subseteq L(s)$ and $L(s) \subseteq L(r)$

② $(\Sigma^* \setminus L(r)) \cap L(s) = \phi = (\Sigma^* \setminus L(s)) \cap L(r)$

③ $L((\sim r) \,\&\, s) = \phi = L((\sim s) \,\&\, r)$

④ $L(M) = L(N) = \phi$ where M and N are DFAs accepting the sets of strings matched by the regular expression $(\sim r)\,\&\, s$ and $(\sim s)\,\&\, r$

Therefore effectively check, given ~~DFA~~ M, whether it accepts any strings $\Rightarrow$ since finite state, need to check finite number of strings.

Pumping Lemma

Non regular languages → set of strings $\{(,), a, b, \dots, z\}$ in which parantheses are well-nested

↳ Set of palindromes

↳ $\{a^n b^n \mid n \geq 0\}$

For every regular language L, there is a number $\ell \geq 1$, which satisfies the pumping lemma property:

↳ All $w \in L$ with $|w| \geq \ell$ can be expressed as a concatenation of three strings, $w = u_1 v u_2$ where

↳ ① $|v| \geq 1$ (effectively $v \neq \varepsilon$)

↳ ② $|u_1 v| \geq \ell$

↳ ③ $\forall n \geq 0$, $u_1 v^n u_2 \in L$

Using Pumping Lemma to prove language is not regular

① $L_1 \triangleq \{a^n b^n \mid n \geq 0\}$

↳ For each $\ell \geq 1$, take $w = a^\ell b^\ell$

If $w = u_1 v u_2$, with $|u_1 v| \leq \ell$ and $|v| \geq 1$ then for some r and s

↳ $u_1 = a^r$

↳ $v = a^s$ with $r+s \leq l$ and $s \geq 1$

↳ $u_2 = a^{l-r-s} b^l$

↳ $u_1 v^0 u_2 = a^r a^{l-r-s} b^l = a^{l-s} b^l$

But $a^{l-s} b^l \notin L_1$, so by Pumping Lemma, L_1 is not a regular language.

↳ It is important to note that the Pumping Lemma is necessary for a language to be regular, but it is <u>not</u> sufficient