

Chapter 3

Basics

It's time to take a break from history and look at some math from school. Focus will be on concepts and notation rather than theorems and proofs.

3.1 Learning Mathematics

Fads in education come and go. I remember from my first years in school that we were exposed to sets, unions and intersections. No historical civilization I know of started their mathematical development from such concepts. The idea of complementing basic counting and arithmetic with set theory was part of New Mathematics. It all started with Sputnik and American fear of falling behind the Soviet Union in technology and science. Another, more fruitful consequence of the Sputnik crisis was the creation of NASA.

I will not present any views on teaching methods. People are different; a method that works for some would be less suitable for others. But I do think it is important to master one level before going on to a higher more general and abstract level. Before using a calculator you should be skilled in handling calculations in your head and on paper, and before using a symbol handling calculator you should master algebraic manipulation and trigonometrical identities for derivation and integration. That said, devices, programs and apps are powerful tools for mathematical progress.

In this chapter I will give a quick but slightly extended tour of what might be contained in school mathematics up to the university level. This will give me the opportunity to present mathematical notation and symbols that I will use freely in later chapters. Our everyday language is too ambiguous and too wordy for math. Looking back at history, poor notation has often been an obstacle for mathematical progress. Mathematical language can seem quite incomprehensible and discouraging to the uninitiated but the condensed and precise way of writing is essential to see the logical structure, get a quick overview and to free the very limited short-term memory from unnecessary information.

Each branch of mathematics has its objects and operations that are defined by axioms. They are the starting point from which theorems can be derived.

Statements formulated within this context can be true or false. Mathematics is about constructing interesting and useful branches and finding true statements that are informative and not obvious from the definitions.

The axioms should be:

- Self-consistent Not possible to deduce contradictions such as a statement being both true and false.
- Independent No axiom should be deducible from the others. Euclid's parallel axiom was debated for two millennia before being replaced by axioms leading to non-Euclidean geometries.
- Complete Can all relevant theorems be deduced to be either true or false from the axioms, or are more assumptions needed.

Getting theorems from axioms is done by doing logical deductions. This machinery forms a subject of its own outside of any particular mathematical system, like a universal tool for any science or argumentation. Mathematics itself is a powerful tool that can be used to analyze the tool of logic.

Mathematical branches interconnect in complex and surprising ways so there is no given path in the mathematical landscape but some are more natural than others. I will start with logic and set theory. It is not the most natural way for young kids to learn about math but once you have learnt the basics it is a good starting point since it is a foundation on which all of mathematics can be based.

3.2 Logic and Set theory

A correctly formulated mathematical statement should be either true or false. This is the starting point of **propositional logic** also known as **zeroth-order logic**. Atomic statements (P,Q,R,...) are like variables that are either TRUE (1) or FALSE (0). They can be combined with logical operators into compound statements like: $\neg(P \wedge Q) \rightarrow (\neg P \vee \neg Q)$.

Logical operators		
Unary		
NOT	\neg	$\neg P$
Binary		
AND	\wedge	$P \wedge Q$
OR	\vee	$P \vee Q$
IF...THEN...	\rightarrow	$P \rightarrow Q$

Truth table					
P	Q	$\neg P$	$P \wedge Q$	$P \vee Q$	$P \rightarrow Q$
1	1	0	1	1	1
1	0	0	0	1	0
0	1	1	0	1	1
0	0	1	0	0	1

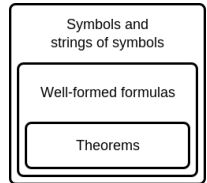
Note that IF P THEN Q has nothing to do with causation, $P \rightarrow Q$ is only false when P is TRUE and Q is FALSE whatever the meaning of P and Q. Another difference with everyday language is P OR Q which is true if one or both of P and Q is true. If you don't want the option where both are true you need an exclusive or, XOR with the same truth table as $(P \vee Q) \wedge \neg(P \wedge Q)$.

Other binary operators could be introduced like $\text{NAND}(P, Q) \equiv \neg(P \wedge Q)$ or $P \leftrightarrow Q \equiv (P \rightarrow Q) \wedge (Q \rightarrow P)$. Any operator $f(P_1, \dots, P_n)$ with a given truth table can be expressed with \neg and \wedge , and they can be reduced to NAND:

$$\begin{array}{ll}
 P \text{ NAND } P \Leftrightarrow & (P \text{ NAND } Q) \text{ NAND } (P \text{ NAND } Q) \Leftrightarrow \\
 \neg(P \wedge P) \Leftrightarrow & \neg(\neg(P \wedge Q) \wedge \neg(P \wedge Q)) \Leftrightarrow \neg\neg(P \wedge Q) \Leftrightarrow \\
 \neg P & P \wedge Q
 \end{array}$$

A common compromise between few and many is to use \neg, \wedge, \vee and \rightarrow . Propositional logic is one of many formal systems. A formal system has a certain structure that can be used to formalize theories within logic or mathematics.

Two forms of logical systems will be presented, propositional logic and predicate logic. They have a formal language with a list of symbols known as an alphabet; rules known as a grammar to construct well-formed formulas of the language and a deductive apparatus with axioms and rules for deducing logical theorems. This is done without any interpretation or meaning given to symbols, formulas or theorems. These “meaningless” aspects of formal languages are called syntax. They are studied in a branch of mathematics called proof theory.



The “meaningful” aspects are called semantics. Meaning is given by introducing an interpretation of non-logical symbols. For instance, P and Q can be linked to propositions that are true or false. The logical symbols \neg and \vee always have their assumed meaning. The truth of sentences and formulas will depend on the interpretation. The interaction between syntax and semantics is studied in model theory. Focus here will be on notation and concepts that are widely used in general mathematics. Proof theory and model theory will be explored more fully in a later chapter.

Formal system	Propositional logic $\mathcal{L}(A, \Omega, Z, I)$	Example
Alphabet	Set A of atomic formulas	$A = \{p, q, r, s, t\}$
	Set Ω of logical operators $\Omega = \Omega_0 \cup \Omega_1 \cup \dots \cup \Omega_n$	$\Omega_0 = \{0, 1\}, \Omega_1 = \{\neg\}$ $\Omega_2 = \{\wedge, \vee, \rightarrow, \leftrightarrow\}$
Grammar for well-formed formulas (wff)	Inductively defined by <ul style="list-style-type: none"> • Elements of set A • If p_1, \dots, p_j wffs and $f \in \Omega_j$ then $(f(p_1, \dots, p_j))$ is a wff 	$(\neg p)$ $(q \wedge r), (s \rightarrow t)$ $((p \rightarrow (q \wedge (\neg r))) \vee s)$ etc.
Deductive system Axioms and Inference rules	Set I of axioms	\emptyset
	Set Z of inference rules	$\{\neg\neg p\} \vdash p$ $\{p, p \rightarrow q\} \vdash q$ etc.

An axiom is a wff of the system but it can also be an axiom schemata where variables can represent any wff, for example:

1. $\phi \rightarrow (\psi \rightarrow \phi)$
2. $(\phi \rightarrow (\psi \rightarrow \chi)) \rightarrow ((\phi \rightarrow \psi) \rightarrow (\phi \rightarrow \chi))$
3. $(\neg\phi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \phi)$

All tautologies can be deduced with these axioms and Modus Ponens $\{p, p \rightarrow q\} \vdash q$ as inference rule. A tautology T is true in every interpretation $\models T$, i.e. T is true for all assignments of truth-values to atomic formulas.

The deductive system is free from interpretation. A formal proof within the system consists of a sequence of wffs, each of which is either an axiom or the result of an inference rule used on previous wffs in the sequence. The meta-language symbol \vdash read as “infers that” is used for inference rules and for proofs. If a wff ψ has been deduced from a set Γ of premises then $\Gamma \vdash \psi$.

The deductive system is “designed” to fit our interpretation of $\{\neg, \wedge, \vee, \rightarrow\}$ as logical connectives {not, and, or, implies} so it is perfectly natural that we get the theorems we expect:








\wedge, \vee	are both commutative and associative	$p \wedge q \leftrightarrow q \wedge p$ $p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$	We can write: $p \vee q \vee r$
\rightarrow	is neither commutative nor associative	$p \rightarrow q \leftrightarrow q \rightarrow p$ $(p \rightarrow q) \rightarrow r \leftrightarrow p \rightarrow (q \rightarrow r)$	
\wedge, \vee	are doubly distributive, inner and outer operators can be interchanged.	$p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r)$ $p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$ $(a \wedge b) \vee (c \wedge d) \leftrightarrow (a \vee c) \wedge \dots \wedge (b \vee d)$	

These rules are good to have in mind in the less formal use of logic in mathematical proofs. Other useful formulas from propositional logic:

$((p \rightarrow q) \wedge p) \vdash q$	Modus Ponens
$((p \rightarrow q) \wedge \neg q) \vdash \neg p$	Modus Tollens
$\neg(p \wedge q) \leftrightarrow (\neg p \vee \neg q)$	De Morgan's law I
$\neg(p \vee q) \leftrightarrow (\neg p \wedge \neg q)$	De Morgan's law II
$(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$	Transposition
$(p \rightarrow q) \leftrightarrow (\neg p \vee q)$	
$((p \wedge q) \rightarrow r) \leftrightarrow (p \rightarrow (q \rightarrow r))$	
$\vdash (p \vee \neg p)$	

The rules obeyed by \wedge , \vee and \neg when working on propositions suggests an algebra of logic. Such a system is called a **Boolean algebra**. It was studied by George Boole in his book *The mathematical analysis of logic* from 1847. The use of the word "algebra" can be a bit confusing. In school it usually means manipulating formulas with x in them. In university it is often preceded by "abstract" and involves the study of algebraic structures, formalized systems based on sets of objects with given operators that obey specified axioms. These structures can be group-like, ring-like, lattice-like, algebra-like etc. An algebra in the latter sense is a vector space with a multiplication operator that takes two vectors into a third vector, a Boolean algebra is not an algebra in this sense. A Boolean algebra is a special case of lattice and ring structures.

Boolean algebra is central for digital electronics and circuit engineering. Diagrams of circuits use the following symbols for logic gates:

						
AND $A \cdot B$	OR $A + B$	NOT \bar{A}	NAND $\overline{A \cdot B}$	NOR $\overline{A + B}$	XOR $A \oplus B$	XNOR $\overline{A \oplus B}$

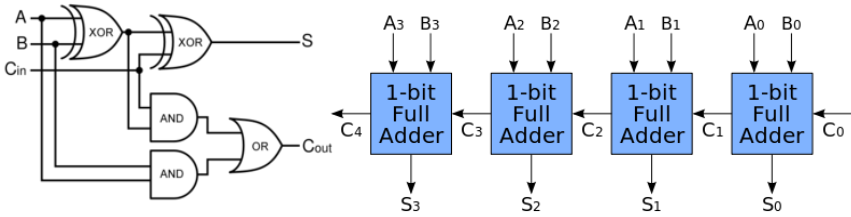


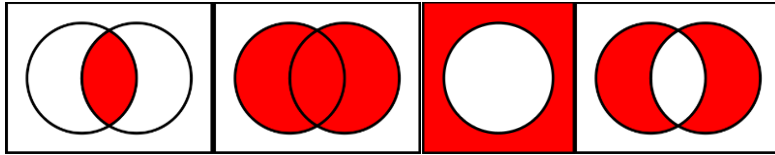
Fig. 3.2.1 Digital circuits for binary addition of 1-bit and 4-bit numbers.

Many branches of mathematics have close links to computer science. One important problem in this area is NP-completeness, how effective can you make an algorithm that decides a certain problem. The first problem to be shown to be NP-complete was the Boolean satisfiability problem (SAT). The question is to decide if there is an assignment of truth-values (interpretation) that makes a given propositional formula true. Such a formula is called satisfiable ($p \wedge \neg p$ is unsatisfiable).

The rules that are obeyed by propositional formulas are also followed by other systems. This makes it useful to strip Boolean algebra of its interpretation and study it as a formal system. A formalized Boolean algebra is set with three operators \wedge, \vee, \neg called meet, join, complement and two elements 0/1 that are sometimes denoted \perp/\top called bottom/top or least/greatest.

Boolean algebra ($A, \wedge, \vee, \neg, 0, 1$)	Example
A is a set	All subsets of a set U $A = 2^U \equiv \{S : S \subseteq U\}$ (the power set)
with operators and members: $\wedge, \vee : A \times A \rightarrow A$ $\neg : A \rightarrow A$ $0 \in A$ and $1 \in A$	$x \wedge y \equiv x \cap y$ $x \vee y \equiv x \cup y$ $\neg x \equiv U - x$ $0 \equiv \emptyset$ and $1 \equiv U$
that satisfy the following axioms:	
$x \wedge (y \wedge z) = (x \wedge y) \wedge z$	Associative $x \vee (y \vee z) = (x \vee y) \vee z$
$x \wedge y = y \wedge x$	Commutative $x \vee y = y \vee x$
$x \wedge 1 = x$	Identity $x \vee 0 = x$
$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$	Distributive $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$
$x \wedge \neg x = 0$	Complement $x \vee \neg x = 1$

A Boolean algebra based on sets has operators meet (\cap) and join (\cup). The names become natural when viewed as Venn diagrams



meet

$$x \wedge y = x \otimes y$$

join

$$x \vee y$$

complement

$$\neg x = U \setminus x$$

XOR

$$x \oplus y$$

The duality in the axioms under exchange of \wedge with \vee and 0 with 1 gives every Boolean algebra a dual with reversed roles of \wedge / \vee and $0 / 1$. A partial order can be introduced in a Boolean algebra by setting $x \leq y$ iff $x = y \wedge x$ or equivalently $y = x \vee y$. In this partial order 0 will be the least element and the greatest element will be 1 . With respect to this partial ordering $x \wedge y$ coincides with infimum and $x \vee y$ coincides with supremum.

A **partially ordered set** (P, \leq) or **poset** is a set with a binary relation \leq s.t.:

$$x \leq y \text{ and } y \leq x \Rightarrow x = y$$

Antisymmetric

$$x \leq x$$

Reflexive

$$x \leq y \text{ and } y \leq z \Rightarrow x \leq z$$

Transitive

Ordering of elements in a Boolean algebra of sets coincides with ordering by inclusion $x \leq y \Leftrightarrow x \subseteq y$. Finite posets can be illustrated by Hasse diagrams.

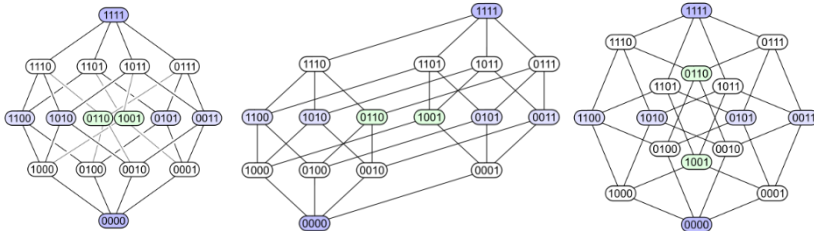
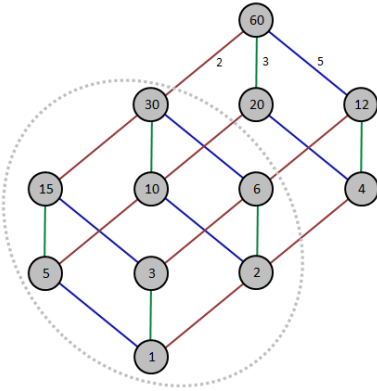


Fig. 3.2.2 Possible Hasse diagrams for binary encoded subsets of a 4-element set

From the Hasse diagrams it's clear that a poset P can have pairs (x, y) that are not comparable, neither $x \leq y$ or $y \leq x$. To impose a Boolean algebra on a poset it should be bounded with a greatest element \top and a smallest one \perp such that $\perp \leq x \leq \top$ for every $x \in P$. If every pair in P has a unique least upper bound called supremum and a unique greatest lower bound infimum then the poset is called a **lattice** L .

Every lattice has natural operations, join $x \wedge y \equiv \inf(x, y)$ and meet $x \vee y = \sup(x, y)$. If these operations are distributive over each other and L is bounded and each element x has a complement $\neg x$ such that $x \vee \neg x = \top$ and $x \wedge \neg x = \perp$ then it is a complemented distributive lattice. Every Boolean algebra is a complemented distributive lattice and vice versa.



An example of a distributive lattice is an integer $n \in \mathbb{Z}^+$ together with its divisors, ordered by divisibility, $x \leq y$ iff $x|y$.

$$x \wedge y = \text{GCD}(x, y)$$

$$x \vee y = \text{LCM}(x, y) \quad \neg x = n/x$$

Only for square-free $n = \prod_{i=1}^n p_i$ will the lattice be complemented, in other words a Boolean algebra.

Fig 3.2.3 Lattice and Boolean algebra.

A Boolean algebra give rise to a Boolean ring $(R, +, \cdot)$ by using $x \cdot y \equiv x \wedge y$ and $x + y \equiv x \vee y \wedge \neg(x \wedge y)$ (XOR). A ring is the algebraic structure that captures the properties of addition and multiplication among integers. A Boolean ring has the extra property that $x \cdot x = x$ for all elements in the ring. Every Boolean algebra is a Boolean ring and vice versa.

Stone’s representation theorem for Boolean algebras from 1936 states that: Every Boolean algebra is isomorphic (basically the same) as a field of sets $\langle X, \mathcal{F} \rangle$ where $\mathcal{F} \subseteq 2^X$ is closed under intersection and union of pairs of sets and complements of sets. The proof associates every Boolean algebra B with a topological space $S(B)$ called the Stone space. The sets that are both closed and open (clopen) of this space are isomorphic to B . Conversely, the clopen sets of any topological space will form a Boolean algebra. For a finite Boolean algebra $\mathcal{F} = 2^X$ for some finite set X which means that the number of elements in a finite Boolean algebra must be a power of two.

If mathematics is the language of science then **set theory** is the language of mathematics. Natural numbers $\{1,2,3, \dots\} \sim \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \dots\}$, ordered pairs $(a, b) \sim \{a, \{a, b\}\}$, functions $f: X \rightarrow Y$ can be seen as subsets S of $X \times Y$ s.t. $\{(x, y_1), (x, y_2)\} \subseteq S \Rightarrow y_1 = y_2$ and $\forall x \in X \exists y \in Y: (x, y) \in S$, and so on.

Georg Cantor (1845–1918), the founder of modern set theory defines a set in *Beiträge zur Begründung der transfiniten Mengenlehre* as:

“A set is a gathering together into a whole of definite, distinct objects of our perception or of our thought – which are called elements of the set”.

Dictionary for the language of sets:

Notion	Notation	Examples and comments
Set	{ }	{1,2,3}, $\mathbb{P} = \{2,3,5,7,11,13,17, \dots\}$
Set-builder	{ : }, { }	$\{x : x \in \mathbb{R} \wedge x > 1\} = \{x \in \mathbb{R} : x > 1\}$ $\{n^2 - n \mid n \in \mathbb{Z} \wedge 0 \leq n \leq 7\}$
Membership	$\in, \exists, \notin, \ni$	$2 \in \{1,2,3\}$, $\mathbb{P} \ni 91$
Equality	$=, \neq$	$A = B \Leftrightarrow (x \in A \Rightarrow x \in B \wedge x \in B \Rightarrow x \in A)$
Subset	$\subseteq, \supseteq, \subsetneq, \supsetneq$	$A \subseteq B \Leftrightarrow (x \in A \Rightarrow x \in B)$ $A \subseteq B \Leftrightarrow B \supseteq A$ (B is a superset of A)
Proper subset	$\subset, \supset, \subsetneq, \supsetneq$	$A \subset B \Leftrightarrow (A \subseteq B \wedge A \neq B)$ Alternative notation for proper subset: \subsetneq, \supsetneq
Empty set	\emptyset	Set containing no elements, $\emptyset = \{ \}$
Universal set	\mathbb{U}	Set with all relevant elements, context dependent.
Union	\cup	$A \cup B = \{x \mid x \in A \vee x \in B\}$
Intersection	\cap	$A \cap B = \{x \mid x \in A \wedge x \in B\}$
Disjoint union	\sqcup	$A_1 \sqcup A_2 = A_1 \times \{1\} \cup A_2 \times \{2\}$
Subtraction	$\setminus, -$	$A \setminus B = A - B = \{x \mid x \in A \wedge x \notin B\}$ a.k.a. Relative complement
Complement	$\complement, ^c, ', \bar{}$	$A^c = \mathbb{U} \setminus A$, $\bar{\emptyset} = \mathbb{U}$
Symmetric difference	Δ	$A \Delta B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$
Cartesian product	\times	$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$
Power set	$\mathcal{P}(S), 2^S$	$\mathcal{P}(S) = \{A \mid A \subseteq S\}$, set of all subsets.
Cardinality	$, \#$	Number of elements in a set: $\#\{a, b\} = 2$, $ \mathbb{R} = \mathfrak{c}$

Notation	Special sets of numbers
$\mathbb{N}, \mathbb{N}_1, \mathbb{Z}^+$	Natural numbers: $\{1, 2, 3, \dots\}$
$\mathbb{N}_0, \mathbb{N}_k, \mathbb{Z}^-$	$\mathbb{N}_0 = \{0, 1, 2, \dots\}$, $\mathbb{N}_k = \{k, k + 1, \dots\}$, $\mathbb{Z}^- = \{-1, -2, \dots\}$
\mathbb{Z}	Integers: $\{0, \pm 1, \pm 2, \dots\}$
$2\mathbb{Z}, 2\mathbb{Z}+1$	Even integers and odd integers
\mathbb{Q}	Rational numbers: $\left\{\frac{a}{b} : (a, b) \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\right\}$
\mathbb{R}	Real numbers
$\mathbb{R} \setminus \mathbb{Q}$	Irrational numbers
\mathbb{A}	Algebraic numbers, solutions to polynomials over \mathbb{Z}
$\mathbb{R} \setminus \mathbb{A}$	Transcendental numbers
\mathbb{C}	Complex numbers: $\{a + ib : (a, b) \in \mathbb{R} \times \mathbb{R}\}$
$\mathbb{C} \setminus \mathbb{R}$	Imaginary numbers
\mathbb{H}	Quaternions: $\{a + ib + jc + kd : (a, b, c, d) \in \mathbb{R}^4\}$

Notation	Symbols and terms of general use in mathematics
s.t. , : ,	Such that
\Rightarrow	If, Implication , Entailment
iff, \Leftrightarrow	If and only if
\forall	For all
\exists	There exists
$\nexists, \neg\exists$	There does not exist
$\exists!$	There exists exactly one
\therefore	Therefore
(a,b)	Ordered pair
(x_1, x_2, \dots, x_n)	Ordered n -tuple
Q.E.D , \square , \blacksquare	Quod Erat Demonstrandum “which is what should be proved”
$\equiv, :=$	Definition
$\dots, \vdots, \ddots, \dotscdot$	Ellipsis, given sequence continues according to given pattern

There are many formulas like $(A \cup B)^c = A^c \cap B^c$ but they all coincide with rules from propositional logic and Boolean algebra $\neg(A \vee B) = \neg A \wedge \neg B$. A convenient way of checking such formulas and to keep track of different possibilities when properties overlap is to draw a Venn diagram.

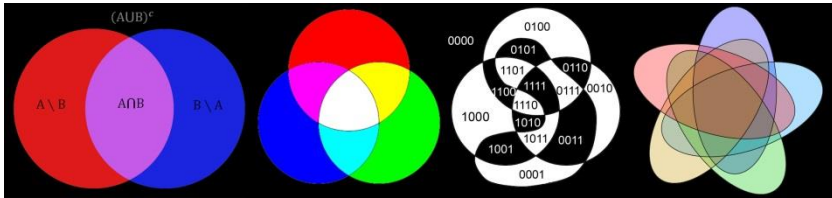


Fig. 3.2.4 Venn diagram for 2, 3, 4 and 5 sets.

A useful formula for combinatorics and probability is the cardinality of a union of sets. It's a generalization of $|A \cup B| = |A| + |B| - |A \cap B|$ to n sets.

$$\left| \bigcup_{i=1}^n A_i \right| = \sum_{i=1}^n |A_i| - \sum_{i < j} |A_i \cap A_j| + \sum_{i < j < k} |A_i \cap A_j \cap A_k| - \dots + (-1)^{n-1} |A_1 \cap \dots \cap A_n|$$

Index sets are used to handle infinite collections of sets. They can be of any size, example: $\mathbb{R} = \bigcup_{i \in \mathbb{R}} A_i$ with $A_i = \{i\}$ and index set \mathbb{R} .

A partition of a set X is a separation of X into mutually disjoint nonempty subsets A_i such that, $X = \bigcup_{i \in I} A_i$ with $A_i \cap A_j = \emptyset$ when $i \neq j$.

In a Cartesian product like $\overbrace{\mathbb{R} \times \dots \times \mathbb{R}}^n = \mathbb{R}^n = \{(x_1, \dots, x_n) : (\forall i)(x_i \in \mathbb{R})\}$, each element can be seen as a function $f: \{1, \dots, n\} \rightarrow \mathbb{R}$. This is a natural way to generalize the definition of Cartesian products to indexed sets $\{X_i\}_{i \in I}$:

$$\prod_{i \in I} X_i \equiv \{f: I \rightarrow \bigcup_{i \in I} X_i \mid (\forall i)(f(i) \in X_i)\} \quad X^I \equiv \prod_{i \in I} X$$

Component x_j is retrieved via projection $(x_1, \dots, x_n) \mapsto x_j$. The general case is handled with projection maps $\pi_j: \prod_{i \in I} X_i \rightarrow X_j$ with $\pi_j(f) = f(j)$. A vector like (x_1, x_2, \dots) is part of the set $\mathbb{R}^{\mathbb{N}}$ which is also denoted as \mathbb{R}^ω .

A formalized theory of sets will require first-order logic. Zermelo–Fraenkel set theory will be described in a later chapter, as will Cantor's foundational contribution with ordinal and cardinal numbers.

If propositional logic is called zeroth-order logic there should be a **first-order logic**. There is and it is called **predicate logic**. Predicate is a Boolean valued function $P: X \rightarrow \{TRUE, FALSE\}$, an example from natural language would be $P(x) = "x \text{ is a philosopher}"$. The variable x ranges over a domain of discourse and when given a value from the domain of people it becomes a proposition like "Plato is a philosopher" that can be true or false. The extension of propositional logic to predicate logic lies in the use of variables and quantifiers; the universal quantification, for every \forall and the existential quantification, there exists \exists . Quantifiers act on free variables which then become bounded variables. In a 2nd order logic, quantifiers can act over predicates or sets, 3rd order logic quantifies over sets of sets and in higher-order logic quantification can be over predicates and sets nested to any depth. The principle of induction can be loosely formulated in 2nd order logic as:

$$\forall P \left((0 \in P \wedge \forall i (i \in P \rightarrow i + 1 \in P)) \rightarrow \forall n (n \in P) \right)$$

This is the last of Peano's axioms that formalize all properties of the natural numbers. A weaker first order system called Peano arithmetic introduces addition and multiplication operators. The induction axiom of 2nd order logic is replaced with axiom schemata of 1st order logic. Löwenheim-Skolem's theorem shows that if there is an infinite model like \mathbb{N} in a 1st order logic then there will be non-standard models different from \mathbb{N} that satisfy all axioms. 2nd order logical systems can capture \mathbb{N} without non-intended models.

Predicates can also be used with set-builder notation to form sets $\{x|P(x)\}$ and Venn diagrams can illustrate formulas like, "every philosopher is mortal" $\forall x(P(x) \rightarrow M(x))$ and "some mortals are not humans" $\exists x(M(x) \wedge \neg H(x))$.

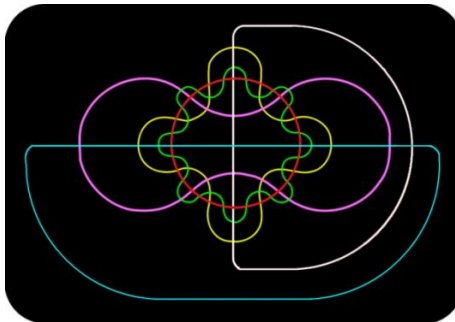


Fig. 3.2.5 Venn diagram of six sets or six predicates.

First order logic	Examples, logic	Examples, math
<p>Alphabet</p> <p>Logical symbols</p> <p>Logical connectives</p> <p>Quantifier symbols</p> <p>Brackets</p> <p>Variables</p> <p>Equality (optional)</p> <p>Non-logical symbols</p> <p>Predicate symbols</p> <p>Function symbols</p>	<p>Logical symbols</p> <p>$\neg, \wedge, \vee, \rightarrow, \leftrightarrow$</p> <p>$\forall, \exists$</p> <p>$()$</p> <p>$x, y, z \dots$ Or $x_0, x_1, x_2 \dots$</p> <p>$=$ (Binary relation)</p> <p>Non-logical symbols</p> <p>$P_0^n, P_1^n, P_2^n \dots n \geq 0$</p> <p>$f_0^n, f_1^n, f_2^n \dots n \geq 0$</p>	<p>Signature $\sigma = (S_f, S_r, ar)$</p> <p>Functions $\in S_f$</p> <p>Relations $\in S_r$</p> <p>ar gives arity of functions and relations</p> <p>Rings: $S_f = \{+, \cdot, -, 0, 1\}$ with arities (2,2,1,0,0)</p> <p>Sets: $S_f = \{\emptyset, C, \mathcal{P}, \cup, \cap\}$</p> <p>$S_r = \{\in, \subseteq\}$</p>
<p>Grammar for wff</p> <p>Terms t_i</p> <p>Inductively defined by:</p> <ol style="list-style-type: none"> Variables $f_i^n(t_1, \dots, t_n)$ <p>Well-formed formulas φ_i</p> <p>Inductively defined by:</p> <ol style="list-style-type: none"> $P_i^n(t_1, \dots, t_n)$ $t_i = t_j$ $\neg \varphi_i, \varphi_i \wedge \varphi_j$, etc. $\forall x_i(\varphi_j), \exists x_i(\varphi_j)$ <p>formulas built from 1 and 2 are called atomic.</p>	<p>Terms t_i</p> <p>x, y, z</p> <p>$f_1^3(x, f_0^2(y, z), f_0^0())$</p> <p>Well-formed formulas φ_i</p> <p>Atomic formulas:</p> <p>$P(x), Q(x, f(y)), x = y$</p> <p>Non-atomic formulas:</p> <p>$x = y \wedge \neg(P(x) = P(f(y)))$</p> <p>$\forall x \forall y (P(x) \rightarrow \neg Q(f(y), z))$</p> <p>$\forall n \neg \exists x \exists y \exists z$</p> <p>$(f_0^3(x, y, n) = f_0^2(z, n) \wedge Q(n, f_2^0()))$</p>	<p>Terms t_i</p> <p>$-z, A \cup B$</p> <p>$\sqrt{x + y^2 + f(x, y)}$</p> <p>Well-formed formulas φ_i</p> <p>Atomic formulas:</p> <p>$A \subseteq B, x \in A$</p> <p>$(x + y + z)/3 \geq (xyz)^{1/3}$</p> <p>Non-atomic formulas:</p> <p>$x \in \mathcal{P}(A) \rightarrow x \subseteq A$</p> <p>$\forall x \forall y \forall z \forall n$</p> <p>$(x^n + y^n \neq z^n \vee n \leq 2)$</p>
<p>Deductive system</p> <p>Axioms, axiom schemas and inference rules</p> <p>Many variations exist:</p> <p>Hilbert-style deduction</p> <p>Natural deduction</p> <p>Sequent calculus</p> <p>etc.</p>	<p>Universal instantiation</p> <p>As axiom scheme</p> <p>$\forall x \varphi \rightarrow \varphi[t/x]$ *</p> <p>As inference rule</p> <p>$\forall x \varphi \vdash \varphi[t/x]$</p> <p>Existential generalization</p> <p>$\varphi[t/x] \vdash \exists x \varphi$</p> <p>etc.</p>	<p>Robinson arithmetic axioms</p> <ol style="list-style-type: none"> $Sx \neq 0$ ** $(Sx = Sy) \rightarrow x = y$ $y = 0 \vee \exists x(Sx = y)$ $x + 0 = x$ $x + Sy = S(x + y)$ $x \cdot 0 = 0$ $x \cdot Sy = (x \cdot y) + x$

* Substitution: $\varphi[t/x]$ where t is a term, x is a variable in φ and all free occurrences of x in φ are replaced by the term t .

** Sx corresponds to successor function

- Parentheses can be used for readability, excess use of parentheses is avoided by establishing an order of evaluation, from first to last $\neg \sim \wedge / \vee \sim \forall / \exists \sim \rightarrow$.
- First order logic with equality is assumed here, a slight extension with a special binary predicate $t_i = t_j$ that satisfies certain axioms and serves as an equality relation.
- The number of arguments of functions and predicates (a.k.a. relations) is called arity.
- Predicate symbols and functions can have arity in \mathbb{N}_0 , $P_i^1(x)$, $P_i^2(x, y)$, $f_i^3(x, y, z)$, ...
- Arity for $n \geq 1$ are called unary, binary, ternary etc. Arity-0 predicates are like propositional variables $\{P, Q, \dots\}$ or constants $\{\text{TRUE}, \text{FALSE}\}$. Arity-0 functions are constant elements of \mathbb{U} the domain of discourse also known as the universal set.
- Symbols of first-order logics that formalize mathematical structures are given by a signature defined by a triple $\sigma = (S_f, S_r, ar)$ with a set of function symbols S_f , a set of relation symbols S_r and an arity function $ar: S_f \cup S_r \rightarrow \mathbb{N}_0$.
Examples are: $S_f = \{0, 1, +, \cdot\}$, $S_f = \{\emptyset, \mathcal{P}, \cup, \cap\}$, $S_r = \{T, F, \in, \subseteq\}$ or $S_r = \{=, \leq\}$.
The cardinality of a signature σ is $|\sigma| = |S_f| + |S_r|$
- Mathematical functions and relations are often written with infix or other notation:
Function: $+(x, y) \sim x + y$, $\mathcal{P}^1(X) \sim 2^X$, Relation (predicate): $\leq(x, y) \sim x \leq y$
- \forall and \exists can replace each other: $\forall x P x \sim \neg \exists x \neg P x$ and $\exists x P x \sim \neg \forall x \neg P x$.
- Universal and existential quantifiers do not commute, order matters as can be seen in a binary predicate like $L(x, y) = \text{"x likes y"}$, $\forall x \exists y L(x, y) \neq \exists y \forall x L(x, y)$.
Another example is pointwise (1) and uniform (2) continuity of a function $f: \mathbb{R} \rightarrow \mathbb{R}$.
(1) $\forall \epsilon > 0 \forall x \in \mathbb{R} \exists \delta > 0 \forall h \in \mathbb{R} (|h| < \delta \rightarrow |f(x) - f(x+h)| < \epsilon) \rightarrow \delta(\epsilon, x)$
(2) $\forall \epsilon > 0 \exists \delta > 0 \forall x \in \mathbb{R} \forall h \in \mathbb{R} (|h| < \delta \rightarrow |f(x) - f(x+h)| < \epsilon) \rightarrow \delta(\epsilon)$
- Unique existence can be expressed as $\exists! x P(x) \sim \exists x (P(x) \wedge \forall y (P(y) \rightarrow (x = y)))$
- In a formula like $\forall x (P(y) \rightarrow \exists z Q(x, z))$ is y a free variable while x and z are bound. A formula with no free variables is a first-order sentence, it is either true or false.
 $\forall y \exists x (x^2 = y)$ is true for $\mathbb{U} = \mathbb{R}^+$ or \mathbb{C} but false when $\mathbb{U} = \mathbb{R}$ whereas the truth of $\exists x (x^2 = y)$ with $\mathbb{U} = \mathbb{R}$ will depend on if y is substituted with a negative or positive.
- The deductive system is purely syntactic, a formalized way of deriving logical consequences of a set of wffs Γ , $\Gamma \vdash \varphi$. The derivation itself is a syntactic object.
- Hilbert-Style deduction systems are axiomatic, many schemes of axioms and few inference rules, modus ponens and universal generalization: if $\vdash P(x)$ then $\vdash \forall x P(x)$
- Natural deduction systems replace axioms with rules of inference as much as possible.

3.3 Arithmetic

The limitations of classical Greek mathematics; no zero, no negative numbers and no fractional arithmetic were not due to any lack of intelligence or creativity of the Greeks. It had more to do with preconceived, philosophically grounded notions of what a number is. A modern approach would be to introduce a neutral element with respect to addition, give it a symbol, and a meaning that amount to “nothing”, $x + 0 = x$. Then we could introduce an imaginary number \bar{x} to each natural number x and call it the additive inverse of x with the property $x + \bar{x} = 0$. Its meaning would be “a lack of x ”. Arithmetic could be expanded to these new numbers:

$$x + \bar{y} = \begin{cases} x - y & \text{if } x > y \\ 0 & \text{if } x = y \\ \bar{y} - \bar{x} & \text{if } x < y \end{cases} \quad \begin{array}{l} \bar{x} + \bar{y} = \overline{x + y} \\ x - \bar{y} = x + y \\ \bar{x} - y = \overline{x + y} \\ \bar{x} - \bar{y} = y + \bar{x} \end{array} \quad x - y = \begin{cases} x - y & \text{if } x > y \\ 0 & \text{if } x = y \\ \bar{y} - \bar{x} & \text{if } x < y \end{cases}$$

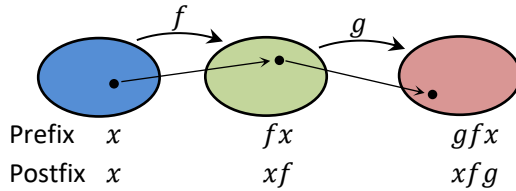
The rules of arithmetic would still apply for this extended set of numbers and $x - y$ has become meaningful also when $y > x$.

These new numbers are of course the negative numbers that we denote $-x$. This notation and our name for it “minus” are the same that we use for subtraction; an unfortunate coincidence that has caused much confusion for children learning math and headaches for teachers teaching math. So much that elementary education in the U.S. has replaced the term “minus x ” with “negative x ”. Math.stackexchange has a thread “Negative” vs “Minus” on the pros and cons of these conventions. The crucial difference is that subtraction is a binary operator whereas additive inverse is a unary operator. Some confusion such as having two calculator buttons with the same sign could have been avoided with a special symbol for negative, maybe $\dot{-}$ with one dot to show its unary nature with one argument after or below the symbol.

Mathematical notations are full of possibilities, often decided by historical accident in a contest between old notation with tradition and acquaintance challenged by new and improved notation. If there had not been a symbol for pi already then $\tau \equiv 2\pi$ would surely be the natural constant to introduce. Another choice is the position of the operator in relation to the argument.

Prefix $-x$	Postfix $x!$	Around $ x $	Upfix \bar{x}	Infix (\leftrightarrow) $x + y$	Infix (\Downarrow) $\frac{x}{y}$
----------------	-----------------	-----------------	--------------------	--	---

Prefix notation is also called Polish notation whereas postfix notation is called reverse polish notation (RPN). Everybody with a HP-calculator is familiar with the advantages of using postfix operation. By putting numbers on a stack you can avoid parentheses and make your bench neighbor very confused when he or she has to borrow your calculator. Functional notation is usually written in prefix notation $f(x)$ or fx but with postfix notation xf , reading direction and order of actions would become the same.



Another common source of misunderstanding is the different meaning of parentheses in $f(x)$ and $x(y + z)$. It would probably be better to use square brackets for function arguments $f[x]$.

The second use of parentheses is used to show the intended order of evaluation. The default precedence of operators is:

- 1. Unary operators $-n! = -(n!)$
- 2. Exponents and roots
- 3. Multiplication and division $a/b \cdot c = a \cdot \frac{1}{b} \cdot c$
- 4. Addition and subtraction $a - b + c = a + (-b) + c$

The ambiguity in point 3 and point 4 is resolved by calculating from left to right which is what you get if you treat division as multiplication with the reciprocal and subtraction as addition with additive inverse. Multiplication and addition are associative so order of evaluation is no longer an issue. Exponentiation is not associative $(a^b)^c \neq a^{(b^c)}$. The natural choice is to do it the right-associative way $a^{b^c} \equiv a^{(b^c)}$. Parentheses can be replaced with other brackets like [] or { } when it simplifies reading.

The horizontal bar in the division and root symbol functions as a parenthesis.

$$\sqrt{x + y} = (x + y)^{1/2}$$

$$\frac{1}{x + y} = 1/(x + y)$$

Summation and multiplication of many arguments is best done with the sum and product symbols, Greek capital letter S and Greek capital letter P.

$$\sum_{i=1}^n a_i \equiv a_1 + a_2 + \dots + a_n \quad \prod_{j \in \mathbb{Z}^+} b_j \equiv b_1 \cdot b_2 \cdot \dots \quad \prod_{k=1}^n k = 1 \cdot 2 \cdot \dots \cdot n \equiv n!$$

Big numbers part 2

Repeated factorials $n!!$ is no match against repeated exponentiation n^{n^n} . In part one of our quest for large numbers we saw Knuth's up arrows. The next step is Conway chained arrow notation created by John H. Conway. A chain of length n , $p_1 \rightarrow p_2 \rightarrow \dots \rightarrow p_n$ has a value defined recursively:

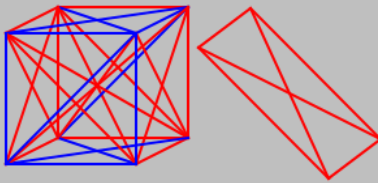
1. $p \rightarrow q \equiv p^q \quad (p, q \in \mathbb{Z}^+)$
2. $X \rightarrow 1 \equiv X \quad (X \text{ is any chained expression})$
3. $X \rightarrow p \rightarrow (q + 1) \equiv \underbrace{X \rightarrow (X \rightarrow (\dots (X \rightarrow (X) \rightarrow q) \dots)) \rightarrow q}_{p \text{ repetitions of } X} \rightarrow q$

Example:

$$\begin{aligned} a \rightarrow b \rightarrow 2 &= \underbrace{a \rightarrow (a \rightarrow \dots (a \rightarrow a \rightarrow 1) \dots) \rightarrow 1}_{b \text{ repetitions of } a \rightarrow} \\ &= \underbrace{a \rightarrow (a \rightarrow \dots (a \rightarrow a^a \rightarrow 1) \dots) \rightarrow 1 \rightarrow 1}_{b-2 \text{ repetitions of } a \rightarrow} \\ &= a^{\dots^a} \} b \text{ levels} = a \uparrow\uparrow b = a \uparrow^2 b \end{aligned}$$

Chains of length three match Knuth's up arrows, $p \rightarrow q \rightarrow r = p \uparrow^r q$. Calculate $3 \rightarrow 3 \rightarrow 3 \rightarrow 2$ and you'll see Conway's \rightarrow outgrow Knuth's \uparrow . Chains of length 5 will beat anything expressible with up-arrows. A good show of this is Metzler's YouTube "Ridiculously huge numbers", part 3.

Can numbers of these magnitudes that make a googolplex look like an infinitesimal be of any use? Yes, one such big number once occurred as an upper bound to the following problem. Connect all vertices in a cube of n dimensions and color the edges blue or red. What is the smallest n for which every coloring has at least one single-colored graph of four coplanar vertices? This number N was known to be finite $6 \leq N \leq \bar{N}$. An upper bound G called Graham's number became famous in 1977 as the largest number ever used in a proof. $G = f^{64}(4)$ with $f(n) = 3 \uparrow^n 3$. In Conway notation $3 \rightarrow 3 \rightarrow 64 \rightarrow 2 < G < 3 \rightarrow 3 \rightarrow 65 \rightarrow 2$. The upper and lower bounds have since improved to $13 \leq N \leq 2 \uparrow\uparrow\uparrow 6$.

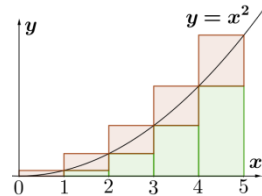


$$G = \left. \begin{array}{l} 3 \uparrow\uparrow \dots \uparrow 3 \\ \underbrace{3 \uparrow\uparrow \dots \uparrow 3} \\ \vdots \\ \underbrace{3 \uparrow\uparrow \dots \uparrow 3} \\ 3 \uparrow\uparrow\uparrow 3 \end{array} \right\} 64 \text{ layers}$$

A famous anecdote of Gauss says that when he was eight years old his teacher gave the class a problem to keep them occupied; add all numbers from 1 to 100. After a few seconds Gauss gave the answer 5050 and said it was quite simple, just add $100+1$ and multiply by 50.

$$S_1(n) = \sum_{k=1}^n k = \frac{(n+1) \cdot n}{2}$$

$$S_2(n) = \sum_{k=1}^n k^2$$



The second problem looks as if it could be a polynomial of degree three.

$$\frac{n^3}{3} = \int_0^n x^2 dx \leq \sum_{k=0}^n k^2 \leq \int_1^{n+1} x^2 dx = \frac{(n+1)^3 - 1}{3}$$

$$3 \cdot \sum_{k=0}^n k^2 = n^3 + a_2 n^2 + a_1 n + a_0 \quad \text{with } 0 \leq a_2 \leq 3$$

$$n = 0 \rightarrow a_0 = 0$$

$$n = 1 \rightarrow a_1 + a_2 = 2 \quad \rightarrow 3 \cdot \sum_{k=0}^n k^2 = \frac{2n^3 + 3n^2 + n}{2} \quad (\text{Conjecture})$$

$$n = 2 \rightarrow 2a_1 + 4a_2 = 7$$

Proof by induction.

It is true for $n=0$, assume it is true for n then:

$$6 \cdot \sum_{k=0}^{n+1} k^2 = 2n^3 + 3n^2 + n + 6(n+1)^2 = 2(n+1)^3 + 3(n+1)^2 + (n+1)$$

$$\therefore \sum_{k=1}^n k^2 = \frac{2n^3 + 3n^2 + n}{6}$$

$$\text{Sum of powers: } S_p(n) = \sum_{k=1}^n k^p = \frac{1}{p+1} \sum_{j=0}^p (-1)^j \binom{p+1}{j} B_j n^{p+1-j}$$

The Bernoulli numbers $B_n \in \mathbb{Q}$ have deep connection to number theory and the Riemann zeta function $\zeta(s)$. They occur in the Taylor expansion of $\tan(x)$ and many other places, $(B_n)_{n=0}^\infty = (1, -\frac{1}{2}, \frac{1}{6}, 0, -\frac{1}{30}, 0, \frac{1}{42}, \dots)$.

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ is prime}} \frac{1}{1-p^{-s}} \quad s \in \mathbb{C} \setminus \{1\}, \zeta(-n) = -\frac{B_{n+1}}{n+1} \quad n \in \mathbb{N}$$

The arithmetic properties of addition and multiplication among integers can be summarized as a set \mathbb{Z} with two binary operators $(+, \cdot): \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, with neutral elements zero and one $(\mathbb{Z}, +, \cdot, 0, 1)$ that satisfies: (Axioms of a ring)

- $(a + b) + c = a + (b + c)$ Addition is associative
- $a + b = b + a$ commutative
- $a + 0 = a$ has an additive identity
- $a + (-a) = 0$ and an additive inverse $-a$
- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ Multiplication is associative
- $a \cdot b = b \cdot a$ commutative (optional for a ring)
- $a \cdot 1 = a$ has a multiplicative identity
- $a \cdot (b + c) = ab + ac$ Multiplication is distributive over addition

Like we did for logical systems we can collect these properties or axioms and study them without any special interpretation in mind. This is practical since many structures obey the same rules, polynomials is one example. What we learn will apply to any algebraic structure that follows the rules. The name of the structure is a ring $(R, +, \times, 0_R, 1_R)$. It's a bit more general than described above; multiplication does not have to be commutative so 1_R must also obey $1_R \cdot a = a$ for every element in R and the distributive law should apply both from the left $a \times (b + c) = (a \times b) + (a \times c)$ and from the right $(b + c) \times a = (b \times a) + (c \times a)$. Our familiar $(\mathbb{Z}, +, \cdot, 0, 1)$ is a commutative ring. Equations like $a + x = b$ are solved by introducing subtraction $a - b \equiv a + (-b)$. The natural numbers \mathbb{N} is not a ring, it does not have additive inverses and no guaranteed solution to $a + x = b$.

The Greeks had philosophical concerns over incorporating fractional numbers into their arithmetic. For a long time they were relegated to geometry. To introduce division into our number system so that we can solve equations of the form $a \cdot x = b$ we need to introduce rational numbers. The modern approach to introduce rational numbers works for any commutative ring with the additional property that the product of any two nonzero elements is nonzero. This is called an integral domain and its supersized version is a field of fractions. An example of a ring where this would not work is \mathbb{Z}_6 , integers modulo 6. What would be the meaning of $1/2 \cdot 1/3$?

The stage is set for a formal introduction of division and rational numbers. Rational numbers are ordered pairs $(p, q) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ where we regard some pairs like $(1, 2)$ and $(2, 4)$ as basically identical. This merger is done by an equivalence relation, $(p_1, q_1) \sim (p_2, q_2)$ if and only if $p_1 q_2 = p_2 q_1$.

With rational numbers and their arithmetic in place we can now solve the equations from chapter one, but to handle the repeating decimals such as $1/3 = 0.333 \dots$ we need to introduce limits.

Let $S_n = \sum_{k=1}^n \frac{3}{10^k} = 0.\underbrace{33\dots3}_{n \text{ digits}}$. The limit of S_n as $n \rightarrow \infty$ is defined by

$$\lim_{n \rightarrow \infty} S_n = S \text{ if } \forall \varepsilon \in \mathbb{Q}^+ \exists N \in \mathbb{N} : (n > N \Rightarrow |S_n - S| < \varepsilon)$$

Applied to $x_n = \frac{1}{n}$ we can choose $N = \frac{1}{\varepsilon}$ and get $\lim_{n \rightarrow \infty} \frac{1}{n} = 0$.

A partial or total order on a set A is a **dense order** iff for every $x \in A$ and every $y \in A$ s.t. $x < y$ there is a $z \in A$ s.t. $x < z < y$. \mathbb{Q} is obviously dense $x + \frac{1}{n} \rightarrow x$ as $n \rightarrow \infty$ and $z = \frac{x+y}{2}$ is a number that fits the description. Even though rational numbers are dense they can still be counted as if they were standing on a line $(x_1, x_2, x_3 \dots)$.

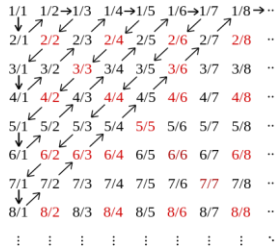


Fig. 3.5 Counting the rational numbers \mathbb{Q}^+ (reds have already been represented).

Any two sets that are totally ordered, dense and countable are order-isomorphic. For the usual order relations on natural numbers and algebraic numbers there must be a bijection $f: \mathbb{Q} \rightarrow \mathbb{A}$ s.t. $x <_{\mathbb{Q}} y \Leftrightarrow f(x) <_{\mathbb{A}} f(y)$.

A set with a distance measure is called a metric space. A Cauchy sequence is a sequence whose members approach each other. A complete metric space M is a space where every Cauchy sequence has a limit also in M .

Distance measure:

$$D: M \times M \rightarrow [0, \infty)$$

$$D(x, y) \geq 0$$

$$D(x, y) = 0 \Leftrightarrow x = y$$

$$D(x, y) = D(y, x)$$

$$D(x, z) \leq D(x, y) + D(y, z)$$

Cauchy sequence, $(a_n)_{n=1}^{\infty}$:

$$\forall \varepsilon > 0 \exists N \forall m, n > N : D(a_m, a_n) < \varepsilon$$

Complete metric space, M :

$$(a_n)_{n=1}^{\infty} \text{ a Cauchy sequence in } M \Rightarrow$$

$$\exists a \in M: a_n \rightarrow a \text{ as } n \rightarrow \infty$$

\mathbb{Q} is a metric space with distance measure $D(x, y) = |x - y|$. The series defined by $x_1 = 1$ and $x_{n+1} = x_n/2 + 1/x_n$ is a Cauchy sequence with no limit in \mathbb{Q} since any limit would have to satisfy $x^2 = 2$ which as we have seen is not a member of \mathbb{Q} . Hence \mathbb{Q} is uncomplete and there are many gaps to fill if every Cauchy sequence is to have a limit in \mathbb{Q} . Every non-complete metric space M can be made into a complete metric space \bar{M} that contains M as a **dense subspace**. A dense subspace means that every point in \bar{M} belongs to M or is a limit point of points in M .

Completion of M is done by setting up the set of Cauchy sequences C . The distance between $x = (x_n)$ and $y = (y_n)$ is $D(x, y) := \lim_n D(x_n, y_n)$. To make it a proper distance measure (axiom 2) we introduce an equivalence relation, $x \sim y$ iff $D(x, y) = 0$ and let \bar{M} be the quotient set C/\sim . Any element m in M is naturally embedded in \bar{M} as the sequence (m, m, \dots) . This can be done for \mathbb{Q} if care is taken in not assuming the completeness of the real numbers since they are under construction $\bar{\mathbb{Q}} = \mathbb{R}$. Addition and multiplication of Cauchy sequences are given by $(x_n) + (y_n) := (x_n + y_n)$ and $(x_n) \cdot (y_n) := (x_n \cdot y_n)$. In this way we get the real numbers \mathbb{R} with all its arithmetical properties as the completion of the rational numbers. There are many other ways of setting up the real numbers.

Decimal notation has a natural connection to Cauchy sequences. π is the equivalence class $[(3, 3.1, 3.14, 3.141, 3.1415, \dots)] = 3.1415 \dots$. When I introduced my problems from chapter one and failed to convince one of my students that $0.999 \dots = 1$ I should have said. Yes, $0.999 \dots$ and 1 represent different Cauchy sequences but they belong to the same equivalence class of the equivalence relation used when constructing \mathbb{R} from \mathbb{Q} .

Another construction is named after Richard Dedekind (1831–1916). In the Dedekind cut, \mathbb{Q} is partitioned into two sets $\mathbb{Q} = L \cup U$ in such a way that the lower set L has no greatest element and all its elements are less than any element in the upper set U . If U has a smallest element the cut represents that element, if not it defines an irrational that fills the gap in the cut. Ordering and arithmetic on Dedekind cuts (L, U) and embedding of \mathbb{Q} into them are easily defined with common set operations.

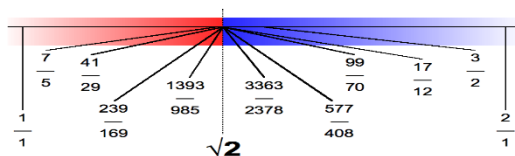


Fig 3.3.1 Dedekind cut for $L = \{x \in \mathbb{Q} | x^2 < 2\}$ and $U = \mathbb{Q} \setminus L$.

After completion there are no gaps, the real numbers corresponds to the Greek geometric idea of the continuum on a straight line. Any bounded set $S \subset \mathbb{R}$ has a greatest lower bound $x = \inf(S)$ in \mathbb{R} , the **infimum** and a least upper bound in \mathbb{R} , $y = \sup(S)$, the **supremum**. If S is not bounded then $\inf(S) = -\infty$ or $\sup(S) = \infty$. Infimum and supremum can also be used on subsets of partially ordered sets (P, \leq) . For natural numbers ordered by divisibility $(\mathbb{N}, |)$ we get $\inf(\{a, b\}) = \gcd(a, b)$, greatest common divisor and $\sup(\{a, b\}) = \text{lcm}(a, b)$, least common multiple. For the subset ordering $(\mathcal{P}(S), \subseteq)$, $\inf(\{A, B\}) = A \cap B$ and $\sup(\{A, B\}) = A \cup B$.

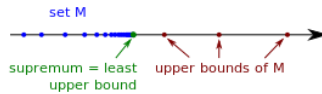


Fig 3.3.2 Supremum of a set.

Real numbers can also be constructed by axioms. \mathbb{R} is a set \mathbf{R} that has elements $(0,1)$, binary operators $(+, \cdot)$ and an order relation (\leq) for which:

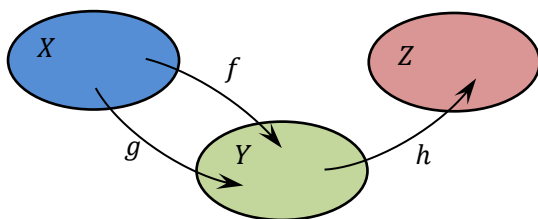
1. $(\mathbf{R}, +, \cdot, 0, 1)$ is a field which means that for each $x, y, z \in \mathbf{R}$: (Definition of a field)
 - $x + (y + z) = (x + y) + z$ and $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ Associative
 - $x + y = y + x$ and $x \cdot y = y \cdot x$ Commutative
 - $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ Distributive
 - $x + 0 = x$ Additive identity
 - $x \cdot 1 = x$ Multiplicative identity
 - $x + (-x) = 0$ Additive inverse $-x$ exists
 - $x \cdot (x^{-1}) = 1$ Multiplicative inverse x^{-1} exists if $x \neq 0$
2. (\mathbf{R}, \geq) is a totally ordered set and for each $x, y, z \in \mathbf{R}$:
 - $x \leq x$ Reflexive
 - $x \leq y$ and $y \leq x \Rightarrow x = y$ Antisymmetry
 - $x \leq y$ and $y \leq z \Rightarrow x \leq z$ Transitive
 - $x \leq y$ or $y \leq x$ Total
3. $(+, \cdot)$ are compatible with the order (\leq) and for each $x, y, z \in \mathbf{R}$:
 - $x \leq y \Rightarrow x + z \leq y + z$ Preservation of order under addition
 - $x \geq 0$ and $y \geq 0 \Rightarrow x \cdot y \geq 0$ Preservation of order under multiplication
4. The order is complete:
 - Every non-empty subset of \mathbf{R} bounded from above has a least upper bound in \mathbf{R} .

These axioms are enough to “characterize” \mathbb{R} . If $(R, 0_R, 1_R, +_R, \times_R, \leq_R)$ and $(S, 0_S, 1_S, +_S, \times_S, \leq_S)$ are two models that satisfy all of these axioms then there will be a structure preserving bijection $f: R \rightarrow S$ such that:

- $f(0_R) = 0_S$ and $f(1_R) = 1_S$
- $f(x +_R y) = f(x) +_S f(y)$ and $f(x \times_R y) = f(x) \times_S f(y)$
- $x \leq_R y \Leftrightarrow f(x) \leq_S f(y)$

Functions

A function f is a relation between a **domain** X and a **codomain** Y such that each element $x \in X$ is related to exactly one element $y = f(x) \in Y$.



$f: X \rightarrow Y$
 $x \mapsto f(x)$
 \square
 $g: X \rightarrow Y$
 $x \mapsto g(x)$
 \square
 $h: Y \rightarrow Z$
 $y \mapsto h(y)$

Pointwise operation:

$f * g: X \rightarrow Y$ if $*$ defined on Y
 $x \mapsto f(x) * g(x)$

Composition:

$h \circ f: X \rightarrow Z$ if $f(X) \subseteq h^{-1}(Z)$
 $x \mapsto h(f(x))$

If $A \subseteq X$ then $f(A) \equiv \{f(x) | x \in A\}$ is called the **image** of A under f .

If $B \subseteq Y$ then $f^{-1}(B) \equiv \{x \in A | f(x) \in B\}$ is the **preimage** of B under f .

The preimage of a single element $f^{-1}(y)$ is the **fiber** of y under f .

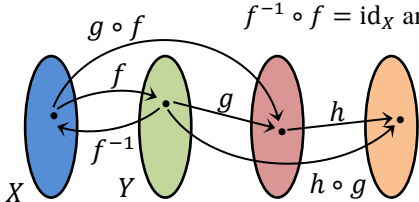
If $x \neq y \Rightarrow f(x) \neq f(y)$ then f is an **injective** function.

If $f(X) = Y$ then f is a **surjective** function.

If f is both injective and surjective then f is a **bijective** function.

These terms were introduced by the Bourbaki group, a group of French mathematicians, that wrote under the pseudonym Nicolas Bourbaki.

Every set X has an identity function, $id_X: X \rightarrow X, x \mapsto x$ and every bijective function $f: X \rightarrow Y$ has an **inverse** $f^{-1}: Y \rightarrow X$ such that:



Composition is associative
 $h \circ (g \circ f) = (h \circ g) \circ f$
 If $f: X \rightarrow X$ then $f^n \equiv f \circ f^{n-1}$
 but not commutative $g \circ f \neq f \circ g$
 $f(x) = x - 1, g(x) = 2 \cdot x \curvearrowright$

A **restriction** of $f: X \rightarrow Y$ to $S \subset X$ is written $f|_S: S \rightarrow Y, x \mapsto f(x)$.

If g is a restriction of f then f is an **extension** of g .

The set of all functions $f: X \rightarrow Y$ form a set denoted $Y^X \equiv \{f | f: X \rightarrow Y\}$.

Rational numbers are represented by two integers and they are countable. The real numbers can be represented by an infinite series of digits.

$$x \in \mathbb{R} \iff x = \dots d_1 d_0 . d_{-1} d_{-2} \dots$$

with $d_i \in \{0, 1 \dots b - 1\}$ for some $b \in \{2, 3 \dots\}$
and $d_i = 0$ when $i > N$ for some $N \in \mathbb{Z}$

This is the positional system in base b . Each digit d_i represents a value that depends on its position i , $d_i \sim d_i \cdot b^i$. The point between the integer part and the rest is the radix point. The word “digit” is used in medicine and anatomy. It comes from the Latin “digitus” which means finger or toe. It is no wonder that most number system through history have used base 10. Assuming base 10, the value of x is:

$$x = \sum_{i \in \mathbb{Z}} d_i \cdot 10^i = \sum_{k=0}^{\infty} d_{N-k} \cdot 10^{N-k}$$

x corresponds to the class of Cauchy sequences represented by the rational numbers $S_n = \sum_{k=0}^n d_{n-k} 10^{N-k}$. Each digit sequence represents a unique real number except for $\dots d_{i+1}(d_i - 1)999 \dots$ and $\dots d_{i+1}d_i 000 \dots$. They represent the same number. My argument for this with my student was $0.\bar{3} = 1/3$ so $(\times 3) \Rightarrow 0.\bar{9} = 1$. Initial zeros before the decimal point and trailing zeros after the decimal point can be ignored.

Different symbols are used for digits in different parts of the world but 123 is written in the same direction whether it is used in a left-to-right written language such as English, Sanskrit or Hindi (Devanagari script) or in a right-to-left written language such as Hebrew, Arabic, Persian or Urdu (Persian alphabet). Positional notation had its origin in India and spread to the west via the Arab world. It would have been a source of many mishaps had they chosen different conventions with a risk of mistaking 123 for 321. Some languages such as Danish and German use both directions when they speak of numbers like “einhundertdreißigundzwanzig”.

Two set of conventions exist for byte ordering in the digital world where numbers are handled in a binary, octal or hexadecimal base, $b = 2, 8$ or 16 . In a little-endian format as used in Intel processors the least significant byte of a word is stored in the lower memory address while a big-endian format as used by Motorola processors and Internet protocols stores word in reversed order. Today many processors are bi-endian with switchable endianness.

On page 3 with the division algorithm it was shown how a fraction p/q leads to a string of digits $(d_N \dots d_1 d_0 . d_{-1} \dots)_b$ that ends either in a string of zeros, effectively a finite expansion or a repeating block of digits.

From periodic decimal to quotient p/q .

A periodic decimal can be written $x = (a_1 \dots a_i . b_1 \dots b_j \overline{c_1 \dots c_k})_b$

$$x = a_1 \dots a_i + b^{-j} \cdot b_1 \dots b_j + b^{-j} \cdot 0.\overline{c_1 \dots c_k}$$

$$(b^k - 1) \cdot 0.\overline{c_1 \dots c_k} = c_1 \dots c_k \Rightarrow 0.\overline{c_1 \dots c_k} = \frac{c_1 \dots c_k}{b^k - 1}$$

$$x = a_1 \dots a_i + \frac{b_1 \dots b_j}{b^j} + \frac{c_1 \dots c_k}{b^{j+k} - b^j} = \frac{P}{Q} = \frac{P/\text{GCD}(P, Q)}{Q/\text{GCD}(P, Q)} = \frac{p}{q}$$

Example: $x = 12.\overline{345}$ with $b = 10$, $i = 2$, $j = 0$, $k = 3$

$$x = 12 + \frac{345}{999} = \frac{12333}{999} = \frac{4111}{333}$$

Finite or infinite expansion and length of repeating block depends on base.

$$(1.0101 \dots)_2 = 1 + \frac{(01)_2}{2^2 - 2^0} = 1 + \frac{0}{2^1} + \frac{(10)_2}{2^3 - 2^1} = 1 + \frac{1}{3} = (1.1)_3 = 1.\overline{3}$$

Which fractions have finite expansions?

$$\frac{p}{q} = \left[\frac{p}{q} \right] + \sum_{k=1}^N \frac{d_i}{b^i} (\times b^N) \Rightarrow \frac{pb^N}{q} \in \mathbb{Z} \quad (p, q) = 1 \Rightarrow$$

q can have no prime factors other than those in the base.

Base 10: $b = 2 \cdot 5 \Rightarrow p/q$ has an finite decimal expansion if $q = 2^m 5^n$

$\frac{p}{q}$ has an infinite decimal expansion if $q \in \{3, 6, 7, 9, 11, 12, 13, 14, 15, 17, \dots\}$

The gaps in \mathbb{Q} , the irrational numbers correspond to infinite strings of digits with no repeating block. How many gaps are there? Cantor introduced a way to measure the size of infinite sets, their cardinality. For a finite set A the cardinality is simply the number of elements in A , $|A| \in \mathbb{N}_0$, $|\emptyset| = 0$. If there is a pairing of elements between A and B , a bijection, then $|A| = |B|$. The same should apply to infinite sets.

$|A| = |B|$ if there is a bijective function $f: A \rightarrow B$.

$|A| \leq |B|$ if there is an injective function $f: A \rightarrow B$.

$|A| < |B|$ if $|A| \leq |B|$ and not $|A| = |B|$.

A set S is countable iff $|S| = |\mathbb{N}_1|$, $S = \{f(1), f(2), \dots\}$. The first letter in the Hebrew alphabet is used for infinite cardinals. Countable sets have cardinality aleph-null, $|\mathbb{N}_1| = \aleph_0$. Dedekind defined an infinite set as a set that has the same cardinality as a proper subset, $|\mathbb{N}_0| = |\mathbb{N}_1|$ ($\aleph_0 + 1 = \aleph_0$) since $f: \mathbb{N}_0 \rightarrow \mathbb{N}_1, x \mapsto x + 1$ is a bijection. Transfinite arithmetic is not the same as finite arithmetic. The rational numbers are countable $|\mathbb{Q}| = \aleph_0$.

If the number of gaps $|\mathbb{R} \setminus \mathbb{Q}|$ is countable we could combine them with the rational numbers into an enumeration for \mathbb{R} .

Assume there exists an enumeration of real numbers in $(0,1)$: x_1, x_2, x_3, \dots

$$x_i = 0. d_{i1} d_{i2} \dots \text{ with } d_{ij} \in \{0,1, \dots, 9\}.$$

$$x_1 = 0. d_{11} d_{12} \dots$$

$$x_2 = 0. d_{21} d_{22} \dots$$

$$\vdots \quad \quad \quad \vdots$$

$$x_\omega = 0. d_1 d_2 \dots \text{ with } d_i = \begin{cases} 1 & \text{if } d_{ii} = 2 \\ 2 & \text{if } d_{ii} \neq 2 \end{cases}$$

$x_\omega \in (0,1)$ has a unique representation and it is not in the list \Rightarrow

$\{x \in \mathbb{R} | 0 < x < 1\}$ is not countable \Rightarrow

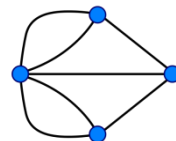
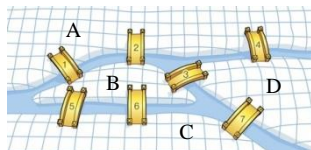
$$|\mathbb{R}| \geq |(0,1)| > \aleph_0$$

This proof uses Cantor’s diagonal argument. The cardinal number of the continuum is denoted by c . Cantor proved that every cardinal number has a next-larger cardinal: $\aleph_0, \aleph_1, \aleph_2, \dots$. The assumption that there is no set with a size between \mathbb{N} and \mathbb{R} is known as the continuum hypothesis, $c = \aleph_1$.

3.4 Discrete mathematics

Discrete in this context, not to be confused with discreet is the opposite of continuous. Discrete mathematics is an umbrella term for diverse fields of mathematics with a focus on discrete properties. The archetypal discrete set is the set of integers, discrete mathematics deals with countable sets. Things excluded could be called “continuous mathematics” based on quantities that vary continuously. Branches of mathematics with much discrete content are computer science, combinatorics, cryptology, graph theory, number theory, algebra and analysis when it is based on intervals or discrete time steps.

Two typical problems belonging to discrete mathematics would be, “What is the probability that two students in a class of 30 have the same birthday?” or “Is it possible to make a roundtrip in the city of Königsberg with seven bridges and visit every district and cross each bridge exactly once?”.



The first problem is handled in the field of combinatorics and the latter problem is dealt with in graph theory.

3.4.1 Combinatorics

Combinatorics is often about counting; how many ways to form a certain pattern, forming permutations, selecting items from a collection or partitioning a set according to some criteria. In combinatorial optimization the goal is to find the best solution from a finite set of possibilities, like the travelling salesman problem. Combinatorial problems arise in every field of mathematics, not least in algebra, probability, topology and geometry.

The birthday problem needs clarification. No twins, each student’s birthday probability distribution is independent of the others and spread equally over 365 days. The number of combinations $\#(DD)$ with every birthday on different days and the total number of combinations $\#(T)$ are:

$$\#(DD) = \underbrace{365 \cdot 364 \cdot \dots \cdot (365 - (30 - 1))}_{30 \text{ factors}} = \frac{365!}{335!} \quad \#(T) = 365^{30}$$

$$P(\text{some have the same birthday}) = 1 - \frac{365!}{335! \cdot 365^{30}} \approx 70\%$$

$365!$ is too big for most calculators, Stirling’s approximation of $n!$ gives:

$$n! \sim \sqrt{2\pi n} \left(\frac{n}{e}\right)^n \rightarrow \log(n!) \sim \frac{\log(2\pi n)}{2} + n \log\left(\frac{n}{e}\right) \rightarrow 365! \sim 10^{778}$$

Expressions like $\#(DD)$ to count sequences without repetition are often given on calculators with symbols like $P(n, k)$, nPk or something similar. An alternative and more telling notation is falling and rising factorials.

$$n^{\underline{k}} \equiv \underbrace{n(n-1) \dots (n-k+1)}_{k \text{ factors}} \quad (\text{Pronounced “}n \text{ to the } k \text{ falling”})$$

$$n^{\overline{k}} \equiv \underbrace{n(n+1) \dots (n+k-1)}_{k \text{ factors}} \quad (\text{Pronounced “}n \text{ to the } k \text{ rising”})$$

The number of injective functions $f: A \rightarrow B$ with $|A| = n, |B| = k$ is n^k . A sequence of length n (without repetitions) from a set of n objects is a permutation (reordering). The number of ways to pick k objects (no order) from n objects, $\#\{A \subseteq S | \#S = n \wedge \#A = k\}$ is:

$$\frac{n^k}{k!} = \frac{n!}{(n-k)!k!} \equiv \binom{n}{k} \text{ (Pronounced "n choose k")}$$

Another symbol often seen on calculators is $C(n, k)$ or nCk . Integers of this type are called binomial coefficients since it is the number of ways to pick a term with k x 's from the expansion of $(x + y)^n = \underbrace{(x + y) \cdots (x + y)}_{n \text{ factors}}$.

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

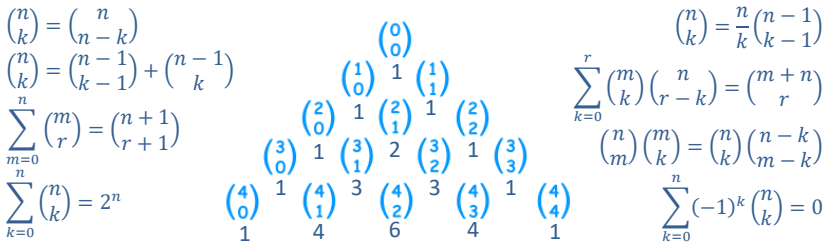


Fig 3.4.1 Pascals triangle with binomial coefficients and some of their identities.

The binomial theorem has a multinomial version with multinomial coefficients:

$$(x_1 + x_2 + \dots + x_m)^n = \sum_{k_1 + \dots + k_m = n} \binom{n}{k_1, k_2, \dots, k_m} x_1^{k_1} x_2^{k_2} \dots x_m^{k_m}$$

$$\binom{a_1 + a_2 + \dots + a_m}{a_1, a_2, \dots, a_m} \equiv \frac{(a_1 + a_2 + \dots + a_m)!}{a_1! a_2! \dots a_m!}$$

The laws $x^m x^n = x^{m+n}$, $x^m / x^n = x^{m-n}$ and $(x^m)^n = x^{mn}$ for positive integers makes it natural to introduce $x^0 \equiv 1$ and $x^{-n} \equiv 1/x^n$ to extend the laws to all integers. The simplest case of a law is often interesting as a start in an inductive proof or recursive definition. Conventions should be chosen to reflect that. For the factorial this means $0! \equiv 1$. Another way to see this:

One way to pick all objects $1 = \binom{n}{n} = \frac{n!}{n! \cdot 0!} \rightarrow 0! = 1$

In "continuous mathematics" the factorial has a natural extension in the gamma function $z! = \Gamma(z + 1)$ which is defined for all $z \in \mathbb{C} \setminus \mathbb{Z}^-$.

For 0^0 there appear to be two incompatible choices $x^0 \rightarrow 1$ and $0^x \rightarrow 0$ but $f(x) = 0^x$ is not very important and combinatorial arguments are more fundamental to decide the value of 0^0 : ($x^x \rightarrow 1$ as $x \rightarrow 0$)

$$(1 + 0)^0 = \sum_{\substack{k_1+k_2=0 \\ k_i \geq 0}} \binom{0}{k_1, k_2} 1^{k_1} 0^{k_2} = \binom{0}{0} \cdot 1^0 \cdot 0^0 \rightarrow 0^0 \equiv 1$$

$$\binom{0}{0} = \frac{0!}{0! \cdot 0!} = 1. \text{ There is one subset of } \emptyset \text{ (} \emptyset \subseteq \emptyset \text{)}.$$

The most natural definitions for sums and products of zero elements are:

$$\sum_{i \in \emptyset} a_i \equiv 0 \quad \text{additive identity} \qquad \prod_{i \in \emptyset} a_i \equiv 1 \quad \text{multiplicative identity}$$

Binomial coefficients have two cousins called Stirling numbers of the first and second kind, $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ and $\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$. The second kind is the most common. They can be defined in combinatorial, functional or algebraic terms:

$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is the number of ways to put n different balls in k equal boxes with no empty box or the number of ways to partition a set of n elements into k non-empty subsets. The symbol can be read “ n subset k ”.

$n! \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\}$ is the number of surjective $f: A \rightarrow B$ with $|A| = n$ and $|B| = k$.

$$\left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \frac{1}{k!} \sum_{j=0}^k (-1)^{k-j} \binom{k}{j} j^n$$

Stirling numbers of the first kind $\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right]$ is the number ways to arrange n objects into k non-empty cycles. The symbol can be read “ n cycle k ”. A cycle like $A \rightarrow B \rightarrow C \rightarrow D$ can be written in 4 different ways $[A, B, C, D] = [B, C, D, A] = [C, D, A, B] = [D, A, B, C]$. Example, $\left[\begin{smallmatrix} 4 \\ 2 \end{smallmatrix} \right] = 11$ with cycles:

$$\begin{matrix} [1,2,3] + [4] & [1,2,4] + [3] & [1,3,4] + [2] & [2,3,4] + [1] & [1,2] + [3,4] \\ [1,3,2] + [4] & [1,4,2] + [3] & [1,4,3] + [2] & [2,4,3] + [1] & [1,3] + [2,4] \\ & & & & [1,4] + [2,3] \end{matrix}$$

$$\begin{matrix} \downarrow n & & & & \swarrow k \\ & 1 & 1 & & \\ & 1 & 3 & 1 & \\ & 1 & 7 & 6 & 1 \\ 1 & 15 & 25 & 10 & 1 \end{matrix} \quad \left\{ \begin{smallmatrix} n \\ k \end{smallmatrix} \right\} = \left\{ \begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right\} + k \left\{ \begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right\}$$

$$\left[\begin{smallmatrix} n \\ k \end{smallmatrix} \right] = \left[\begin{smallmatrix} n-1 \\ k-1 \end{smallmatrix} \right] + (n-1) \left[\begin{smallmatrix} n-1 \\ k \end{smallmatrix} \right]$$

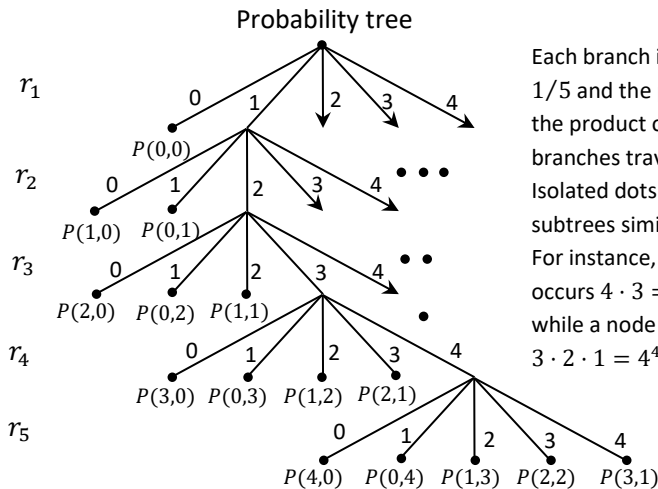
$$\begin{matrix} \downarrow n \cdot & & & & \swarrow k \\ & 1 & 1 & & \\ & 2 & 3 & 1 & \\ & 6 & 11 & 6 & 1 \\ 24 & 50 & 35 & 10 & 1 \end{matrix}$$

3.4.2 Simplified model of decimal expansion

Let r_1, r_2, \dots be a sequence of integers, $r_k \in \{0, 1, \dots, q - 1\}$ for some $q \in \mathbb{Z}^+$, just like the rests that appear in the long division algorithm on page 3. Each new r_k will be chosen independently of the others with uniform probability distribution. The sequence is stopped as soon as r_k becomes zero $r_1, r_2, \dots, r_i, 0$ or if r_k occurs earlier in the sequence

$$\underbrace{r_1, r_2, \dots, r_i}_{i \text{ digits}}, \underbrace{r_{i+1}, \dots, r_{i+j}}_{j \text{ digits}}, r_{i+j+1} = r_{i+1}.$$

Example: $q = 5$ with $P(i, j)$ the probability of i “pre-period digits” and j “repeating digits”.



Each branch is chosen with probability $1/5$ and the probability of a node is the product of the probabilities in the branches traversed to reach the node. Isolated dots represent repetitions of subtrees similar to previous subtree. For instance, a node of type $P(0,2)$ occurs $4 \cdot 3 = 4^2$ times in the tree while a node of type $P(1,3)$ occurs $4 \cdot 3 \cdot 2 \cdot 1 = 4^4 = 4!$ times.

\square	$P(0,0) = \frac{1}{5}$	$P(0,1) = \frac{4}{5^2}$	$P(0,2) = \frac{4^2}{5^3}$	$P(0,3) = \frac{4^3}{5^4}$	$P(0,4) = \frac{4^4}{5^5}$
$\tilde{P}(0)$	$P(1,0) = \frac{4}{5^2}$	$P(1,1) = \frac{4^2}{5^3}$	$P(1,2) = \frac{4^3}{5^4}$	$P(1,3) = \frac{4^4}{5^5}$	\square
$\tilde{P}(1)$	$P(2,0) = \frac{4^2}{5^3}$	$P(2,1) = \frac{4^3}{5^4}$	$P(2,2) = \frac{4^4}{5^5}$	\square	\square
$\tilde{P}(2)$	$P(3,0) = \frac{4^3}{5^4}$	$P(3,1) = \frac{4^4}{5^5}$	\square	\square	\square
$\tilde{P}(3)$	$P(4,0) = \frac{4^4}{5^5}$	\square	\square	\square	\square
$\tilde{P}(4)$	\square	\square	\square	\square	\square

$$P(q, i, j) = \frac{(q - 1)^{i+j}}{q^{i+j+1}}$$

$$i \geq 0, j \geq 0, 0 \leq i + j < q$$

The probability for $n = i + j$ digits in the sequence r_1, \dots, r_n is:

$$\tilde{P}(q, n) = (n + 1) \frac{(q-1)^n}{q^{n+1}} \text{ with } 0 \leq n < q$$

The sum of probabilities in the nodes of a subtree equals the probability of the branch it is attached to. As a result:

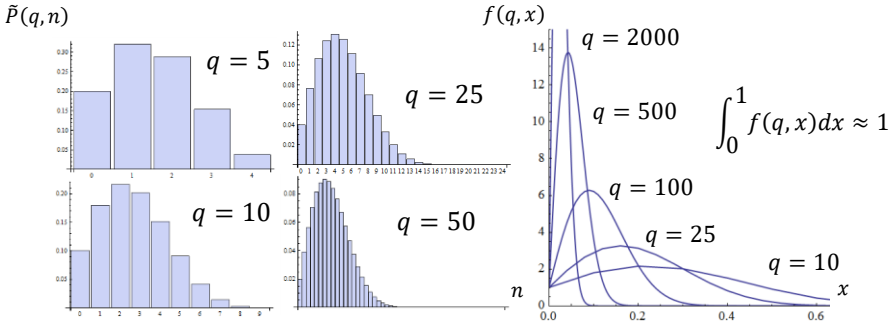
$$\sum_{n=0}^{q-1} (n + 1) \frac{(q-1)^n}{q^{n+1}} = 1$$


Fig 3.4.2 Probability distributions.

The likelihood of different number of digits in the sequence is shown above with probability mass functions (PMF) for various q . As q grows they approach a certain form that can be illustrated by probability densities $\tilde{P}(q, n)/(1/q)$. They are sampled and rescaled $n \sim xq$ with $0 \leq x < 1$ to fit in the same diagram as if they were probability density functions (PDF).

The model does not fit the properties of decimal expansions from page six.

$$\frac{p}{q} = \frac{100\,000}{101\,001} = 0.\overline{990089207 \dots 099900000}$$

16 640 digits

$q = 101001 \neq 2^m 5^n \Rightarrow$ no repeating digits but the probability for this in the model is $\text{Sum}[P(q, i, 0), \{i, 0, q - 1\}]$ which is less than 4%. The same low probability in the model applies for p/q having no pre-periodic digits $\text{Sum}[P(q, 0, j), \{j, 0, q - 1\}] < 4\%$ but p/q has no pre-periodic digits.

The model also predicts that it is highly unlikely to get long sequences. $\tilde{P}(q, 10\,000) \approx 10^{-224}$ and $\tilde{P}(q, 20\,000) \approx 10^{-924}$ so the probability that p/q should need more than 10% of the maximal number of digits in the decimal expansion $\text{Sum}[\tilde{P}(q, n), \{n, 0.1q, q - 1\}]$ is miniscule whereas p/q in fact has 16 640 repeating digits, just 16% less than the maximal number. The numbers p and q were chosen to get long periods, but long periods are not as exceptional as the model predicts. The period of decimal expansions will be analyzed further when we get to number theory.

3.4.3 Sequences, Recursion and Difference equations

Definition 1. A **sequence** is a function $f: \mathbb{N}_0 \rightarrow S$ with $S = \mathbb{Z}, \mathbb{R}, \mathbb{C}$ or some other set. It can be written as:

$$\hat{\mathbf{a}} = \langle a_0, a_1, \dots \rangle \text{ or } \hat{\mathbf{a}} = \langle a_n \rangle \text{ with } a_n = \hat{\mathbf{a}}(n)$$

Examples are the arithmetic sequence where each element is the arithmetic mean of its neighbors, $\hat{\mathbf{a}} = \langle x + ny \rangle = \langle x, x + y, x + 2y, \dots \rangle$ and the geometric sequence where each element is the geometric mean of its neighbors, $\hat{\mathbf{g}} = \langle xy^n \rangle = \langle x, xy, xy^2, \dots \rangle$. Sequences are often defined recursively:

$$\hat{\mathbf{a}} - \begin{cases} a_k = a_{k-1} + y \\ a_0 = x \end{cases} \quad \hat{\mathbf{g}} - \begin{cases} g_k = yg_{k-1} \\ g_0 = x \end{cases} \quad \hat{\mathbf{x}} - \begin{cases} x_k = rx_{k-1}(1 - x_{k-1}) \\ x_0 = x_0 \text{ (logistic map)} \end{cases}$$

Natural operations on sequences are addition $\hat{\mathbf{x}} + \hat{\mathbf{y}} = \langle x_n + y_n \rangle$, multiplication by a constant $a\hat{\mathbf{x}} = \langle ax_n \rangle$. The partial sums of a sequence $\langle a_n \rangle$ is:

$$\langle s_n \rangle \text{ with } s_n = a_0 + a_1 + \dots + a_n \text{ (} n + 1 \text{ terms)} \quad \begin{cases} s_n = s_{n-1} + a_n \\ s_0 = a_0 \end{cases}$$

$$\hat{\mathbf{a}}: s_n = \sum_{k=0}^n x + ky = x(n + 1) + y \frac{n(n + 1)}{2} = (n + 1) \left(\frac{a_0 + a_n}{2} \right)$$

$$\hat{\mathbf{g}}: s_n = \sum_{k=0}^n xy^k = \frac{x}{1 - y} (1 - y)(1 + \dots + y^n) = x \frac{1 - y^{n+1}}{1 - y}$$

Closed formulas for s_n are exceptions, upper and lower bonds based on integrations or approximations are what you can expect in the general case.

A **recurrence relation** $x_n = f(x_{n-1}, n)$ with $n = 1, 2, \dots$ and initial value x_0 can be seen as an equation to be solved. Iterated calculations might be the fastest way for computation but a closed formula $x_n = g(x_0, n)$ can reveal other properties like the asymptotic behavior of the sequence. Equations of this type are often called **difference equations**. They are the counterpart of differential equations in continuous mathematics.

Theorem 1. A difference equation $x_n = f(x_{n-1}, n)$ has a unique solution $\hat{\mathbf{x}}$ for every initial value $x_0 = b$ with x_k in the codomain of f .

Proof. $x_0 = b$ gives a unique value to $x_1 = f(b, 1) = c$ which gives a unique value to $x_2 = f(c, 2) = d$ which gives a unique value to x_3 etc.

Differential equations has a corresponding theorem on unique solutions. Its proof is less obvious.

The name “difference equation” for recurrence relations is based on the difference operator $\Delta(\langle x_n \rangle) = \langle x_{n+1} - x_n \rangle$, $n = 0, 1, \dots$. Other operators on sequences that are useful are:

- $I\langle x_n \rangle \equiv \langle x_n \rangle$ Identity operator
- $E\langle x_n \rangle \equiv \langle x_{n+1} \rangle$ Forward shift operator
- $E^k\langle x_n \rangle \equiv \langle x_{n+k} \rangle$ k steps forward
- $\Delta\langle x_n \rangle \equiv \langle x_{n+1} - x_n \rangle$ Forward difference operator
- $\Delta^k\langle x_n \rangle \equiv \Delta(\Delta^{k-1}\langle x_n \rangle)$ k^{th} forward difference
- $\nabla\langle x_n \rangle \equiv \langle x_n - x_{n-1} \rangle$ Backward difference $n = 1, 2, \dots$
- $E = I + \Delta$ Operator identity

$$E^k = (I + \Delta)^k = \sum_{i=0}^k \binom{k}{i} \Delta^i \rightarrow x_{n+k} = \binom{k}{0} x_n + \binom{k}{1} \Delta x_n + \dots + \binom{k}{k} \Delta^k x_n$$

$$\Delta^k = (E - I)^k$$

Any recurrence relation with $x_n, x_{n+1}, \dots, x_{n+k}$ can be expressed with x_n and $\Delta, \Delta^2, \dots, \Delta^k$. $3x_{n+2} - 4x_{n+1} + 8x_n = 0 \rightsquigarrow 3\Delta^2 x_n + 2\Delta x_n + 7x_n = 0$. Difference equations and differential equations share many properties. The parallel extends to partial differential equations with one-dimensional sequences replaced by multi-dimensional grids.

A difference equation like $x_n = \alpha x_{n-1} + \beta x_{n-2} + \gamma$ needs two initial values $x_0 = b_0$ and $x_1 = b_1$ to give a unique sequence. The **order** of a difference equation equals the difference between the highest and lowest occurring index of the sequence-variable. The order corresponds to the number of initial values needed.

Definition 2. A difference equation is called **linear** if it can be written as $\mathcal{L}(\hat{x}) = \hat{h}$ with an operator \mathcal{L} that satisfies the criteria of a linear operator:

$$\begin{aligned} \mathcal{L}(\hat{a} + \hat{b}) &= \mathcal{L}(\hat{a}) + \mathcal{L}(\hat{b}) \\ \mathcal{L}(\alpha \hat{a}) &= \alpha \mathcal{L}(\hat{a}) \end{aligned}$$

If $\hat{h} = \langle h_n \rangle = \langle 0 \rangle$ then $\mathcal{L}(\hat{x}) = \mathbf{0}$ is called a **homogenous** equation.

Example: $x_n + p_n x_{n-1} + q_n x_{n-2} = h_n$ is a linear 2nd order inhomogenous difference equation. It's linear in $\hat{x} = \alpha \hat{x}_1 + \beta \hat{x}_2$ even though p_n, q_n and h_n may be non-linear functions of n . For a linear operator \mathcal{L} the following theorem is quite obvious.

Theorem 2. If \hat{y} solves $\mathcal{L}(\hat{x}) = \hat{g}$ and \hat{z} solves $\mathcal{L}(\hat{x}) = \hat{h}$ then $\hat{x} = \hat{y} + \hat{z}$ solves $\mathcal{L}(\hat{x}) = \hat{g} + \hat{h}$.

The general solution to $\mathcal{L}(\hat{x}) = \hat{g}$ reduces to finding the general solution \hat{x}_h to the homogenous equation $\mathcal{L}(\hat{x}) = \mathbf{0}$ and one particular solution \hat{x}_p to $\mathcal{L}(\hat{x}) = \hat{g}$ since $\hat{x} = \hat{x}_p + \hat{x}_h = \hat{x}'_p + \underbrace{\hat{x}_p - \hat{x}'_p + \hat{x}_h}_{\text{solves } \mathcal{L}(\hat{x})=0}$.

The first step to find a closed form solution is to look at first order homogenous linear difference equations with a constant coefficient:

$$x_n - rx_{n-1} = 0, n \in \mathbb{N}_1 \rightarrow x_n = r^n x_0, n \in \mathbb{N}_0 \rightarrow \hat{x} = C \langle r^n \rangle$$

It's a geometric sequence with constant C determined by the initial value x_0 . Trying $x_n = Cr^n$ on $x_n + px_{n-1} + qx_{n-2} = 0$ leads to $r^2 + pr + q = 0$ with roots r_1 and r_2 . If $r_1 \neq r_2$ the solution will be $x_n = C_1 r_1^n + C_2 r_2^n$ with constants C_1 and C_2 determined uniquely by x_0 and x_1 .

$$\begin{cases} x_n - 2x_{n-1} + 2x_{n-2} = 0 \\ x_0 = 1 \rightarrow r^2 - 2r + 2 = 0 \rightarrow r = 1 \pm i \rightarrow \\ x_1 = 2 \end{cases}$$

$$x_n = C_1(1+i)^n + C_2(1-i)^n \quad \begin{cases} x_0 = 1 \\ x_1 = 2 \end{cases} \rightarrow \begin{cases} C_1 = (1-i)/2 = 2^{-1/2} e^{-\frac{\pi}{4}} \\ C_2 = (1+i)/2 = 2^{-1/2} e^{+\frac{\pi}{4}} \end{cases}$$

In polar form: $x_n = 2^{n/2} \left(\cos \frac{n\pi}{4} + \sin \frac{n\pi}{4} \right) = 2^{(n+1)/2} \sin \frac{(n+1)\pi}{4}$

A linear homogenous equation of order k with constant coefficients p_i

$$(*) \quad x_n + p_1 x_{n-1} + p_2 x_{n-2} + \dots + p_k x_{n-k} = 0$$

is associated with an equation called the **characteristic equation**

$$(**) \quad r^k + p_1 r^{k-1} + p_2 r^{k-2} + \dots + p_{k-1} r + p_k = 0$$

The general solution to (*) is a direct parallell to the differential equations where $x_n, x_{n-1}, x_{n-2}, \dots$ are replaced with $x(t), x'(t), x''(t), \dots$.

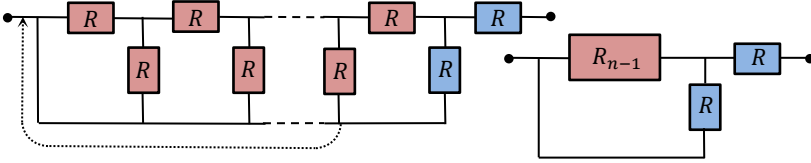
Theorem 3. Let r_1, r_2, \dots, r_t be the distinct solutions to the characteristic equation (**) with multiplicities $m_1, m_2, \dots, m_t, (m_1 + m_2 + \dots + m_t = k)$. The general solution to (*) is given by:

$$\hat{x} = \sum_{i=1}^t \sum_{j=0}^{m_i-1} A_{ij} \langle n^j r_i^n \rangle$$

With k constants $A_{ij} \in \mathbb{C}$, uniquely determined by x_0, x_1, \dots, x_{k-1} .

The proof is the same as for differential equations, I will not give it here. The treatment of inhomogenous difference equations $\mathcal{L}(\hat{x}) = \langle h(n) \rangle$ with $h(n)$ a polynomial, exponential, or trigonometric function is also an exact parallell to differential equations. Finding a particular solution to the in-homogenous linear equation with constant coefficients will be handled later together with differential equations.

A difference equation can just as a differential equation occur as a system of equations. An example of this is the resulting resistance in the following circuit diagram with $2n + 1$ resistors and total resistance R_n .



The second diagram is a parallel coupling followed by a serial coupling.

$$R_n = (R_{n-1}^{-1} + R^{-1})^{-1} + R \quad x_n = R_n/R \rightarrow \begin{cases} x_n = \frac{2x_{n-1}+1}{x_{n-1}+1} (*) \\ x_0 = 1 \end{cases}$$

$x_0 \in \mathbb{Q} \wedge (x_k \in \mathbb{Q} \Rightarrow x_{k+1} \in \mathbb{Q})$. Let $x_n = p_n/q_n$ with $p_n, q_n \in \mathbb{Z}^+$.

$$\frac{p_n}{q_n} = \frac{2p_{n-1}+q_{n-1}}{p_{n-1}+q_{n-1}} \text{ with } \begin{cases} p_0 = 1 \\ q_0 = 1 \end{cases} \rightarrow \begin{pmatrix} p_n \\ q_n \end{pmatrix} \equiv \mathbf{p}_n = \mathbf{A}\mathbf{p}_{n-1} \text{ with } \mathbf{A} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

The non-linear equation (*) has become linear with solution $\mathbf{p}_n = \mathbf{A}^n \mathbf{p}_0$. The matrix \mathbf{A} is diagonalizable which means that there is an invertible matrix \mathbf{S} and a matrix \mathbf{D} that is diagonal.

$$\mathbf{A} = \mathbf{S}\mathbf{D}\mathbf{S}^{-1} \rightarrow \mathbf{A}^n = \mathbf{S}\mathbf{D}^n\mathbf{S}^{-1} \quad \mathbf{D} = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \rightarrow \mathbf{D}^n = \begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix}$$

Matrices and diagonalization are part of linear algebra covered in chapter 5. λ_1 and λ_2 are roots of the characteristic equation $|\mathbf{A} - \lambda\mathbf{I}| = 0$. \mathbf{S} is found by calculating eigenvectors to the roots. The result is:

$$\lambda = \frac{3 \pm \sqrt{5}}{2} \rightarrow x_n = \frac{\lambda_1^{n+1} - \lambda_2^{n+1}}{\varphi\lambda_1^n - \hat{\varphi}\lambda_2^n} \quad \begin{cases} \varphi = (1 + \sqrt{5})/2 \\ \hat{\varphi} = (1 - \sqrt{5})/2 \end{cases}$$

$$\frac{R_\infty}{R} = \lim_{n \rightarrow \infty} x_n = \varphi = 1.618 \dots \quad \left(\begin{array}{l} \varphi = (1 + \sqrt{5})/2 \\ \text{The golden section} \end{array} \right)$$

Non-linear equations like the logistic map $x_k = rx_{k-1}(1 - x_{k-1})$ have the potential for very complex and dynamical behavior. We will study them in a later chapter that deals with non-linearity and chaos theory.

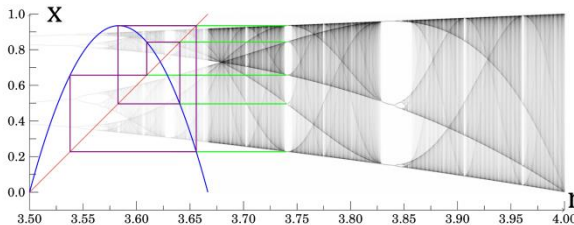


Fig. 3.4.3 The logistic map, cobweb diagram and limits of x_k versus r .

3.4.4 Generating functions

Generating functions is a holistic approach to sequences $\hat{g} = \langle g_n \rangle$ where the numbers g_n are treated as coefficients of z^n in a formal power series:

$$G(z) = \sum_{n=0}^{\infty} g_n z^n = \sum_{n \in \mathbb{Z}} g_n z^n \text{ (if } g_n \text{ is set to zero for } n < 0 \text{)}$$

$G(z)$ is called the generating function for \hat{g} but is not really a function with domain and codomain. Convergence does not matter, z is more of a formal symbol with algebraic properties resembling a real or complex variable.

Generating functions (GF) can also be given for a multi-dimensional array of numbers $G(x, y) = \sum_{m,n} g_{m,n} x^m y^n$. A notation for retrieving coefficients is $[x^m y^n]G(x, y) \equiv g_{m,n}$. GFs can be operated on in some obvious ways.

$\alpha F(z) + \beta G(z) = \sum_n (\alpha f_n + \beta g_n) z^n$	GF of $\hat{f} + \hat{g}$
$z^m G(z) = \sum_n g_{n-m} z^n$	Right shift of \hat{g} , m steps
$z^{-m}(G(z) - g_0 - \dots - g_{n-1} z^{n-1})$	Left shift of \hat{g} , m steps
$G(cz) = \sum_n c^n g_n z^n$	GF of $\langle c^n g_n \rangle$
$G'(z) = \sum_n (n+1) g_{n+1} z^n$	$zG'(z)$ GF of $\langle n g_n \rangle$
$\int_0^z G(t) dt = \sum_{n \geq 1} n^{-1} g_{n-1} z^n$	$D^{-1} \hat{g} = g_0 z + g_1 z^2 / 2 + \dots$
$H(z) = F(z)G(z) = \sum_{n,k} f_k g_{n-k} z^n$	$(f_0 + f_1 z + \dots)(g_0 + g_1 z + \dots) = f_0 g_0 + (f_0 g_1 + f_1 g_0) z + \dots$

The sequence $\hat{h} = \langle h_n \rangle = \langle \sum_k f_k g_{n-k} \rangle = \hat{f} \star \hat{g}$ that is characterized by $H(z) = F(z)G(z)$ is called the **convolution** of \hat{f} and \hat{g} . Convolution is commutative, associative and extends naturally $\hat{f} \star \hat{g} \star \hat{h} = \langle \sum_{i+j+k=n} f_i g_j h_k \rangle$

The Fibonacci sequence $\hat{f} = \langle 0, 1, 1, 2, 3, 5, 8, 11, \dots \rangle$ is defined recursively by $f_n = f_{n-1} + f_{n-2}$, $f_0 = 0$, $f_1 = 1$ and in close form by $f_n = (\varphi^n - \hat{\varphi}^n) / \sqrt{5}$. Generating functions can sometimes be expressed in closed form. For the Fibonacci sequence $F(z) = \sum_n f_n z^n = z / (1 - z - z^2)$. The closed form representations of infinite sequences of numbers is the reason for calling GF a holistic approach. All numbers in the sequence are integrated into one package. One starting point for assigning closed forms to power series' is:

$$1 + z + z^2 + \dots = \frac{1}{1 - z} \text{ (} 1 - z \text{)(} 1 + z + z^2 + \dots + z^\omega \text{) and 1 have the same coefficients for all finite powers.}$$

Closed forms of GFs and operations on closed forms can be formalized in a strict and logically sound way. Without doing this I will present some sequences and their closed form GFs. The notation $[P(x_1, \dots, x_n)]$ with n -ary predicate function P has value 1 when true and 0 otherwise, e.g. $[m=n]=\delta_{m,n}$.

Sequence	GF	Closed form
$\langle 0, \dots, 0, 1, 0, \dots \rangle$	$\sum_{n \geq 0} [n = m] z^n$	z^m
$\langle 1, -1, 1, -1 \dots \rangle$	$\sum_{n \geq 0} (-1)^n z^n$	$1/(1 + z)$
$\langle 1, 0, 1, 0 \dots \rangle$	$\sum_{n \geq 0} [2 n] z^n = \sum_n z^{2n}$	$1/(1 - z^2)$
$\langle 1, 2, 3, \dots \rangle$	$\sum_{n \geq 0} (n + 1) z^n$	$1/(1 - z)^2$

The cumulative sum of a sequence $\langle g_n \rangle$, given by $\langle g_0, g_0 + g_1, \dots \rangle$ has GF given by $(1 - z)^{-1}G(z)$ since $1/(1 - z) = 1 + z + z^2 + \dots$ and

$$\frac{1}{1 - z} G(z) = \sum_{n, k} 1_k g_{n-k} z^n = \sum_n \underbrace{\left(\sum_k g_{n-k} \right)}_{g_0 + \dots + g_n} z^n$$

$\hat{g} = \langle 1, 1, \dots \rangle$ gives the GF $(1 - z)^{-2}$ for the sequence $\langle 1, 2, 3, \dots \rangle$.

Sequence	GF	Closed form
$\langle 1, m, \binom{m}{2}, \dots, \binom{m}{m}, 0 \dots \rangle$	$\sum_{n \geq 0} \binom{m}{n} z^n$	$(1 + z)^m$
$\langle 1, c, c^2, c^3, \dots \rangle$	$\sum_{n \geq 0} c^n z^n$	$1/(1 - cz)$
$\langle 0, 1, \frac{1}{2}, \frac{1}{3}, \dots \rangle$	$\sum_{n \geq 0} \frac{1}{n} z^n$	$\ln \frac{1}{1 - z}$
$\langle 1, 1, \frac{1}{2}, \frac{1}{3!}, \frac{1}{4!}, \dots \rangle$	$\sum_{n \geq 0} \frac{1}{n!} z^n$	e^z

Derivation and integration is another way to get a GF.

$$\hat{f} = 1 + z + z^2 + \dots$$

$$\text{GF: } (1 - z)^{-1}$$

$$D\hat{f} = 1 + 2z + 3z^2 + \dots$$

$$\text{GF: } F(z) = D(1 - z)^{-1} = (1 - z)^{-2}$$

$$\hat{g} = 1 + z + z^2/2! + z^3/3! \dots \quad \text{GF: } G(z)$$

$$D\hat{g} = 1 + z + z^2/2! + \dots$$

$$\text{GF: } DG(z) = G(z) \rightarrow G(z) = e^z$$

$$\hat{h} = z + 2^{-1}z^2 + 3^{-1}z^3 + \dots \quad \hat{h} = \langle 0, 1, 2^{-1}, 3^{-1}, \dots \rangle$$

$$\hat{h} = \int_0^z (1 + t + t^2 \dots) dt$$

$$\text{GF: } H(z) = \int_0^z (1 - t)^{-1} dt = \ln(1 - z)^{-1}$$

To go from GF to a sequence of numbers, use the Maclaurin series.

$$F(z) = \sum_{n=0}^{\infty} \frac{F^{(n)}(0)}{n!} z^n$$

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k \quad \alpha \in \mathbb{R} \quad \text{with} \quad \binom{\alpha}{k} \equiv \frac{\alpha(\alpha-1)\dots(\alpha-k+1)}{k!}$$

$$\text{When } \alpha \in \mathbb{Z}^- \quad \binom{-n}{k} = (-1)^k \binom{n+k-1}{k} \rightarrow \frac{1}{(1+x)} = \sum_{k=0}^{\infty} (-x)^k$$

Another way to get from GF to numbers is by partial decomposition of a rational function. Let's look at the Fibonacci sequence $\langle 0,1,1,2,3,5,8, \dots \rangle$:

$$F_n = F_{n-1} + F_{n-2} + [n = 1] \quad (F_n = 0 \text{ for } n < 0) \rightarrow$$

$$\begin{aligned} G(z) &= \sum_n F_n z^n = \sum_n F_{n-1} z^n + \sum_n F_{n-2} z^n + \sum_n [n = 1] z^n \\ &= zG(z) + z^2 G(z) + z \rightarrow G(z) = \frac{z}{1-z-z^2} \end{aligned}$$

The Fibonacci numbers $F_n = [z^n] \frac{z}{1-z-z^2}$, can be retrieved by a partial fraction decomposition of $R(z) = P(z)/Q(z)$ with $Q(z) = 1 - z - z^2$ and $P(z) = z$. Partial fraction decomposition with quotient and remainder polynomials will be described in the algebra section but since $Q(z)$ is a polynomial over \mathbb{C} its irreducible polynomials will be of degree one.

Theorem 4. Partial fraction decomposition

Let f and g be nonzero polynomials over a field \mathbb{F} with $g = \prod_{i=1}^k p_i^{n_i}$, a product of powers of distinct irreducible polynomials.

There are unique polynomials q and r_{ij} with $\deg r_{ij} < \deg p_i$ s.t.

$$\frac{f}{g} = q + \sum_{i=1}^k \sum_{j=1}^{n_i} \frac{r_{ij}}{p_i^j} \quad \deg f < \deg g \Rightarrow q = 0$$

$$R(z) = \frac{\alpha_1}{z-\rho_1} + \frac{\alpha_2}{z-\rho_2} = \frac{-\alpha_1/\rho_1}{1-z/\rho_1} + \frac{-\alpha_2/\rho_2}{1-z/\rho_2} \rightarrow \langle f_n \rangle = -\frac{\alpha_1}{\rho_1} \langle \rho_1^{-n} \rangle - \frac{\alpha_2}{\rho_2} \langle \rho_2^{-n} \rangle$$

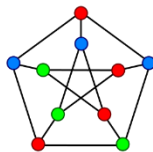
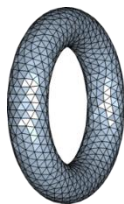
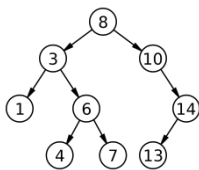
$$R(z) = \frac{z}{1-z-z^2} \rightarrow F_n = \frac{\varphi^n - \hat{\varphi}^n}{\sqrt{5}} \quad \text{with} \quad \begin{cases} \varphi = (1 + \sqrt{5})/2 \\ \hat{\varphi} = (1 - \sqrt{5})/2 \end{cases}$$

A few more examples on generating functions are presented in appendix C.

3.4.5 Graph theory

Graph theory deals with a well-defined class of formalized diagrams that capture the essential properties of issues that occur in many fields of science, not least computer science and algorithms. Some examples:

- Tree structures for sorting and searching.
- Networks for all types of infrastructure, such as IT/information and transport. A typical problem here is the travelling salesman problem of how to find the shortest path that passes given cities.
- Geometry, topology and knot theory.
- The four color problem, a classical example of a problem involving various ways of coloring graphs. Is four colors enough to color a map?



Definitions

An **undirected graph** $G = (V, E)$ is a set of **vertices** (nodes)

$V = \{V_1, V_2, \dots, V_n\} \neq \emptyset$ and a set of **edges** $E = \{\{x, y\} | x, y \in V \dots\}$.

An edge connecting a with b is denoted ab , loops with $a = b$ are allowed.

A graph with several edges between two vertices is called a **multigraph**.

A **simple graph** has no multiple edges or loops.

The **complete graph**, K_n is a simple graph that connects all n nodes.

A **directed graph** $G = (V, E)$ has directed edges $E = \{(x, y) | x, y \in V \dots\}$.

Edge $e = \{a, b\}$ is **incident** with nodes a and b that are **adjacent**.

The **order of a graph** is the number of vertices, $|V|$.

The **size of a graph** is the number of edges, $|E|$.

The **degree of a vertex**, $\deg(v)$ is the number of edges incident with the vertex with loops counted twice.

If every vertex has the same degree then it is a **regular graph**.

If the degree of each vertex is k then it is a **k -regular graph**.

A **path** of length n from a to b in the graph $G = (V, E)$ is a sequence

$a = a_1, e_1, a_2, \dots, e_n, a_n = b$ s.t. $a_i \in V$ and $e_i \in E$. (or $a_1 \dots a_n$ or $e_1 \dots e_n$)

A **simple path** passes each of its vertices only once.

The **distance** between nodes is the length of the shortest connecting path.

In a **connected graph** every pair of vertices is connected by a path.

A path starting and ending in the same vertex is a **cycle**.

A **tree** is a connected graph with no cycles, a **forest** is composed of trees.

A **planar graph** can be drawn in a plane with no edges crossing each other.

These were just some of the many definitions used in graph theory. As is usual among mathematical structures there can be subgraphs and isomorphisms. $G' = (V', E')$ is a **subgraph** of $G = (V, E)$ if $V' \neq \emptyset$, $V' \subseteq V$ and $E' \subseteq E$. Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are essentially the same or **isomorphic** if there is a bijection $f: V_1 \rightarrow V_2$ s.t. if $a, b \in V_1$ then $\{a, b\} \in E_1 \Leftrightarrow \{f(a), f(b)\} \in E_2$.

The **degree sequence** of an undirected graph is the non-increasing list of its vertex degrees. It can be used to tell non-isomorphic graphs apart. A theorem from graph theory that is easy to prove and with a corollary about the number of people that shakes hand with an odd number of people is the following.

Theorem 5. (Degree Sum Formula)

If $G = (V, E)$ is a graph or multigraph then $\sum_{v_i \in V} \deg(v_i) = 2|E|$.

Corollary. (Handshaking Lemma)

The number number of nodes of odd degree in a graph is even.

Graphs can be represented on a computer with lists or matrices. Matrices have fast access but they can be too memory expensive for big and sparse graphs. There are two ways to represent graphs with matrices. Let $G = (V, E)$ be an undirected graph with indexed vertices and edges. The **incidence matrix** of G is a $v \times e$ matrix $\mathbf{A} = (a_{ij})$ defined by:

$$a_{ij} = \begin{cases} 1 & \text{if } v_i \text{ is incident with edge } e_j. \\ 0 & \text{if } v_i \text{ is not connected with edge } e_j. \end{cases} \quad \begin{array}{l} \text{Rows represent vertices} \\ \text{Columns represent edges} \end{array}$$

Two graphs are isomorphic if and only if one of their incidence matrices is obtained from the other by permuting rows and columns.

In the second representation both rows and columns are indexed by the vertices. The **adjacency matrix** of a directed or undirected graph is a square $v \times v$ matrix $\mathbf{B} = (b_{ij})$ defined by:

$$b_{ij} = \begin{array}{l} \text{The number of nodes from vertex } i \text{ to vertex } j, \\ \text{loops counts as two, one for each direction.} \end{array}$$

Theorem 6. \mathbf{B} is a symmetric matrix if the graph is undirected and $(\mathbf{B}^p)_{ij}$ is the number of paths from vertex i to vertex j of length p .

Proof. Follows from induction over p and $(\mathbf{B}^p)_{ij} = \sum_{k=1}^v (\mathbf{B}^{p-1})_{ik} (\mathbf{B})_{kj}$.

Definitions

An **Euler cycle** in a graph is a cycle that passes each edge exactly once.

A graph (or multigraph) that contains an Euler cycle is an **Euler graph**.

A path that passes each edge of a graph exactly once is an **Euler path**.

Replace edge with node to define a **Hamilton cycle, graph and path**.

Theorem 7. (Euler-Hierholzer)

A connected graph or multigraph has an Euler cycle \Leftrightarrow

Every node is of even degree.

Leonhard Euler (1707–1783) proved it in the easier \Rightarrow direction and Carl Hierholzer (1840–1871) proved it in the opposite direction. It is not that hard to prove and I leave it as an exercise to the reader.

Corollary. A connected graph or multigraph G has an Euler path \Leftrightarrow

The number of nodes of odd degree is at most two.

Proof. Assume the RHS of the biconditional. If the number of odd nodes is zero then there is an Euler cycle by Theorem 7. Removing an edge from this cycle will make it into an Euler path. Otherwise the corollary of theorem 5 implies that the number of odd nodes must be 2. Connect these two nodes with an edge and every node is even. By Theorem 7 there will be an Euler cycle. Remove the added edge and what remains is an Euler path. Assume the LHS of the biconditional, then only the start and end nodes of the path can have odd degree i.e. no more than two odd nodes. ■

Graph theory started with Euler in 1736 when he wrote a paper on “the seven bridges of Königsberg”. The city was renamed Kaliningrad in 1946. Through the city of Königsberg flowed the river Pregel with two islands that were connected to each other and the mainland with seven bridges. Sunday walks was a common pastime and the question arose if it was possible to find a closed tour that passed each bridge exactly once. The citizens of Königsberg approached the famous mathematician Euler with their question. He solved it and showed the necessary criterion for an Euler cycle in the general case.

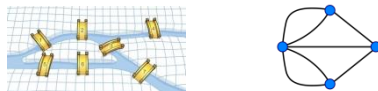


Fig 3.4.4 Map of Königsberg and its multigraph with degree sequence (5,3,3,3).

The multigraph has 7 edges and 4 nodes, all of odd degree. There can be no Euler cycle, not even an Euler path. To get an Euler path one bridge must be removed and to get an Euler cycle two bridges must be removed.

The next example from the 1930s has many applications of great importance. It involves Hamilton cycles in a **weighted graph**. Each edge is weighted with a numerical value that could represent time, cost, energy or something else. To find a path with the smallest waste of resources can be vital for resource management.

The **travelling salesman problem** (TSP) has a set of cities corresponding to nodes. Each edge is weighted by the distance between its incident cities. The goal is to find the shortest round-trip that passes every city. In a complete graph K_n with symmetric weights there is $(n - 1)!/2$ cycles to compare. TSP is relevant for telescope movement, microchip design, DNA-sequencing and many other problems. One way to formalize the problem is:

d_{ik} = Distance between city i and k

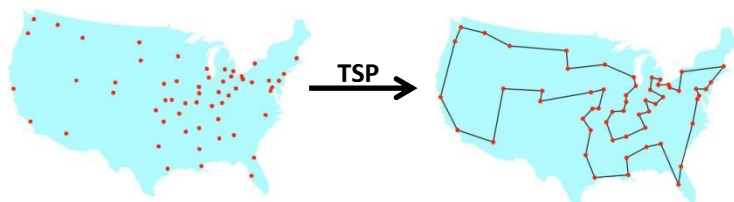
$$x_{ij} = [\text{City } i \text{ is in position } j] \quad (x_{ij} \in \{0,1\})$$

$$\text{Minimize} \quad \sum_{1 \leq i,j,k \leq n} d_{ik}x_{ij}(x_{k,i-1} + x_{k,i+1})$$

cyclical indices

Under the constraints that each city and each position is used once.

$$\sum_{i=1}^n x_{ij} = 1 \quad \sum_{j=1}^n x_{ij} = 1$$



Computational complexity theory classifies algorithms according to how time and memory to solve a problem grows with the size of the input. The Held-Karp algorithm makes use of the fact that minimal distance is preserved by subpaths. Its space complexity is $O(2^n n)$ and its time complexity is $O(2^n n^2)$ which is much better than the time $O(n!)$ needed to consider all cycles. The big O notation for growth rate is explained in a section on analysis. No algorithm for solving TSP faster than $O(2^n)$ is known. Questions concerning Complexity classes and polynomial versus non-polynomial problems deserve a section of their own in a later chapter devoted to computer science. With too many cities, heuristic or approximate algorithms that can retrieve good enough suboptimal solutions are necessary.

The greedy algorithm. Start somewhere and always go to nearest unvisited city. It is quick. For a random distribution its average is no worse than 25% longer than the optimal solution, but it can also go terribly wrong.

Ant colony optimization algorithm. It is based on how ants move between food sources and nest. Trail pheromones, scouting ants and emergent paths based on individual ant behavior translates to an algorithm that finds good solutions and avoid bad ones.

Evolutionary algorithm. This is a method based on concepts from natural evolution: inheritance, mutation, mating, selection and a fitness function to determine the quality of a solution. Set a population size P and a number of generations G to evolve a solution. Generate P random solutions and for each new generation keep the best $0.1P$ solutions, select $0.01P$ solutions randomly and mutate them and create $0.89P$ new solutions by a mating procedure.

Simulated annealing. This is a general method to search for a global optimum of a function without getting stuck in a local optimum. It derives from thermodynamics and how random fluctuations among physical states depend on temperature. The method goes from state to state with temperature deciding the probability of accepting a new solution.

It starts from a high temperature with much fluctuation up and down in energy to scope out the big picture and then gradually cools down. At $T = 0$ only downhill transitions are allowed until finally it lands in a local optimum. At high T evolution is sensitive to coarser energy variations and at smaller T it probes finer details in the energy landscape.

The probability of transition from state S to S' is decided by the acceptance probability $P(E, E', T)$ where $E = e(S)$ and $E' = e(S')$ are state energies. For TSP it amounts to the total length of a cycle. A common choice modelled on transitions in physical systems is:

$$P(E, E', T) = [E' \leq E] \cdot 1 + [E' > E] \cdot e^{-(E'-E)/T}$$

It is named after Metropolis and Hastings. Others with credit for its discovery are Marshall Rosenbluth, Edward Teller, Enrico Fermi and Stanisław Ulam.

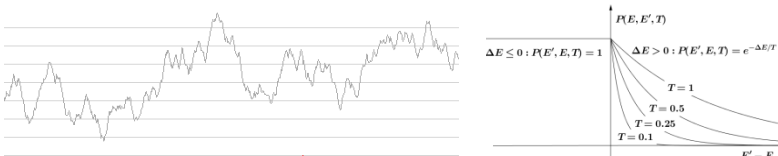


Fig 3.4.5 Local optimum search and Metropolis transition probabilities.

Artificial neural networks (ANN). This is a large class of models suitable for various tasks such as classification; like telling images of dogs and cats apart as was done in a kaggle competition or recognizing faces; pattern recognition for speech and handwriting; combinatorial optimization like TSP or general AI tasks such as being a master GO player. As the title of this book suggests I will allow myself to make digressions and wander about in the mathematical landscape. It's time for a detour to look at neural networks.

The basic function of a neuron in the neural network of the brain is to sum up incoming signals and if above a certain threshold pass a signal on to other parts of the network via synaptic connections. A real brain has 10^{11} neurons and 10^{14} synapses that work in parallel. This is the historic inspiration behind ANNs that have a limited set of nodes arranged in an architecture with hidden layers sandwiched between input nodes and output node(s). Deep learning networks can have up to 30 layers where layers extract properties based on abstractions derived from earlier layers. Between nodes are links with weights that are updated in an adaptive process.

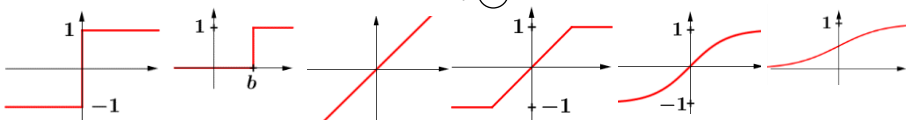
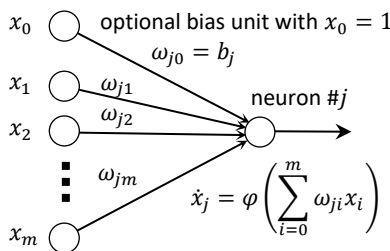
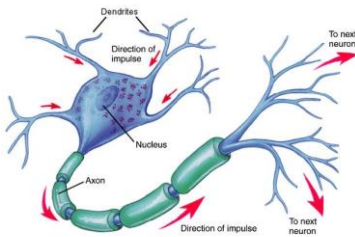
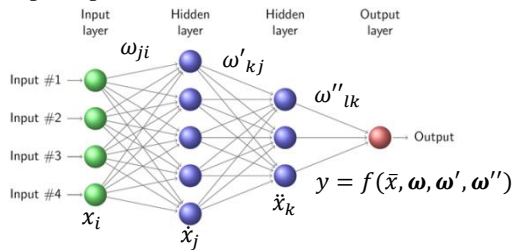


Fig 3.4.6 Neuron, network, multilayer perceptron and transfer functions.

The **transfer function** $\varphi(\cdot)$ can be a step function, a linear function or a smooth function like $\tanh(x)$ or $(1 + e^{-x})^{-1}$, with or without its own bias, (horizontal displacement). Fig. 3.12 pictures a **feedforward neural network** that can be used to classify points \bar{x} into classes coded by the value of y , often 0 or 1 with $\varphi(\cdot)$ being the corresponding step function. Information of

how to classify points is stored in the weights $\omega_{ji}, \omega'_{kj}, \dots$. The weights are assigned by a training process on a sample of classified points (\bar{x}_s, d_s) . Without going into the details, this could be done by assigning random values to ω and ω' for a first iteration $t = 1$ and then calculate $y_t = f(\bar{x}_t, \omega_t, \omega'_t)$ and adapt the weights into ω_{t+1} and ω'_{t+1} to minimize a given error function $(\sum_{s=1}^t |d(s) - y(s)|^2)/t$. Repeat the process until you get a reasonable error. This procedure is called **supervised learning**. Too small an error and the network might be over-trained for the intended task of classifying unclassified data. This happens if the boundary is to 'wiggly' in its demarcation of territories.

The first ANNs were constructed in the 1950s. They were **single-layered perceptrons** (SLP) with no hidden layers. It was soon realized that they could only learn linearly separable patterns where a hyperplane divides the sample space into two areas.

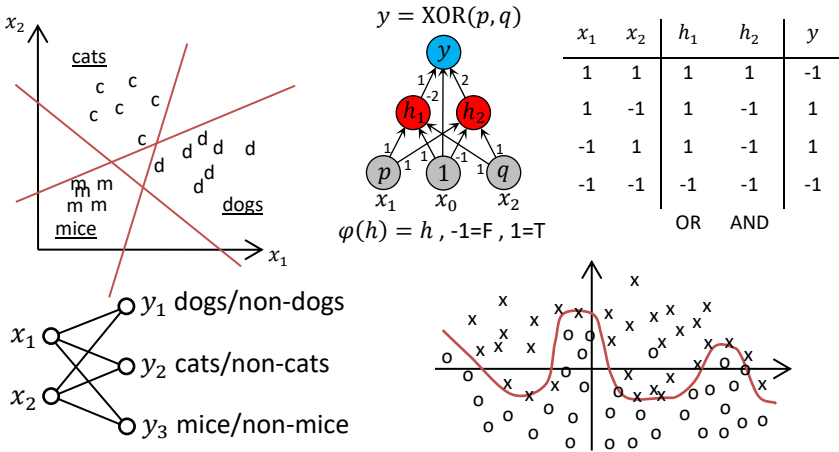


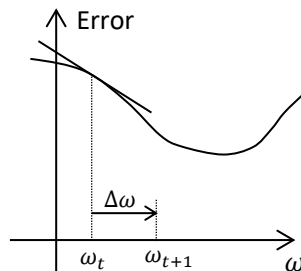
Fig. 3.4.7 SLP for c/m/d, MLP for XOR and non-linear separation of x/o.

Hidden layers necessary for non-linear classifiers are used in **multilayered perceptrons** (MLP) with smooth transition functions for derivation. Weights are updated by gradient descent to minimize errors in the output nodes for all training points (or one point at a time).

Total error normalized
$$E = \frac{1}{2N} \sum_{s=1}^N \sum_{i=1}^n (d_i(s) - y_i(s))^2$$

Correction
$$\Delta \omega''_{ab} = -\eta \frac{\partial E}{\partial \omega''_{ab}} \quad \eta = \text{learning rate}$$

$$\Delta \omega'_{ab} = -\eta \frac{\partial E}{\partial \omega'_{ab}} \quad \text{etc.}$$

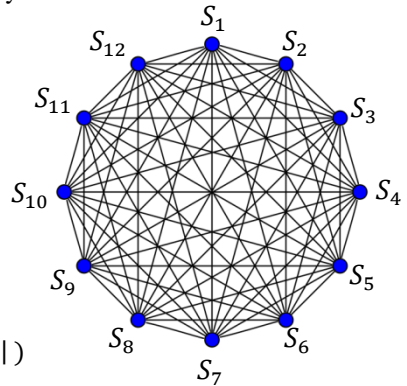


Output is calculated in forward passes through the layers whereas corrections start with the last layer. The result is then used for calculating corrections in the second last layer etc. in a backward propagation of errors. The procedure is repeated until all weights hopefully settle down in a local error-minimum.

Perceptrons with supervised learning are not of much use for the travelling salesman problem. For that you can use a **Hopfield network**, a type of network that was analyzed by John Hopfield in an influential paper from 1982. Hopfield networks can also be used as content-addressable memory, somewhat similar to our associative memory that can retrieve memories from partial information and which lets us recollect things we have forgotten by activating memories associated with what we try to remember.

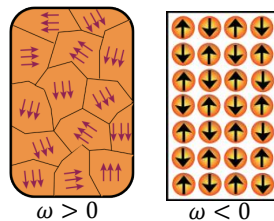
A Hopfield net is a fully connected graph K_N where each node S_i is a binary threshold unit (usually $S_i = 1$ or -1) with restrictions on weights and the following updating rule:

- $\omega_{ii} = 0$, no self-interaction
- $\omega_{ij} = \omega_{ji}$, symmetric interaction strengths
- $S_i \leftarrow \text{sgn}(\sum_j \omega_{ij} S_j - \theta_i)$ (threshold θ_i)
($\text{sgn}(x) = x/|x|$)



Updates can be performed either one unit at a time in a predefined or random order or all units at once. $\omega_{ij} > 0$ leads in the direction of S_i and S_j aligning their signs at updates whereas $\omega_{ij} < 0$ favors opposing signs. It all resembles how magnetic moments behave in materials with certain magnetic properties.

- $\omega > 0$ and declining with distance for ferromagnetic materials.
- $\omega < 0$ and declining with distance for antiferromagnetic materials.



Just as a physical systems have potential energy so does a Hopfield net have a scalar value that behaves like the energy of the network state $\mathbf{S} \in \{-1,1\}^N$. This was one of Hopfield's contributions in his paper on associative memory and neural networks in biology and computer models.

$$H = -\frac{1}{2} \sum_{i,j} \omega_{ij} S_i S_j + \sum_i \theta_i S_i \quad (*)$$

Self-interaction terms ω_{ii} can just as well be set to zero since they only contribute with a constant to the total energy ($S_i^2 = 1$). Symmetric weights guarantee that the energy will always decrease or remain constant during updates. Local minima of E will act as attractors during updating. Given a number of patterns $\xi^\mu \in \{-1,1\}^N$, how do you set ω_{ij} to make them into local minima and how many can you store?

The pattern ξ is stable ($\theta_i = 0$) if $\forall i: \text{sgn}(\sum_j \omega_{ij} \xi_j) = \xi_i$. This is true if $\omega_{ij} \propto \xi_i \xi_j$. The Hebb rule for storing M patterns $\xi^\mu, \mu = 1, 2, \dots, M$ is:

$$\omega_{ij} = \frac{1}{N} \left(\sum_{\mu=1}^M \xi_i^\mu \xi_j^\mu \right) \quad (**)$$

More patterns will reduce the basins of attractions and introduce more unintended minima $\neq \xi^\mu$. The capacity is $0.14N$ if we accept a small percentage of errors in each pattern. If we insist that most patterns should be recalled without errors then the limit is proportional to $N/\log N$.



Fig. 3.4.8 Image retrieval by a Hopfield net

The Hebb rule can be derived through the energy function. The energy should be minimal when the network state \mathbf{S} has maximal overlap with the patterns to store ξ^μ . A good choice for this to happen is:

$$H = -\frac{1}{2N} \sum_{\mu=1}^M \left(\sum_{i=1}^N S_i \xi_i^\mu \right)^2 \Rightarrow E = -\frac{1}{2} \sum_{i,j} \left(\frac{1}{N} \sum_{\mu=1}^M \xi_i^\mu \xi_j^\mu \right) S_i S_j$$

Comparison with(*) gives the Hebb rule (**) for weight assignment. This is a fruitful approach for many optimization problems. Write an energy function whose minimum satisfies the problem, expand it and identify coefficients of $S_i S_j$ as weights and linear terms as thresholds. Constraints are handled with penalty terms that are minimized when the constraints are satisfied. Applying this to the travelling salesman problem from page 117 gives:

$$H = \frac{1}{2} \sum_{i,j,k} d_{ik} x_{ij} (x_{k,i-1} + x_{k,i+1}) + \frac{\gamma}{2} \left[\sum_j \left(1 - \sum_i x_{ij} \right)^2 + \sum_i \left(1 - \sum_j x_{ij} \right)^2 \right]$$

The penalty coefficient γ is handled by experimentation to get the best result.

You don't want to get stuck in a local minimum. This can be handled with stochastic techniques like simulated annealing. Temperature treatment of Hopfield networks is a direct parallel to statistical mechanics of interacting particles with spin, also known as Ising models. More on this in appendix C.

A variation on the TSP is the Euclidean TSP with cities in a (x, y) -plane with Euclidean distances $\sqrt{\Delta x^2 + \Delta y^2}$. This problem is suitable for a Kohonen self-organizational feature map (SOFM). Such a network looks like a simple-layered perceptron with x and y nodes in one layer. The new feature of these ANNs is that nodes in the outgoing layer are ordered in a lattice of one or two dimensions that may or may not curl up.

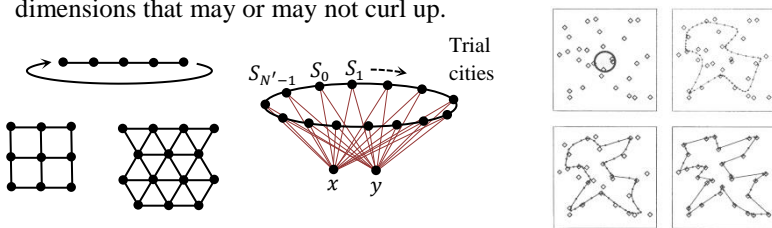


Fig. 3.4.9 ANN with SOFM for TSP.

Trial cities S_i with positions placed in their weights $\bar{\omega}_i = (\omega_{ix}, \omega_{iy})$ are put on an 'elastic rubber band'. Their number N' and weights will change while adapting to the N real cities C_k , with positions \bar{v}_k . The goal is $N' = N$ and $\bar{\omega}_n \rightarrow \bar{v}_{f(n)}$ for some permutation f , with minimal tour length $\sum_i |\bar{\omega}_i - \bar{\omega}_{i+1}|$.

Go through the cities and for each C_k choose the closest trial city S_i . Adapt the weights of S_i and its neighbors in the direction towards C_k , $\Delta \bar{\omega}_j \propto e^{-n^2/\sigma^2} (\bar{v}_k - \bar{\omega}_j)$. Adjustments shrink with increasing $n =$ 'neighbor-distance from i' , and with decreasing σ . This number is lowered in steps to improve convergence and peak the neighborhood of changing weights around i .

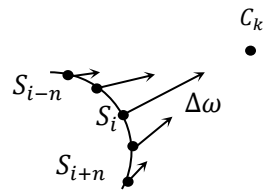


Fig. 3.16 Weight adjustments

The update rule can be retrieved from an energy/error function of a Hopfield network. The error function contains a factor Λ_{ij} that declines with neighbor distance between nodes i and j .

$$E = \frac{1}{2} \sum_{k=0}^N \sum_{j=0}^{N'} \Lambda_{ij} (\bar{v}_k - \bar{\omega}_j)^2 \quad (i \text{ is the } S_j \text{ node closest to } C_k)$$

If a trial city is the closest one to two different cities it will be duplicated and its clone will be inhibited from moving along with its originator. If a trial city fails to be the closest trial city of a real city for several complete surveys it will be deleted.

Which algorithm to choose depends on the number of cities and the computational time allowed. For the Euclidean version the human mind has an impressive ability to intuitively spot improvements missed by advanced and time-consuming computations. One such improvement, easy to see and often missed by the presented algorithms is the removal of crossings in the path.

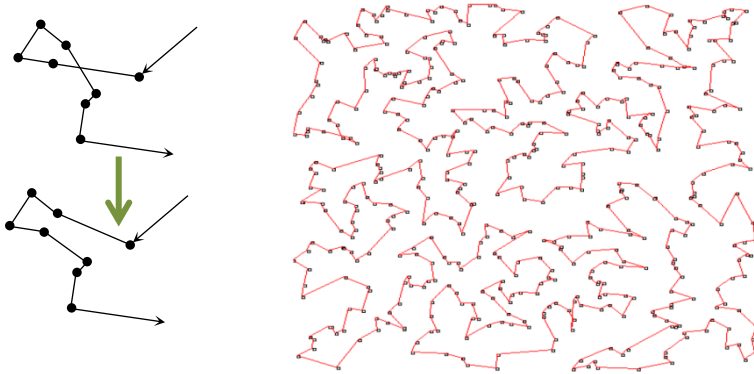


Fig 3.4.10 Removal of crossing and successful end result for 500 cities.

The best programs for the TSP can handle millions of ‘cities’ to within 2-3 % of the optimal tour length. According to Wikipedia the optimal tour length for visiting all 24,978 ‘towns’ of Sweden has been found. It is 72,500 km.

Algorithms for the Euclidean TSP are often tested with a random distribution of points in the unit square. It has been shown that with random variables $(X_i)_1^n$ with uniform distribution in a bounded plane region of area v , the length of the optimal TSP solution is ‘almost always’ asymptotically proportional to \sqrt{nv} . With $\mathbb{E}(L_n)$ being the expected optimal tour length of n points in the unit square there is a well-defined limit of $\mathbb{E}(L_n)/\sqrt{n}$ as $n \rightarrow \infty$:

$$\lim_{n \rightarrow \infty} \frac{\mathbb{E}(L_n)}{\sqrt{n}} = \beta$$

Best known bounds $0.63 < \beta < 0.92$
 Computer experiments give $\beta \gtrsim 0.71$
 Sweden: $450,295 \text{ km}^2 \rightarrow L_n/\sqrt{nv} = 0.68$

After this detour into neural networks and the traveling salesman problem it’s time to return to graph theory.

If a graph $G = (V, E)$ can be illustrated with a drawing on a plane without edges crossing outside vertices might not seem like an important property but **planar graphs** tells us something about polyhedrons and they are also the starting point of topology.

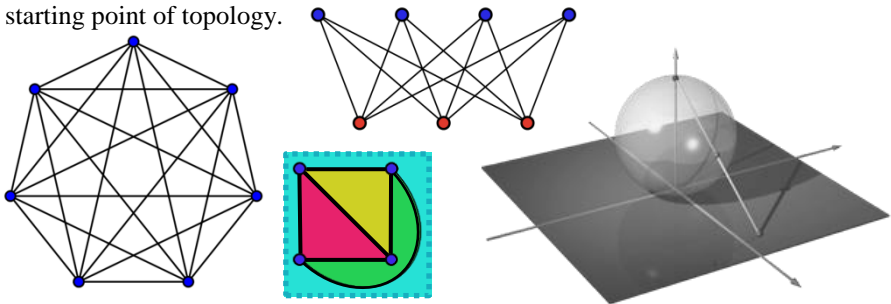


Fig 3.4.11 Graph K_7 , K_4 , Complete bipartite graph $K_{4,3}$ and stereographic projection.

K_4 and $K_{3,2}$ are planar but K_5 and $K_{3,3}$ are not. The last fact is the answer to the classical puzzle of connecting gas-, water- and electrical plant in Flatland to three houses. Every non-planar graph has at least one subgraph that is a subdivision of K_5 or $K_{3,3}$ (Kuratowski’s theorem). A subdivision is simply a series of extensions with extra vertices put on existing edges, $\{a, b\} \subseteq V$ and $\{ab\} \subseteq E$ are replaced by $\{a, b, x\} \subseteq V$ and $\{ax, xb\} \subseteq E$.

A non-crossing drawing of a connected planar graph divides the plane into **faces** that are bounded by edges of the graph. One face is of infinite extent, it’s called the outer face. When the drawing is projected onto a sphere via the stereographic projection the north pole will be somewhere in the outer face. No distinction exists on the sphere between the outer face and the other faces. The number of faces in a planar graph is denoted by f .

Theorem 8. (Euler’s polyhedron formula)

Let $G = (V, E)$ be a connected planar graph, v vertices, e edges and f faces.

$$v - e + f = 2$$

Proof. (By induction over the number of edges)

For $e = 1$ there are two possibilities that both gives $v - e + f = 2$, one node with a loop, $v = 1, e = 1, f = 2$ and two nodes and one edge, $v = 2, e = 1, f = 1$.

Assume the theorem is true for all graphs with $k-1$ edges. Let G be a graph with v vertices, k edges and f faces. There are two cases to consider:

- I. If G has a vertex of degree 1, let H be the subgraph obtained by removing this vertex and its edge. H has $v-1$ vertices, $k-1$ edges and f faces. By assumption the theorem is valid for $H \Rightarrow v - k + f = 2$.
- II. If there is no such vertex then there will be an edge that is part of a finite face. Remove this edge and the remaining graph has v vertices, $k-1$ edges and $f-1$ faces. Using the theorem on this subgraph $\Rightarrow v - k + f = 2$. ■



Fig. 3.4.12 Central projections of regular convex polyhedra (Schlegel diagrams).

Convex polyhedrons are linked to planar graphs via projection from a point onto a plane, hence the name polyhedron formula. Euler’s proof was based on vertices, edges and faces of convex polyhedra. Adding edges to triangulate polygonal faces and deforming a polyhedron away from convexity does not change the value of $v - e + f$. It applies to all polyhedra with a boundary in the shape of a sphere.

Definition. A cycle of a graph $G = (V, E)$ is a set of $k \geq 3$ different vertices such that $a_1 a_2 \dots a_k a_1$ is a path in the graph.

Corollary 1. Every loop-free planar connected graph with one or more cycles, all of length at least k has $e(k - 2) \leq k(v - 2)$.

Proof. Every face is bounded by at least k edges and each of these is the boundary between two faces so $2e \geq kf \Leftrightarrow f \leq 2e/k$ which with Euler’s formula gives $v - e + 2e/k \geq 2 \Leftrightarrow (2 - v)k \leq e(2 - k)$. ■

Corollary 2. Every loop-free planar graph with $v > 3$ has $e \leq 3v - 6$.

Proof. If the graph is connected and contains a cycle it follows from Cor.1 with $k = 3$. Larger k only strengthens the inequality. If there are no cycles, a cycle can be formed by adding edges $e + n \leq 3v - 6 \Rightarrow e \leq 3v - 6$. If the graph is not connected it can be connected by adding edges. ■

Now it’s easy to show that K_5 and $K_{3,3}$ are non-planar graphs.

K_5 has $v = 5$ and $e = 10$, in clear violation of corollary 2 for planar graphs.

If $K_{3,3}$ were planar then any face would have at least 4 edges. $k = 4, v = 6$ and $e = 9$ violates corollary 1 so $K_{3,3}$ must be a non-planar graph.

Theorem 9. There can be no more than five regular convex polyhedra.

Proof. A regular convex polyhedron has v vertices where $n \geq 3$ faces meet, e edges and f faces with $m \geq 3$ edges.

$$2e = mf = nv$$

By stereographic projection into a planar graph we get. (convexity needed)

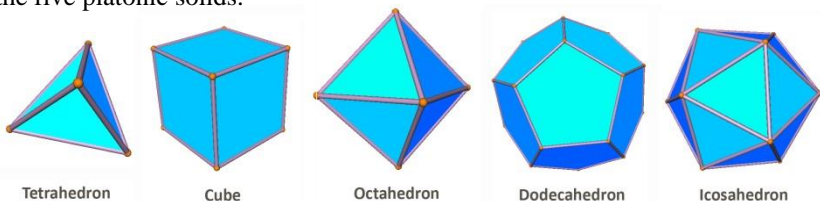
$$2 = v - e + f = \frac{2e}{n} - e + \frac{2e}{m} = e \left(\frac{2m - mn + 2n}{mn} \right)$$

$$2m - mn + 2n > 0 \Rightarrow (m - 2)(n - 2) < 4$$

$(m - 2) \in \mathbb{Z}^+$ and $(n - 2) \in \mathbb{Z}^+$ gives five possibilities:

- | | | |
|--|--------------|---|
| 1. $m = 3, n = 3 \Rightarrow v = 4, e = 6, f = 4$ | Tetrahedron | |
| 2. $m = 4, n = 3 \Rightarrow v = 8, e = 12, f = 6$ | Cube | |
| 3. $m = 3, n = 4 \Rightarrow v = 6, e = 12, f = 8$ | Octahedron | |
| 4. $m = 5, n = 3 \Rightarrow v = 20, e = 30, f = 12$ | Dodecahedron | |
| 5. $m = 3, n = 5 \Rightarrow v = 12, e = 30, f = 20$ | Icosahedron | ■ |

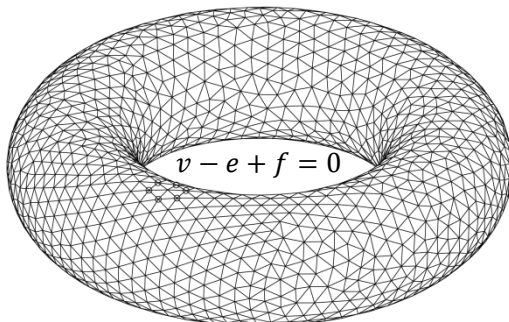
The tetrahedron, cube and octahedron are obviously constructible. It's less obvious that the dodecahedron and icosahedron exist but they do. These are the five platonic solids.



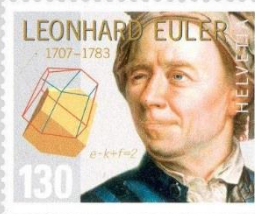
For polyhedrons with a boundary that can't be deformed into a sphere:

$$v - e + f = \chi$$

χ is the Euler characteristic, a topological invariant that describes a shape and stays the same during continuous deformation. A closed orientable surface has $\chi = 2 - 2g$ where g is the genus of the surface, the number of closed curves that can be cut without disconnecting the surface into separate pieces.



Leonhard Euler (1707-1783)



Euler is one of the greatest mathematicians in history and the most prolific. His collected works contains over 25,000 pages. There was often a long period from idea to publication and much of his work was published after his death. It has been said that in order to avoid naming everything after Euler things should instead be named after the first person after Euler who discovered them. He was active in all fields of mathematics as well as physics, astronomy and engineering. Laplace known for his unwillingness to give credits to others said: Read Euler, for he is the master of us all. Euler's life divides naturally into four periods based on where he lived.

1. Basel 1707-1727

Leonhard grew up and studied in Basel. His father was a Calvinist pastor and his mother was a pastor's daughter. He was set on a path to become a pastor and began studies at the University of Basel when he was thirteen, a common age those days for enrollment in higher studies. He wrote a dissertation that compared the philosophies of Descartes and Newton before specializing in theology with subjects such as Greek and Hebrew.

Another family in Basel was the Bernoullis. Johann Bernoulli was one of the best mathematicians of his time. He was a friend of the Euler family and helped Leonhard in his private math studies on Saturday afternoons. He recognized Leonhard's great talent and persuaded his reluctant father that he should switch from theology to mathematics so he could fulfill his destiny and become a great mathematician.

When he was nineteen years old in 1727, Euler submitted an entry on how to arrange masts on a ship for the Grand Prize of the Paris Academy. This was a prestigious and annual competition to solve a selected problem. Euler finished as number two. He returned and shared first prize in 1738 and 1740. It earned him great prestige and respect as a master of his field.

2. Saint Petersburg 1727-1741

Johan Bernoulli had three sons, all mathematicians. Daniel and Nicolaus worked for the Academy in St Petersburg. The city had been founded by Peter the Great in 1703 and the academy was his effort to open Russia to outside influence and close the gap in science with Western Europe. Nicolaus died in 1726 and Daniel took his position in the mathematics department which left Daniel's post in physiology vacant. Daniel recommended his friend Euler for the job. Euler had an exceptional

memory and had no problem educating himself for a medical position. Euler immediately moved on to work with physics and mathematics in close collaboration with his friend Daniel Bernoulli but he did not leave medicine completely. He took on an extra job as a medic in the navy.

The groundwork for the academy had been laid by Leibniz and Peter I who died two years before Euler came to Russia. The plans were carried through by Catherine I, the widow of Peter I. Catherine died the same year that Euler arrived. Many in the Russian nobility viewed the Academy with suspicious eyes, a luxury dominated by foreign scientists. Contrary to most other members of the Academy, Euler quickly learned and mastered Russian. Daniel eventually grew tired of conflicts and returned to Switzerland. Euler became head of the mathematics department, settled down and got married in 1734 to Katharina Gsell, daughter of a Swiss painter. They had thirteen children but only five survived childhood.

Russia was in turmoil after the death of Tsarina Anna Ivanovna. Euler was looking for a way out. After having won the Grand Prize of the Paris Academy he had got an invitation from Frederick the Great of Prussia to come to Berlin and establish an Academy of Sciences there. In 1741 he took his family from Saint Petersburg to Berlin.

3. Berlin 1741-1766

In Berlin he wrote several major works of great influence but in terms of readers nothing could match “Letters to a German princess, on different subjects in physics and philosophy”. It was a compilation of his mail correspondence with Frederick’s niece Friederike Charlotte Leopoldine Louise of Brandenburg-Schwedt, also known as the Princess of Prussia.

Euler was a modest and devout religious man, in many ways the opposite of the spirit of the French enlightenment and personalities like Frederick and Voltaire, a witty and satirical master of argumentation and a popular guest at Frederick’s court. One story says that Euler was reproached by the Queen Mother for not conversing. His reply was, “Madame, I come from a country where if you speak, you are hanged”. She was not amused and relations with Frederick were not improved by disputes over who should lead the Academy.

The Seven Years’ War (1756-1763) was raging in Europe. Euler’s home outside Berlin was ransacked by Russian troops. He received a generous compensation for this by Empress Elisabeth of Russia. Russia stabilized under the reign of Catherine the Great and she invited Euler to come back to the Academy in Saint Petersburg.

4. Saint Petersburg 1766-1783

Euler was offered very good conditions in Russia and in 1766 he accepted the invitation to return to the Academy. He was as productive as ever and spent the rest of his life in Russia but not without tragedies.

Euler had eye problems for most of his life. He had a severe fever in 1735 which might be related to his almost complete loss of sight on the right eye. The bad eye can be seen on the picture from 1753 on the stamp. A cataract appeared in his left eye while in Berlin, it got worse and after an operation in 1771 that led to an abscess he had virtually no sight left. The same year he was very lucky to be saved from his burning home by his workman from Basel. Two years later he lost his wife Katharina. In spite of all the misfortunes he carried on with his work without slowing down. His comment to being blind was: “now I will have less distraction”.

In the words of François Arago a French scientist “He calculated without any apparent effort, just as men breathe, as eagles sustain themselves in the air”. On his last day, he taught one of his grandchildren some math, calculated the motion of balloons on his big slate (the Montgolfier brothers had just done their first balloon flight), discussed the orbit of the newly discovered planet Uranus with a colleague and in the afternoon while playing with the grandchild he suffered a stroke. Marquis de Condorcet wrote in his eulogy for the French Academy “... suddenly, the pipe, which he held in his hand, dropped from it, and he ceased to calculate and to live”. Euler’s final resting place can be seen in the Alexander Nevsky Monastery in Saint Petersburg.

Major works

- 1727, *Dissertatio physica de sono*: Submitted in support of his application to the physics chair at the University of Basel. (He did not get the job, went to St Petersburg instead)
- 1736, *Mechanica*: Comprehensive treatment of mechanics including mechanics of flexible and elastic bodies, fluid mechanics, celestial mechanics. First systematic use of differential and integral calculus to mechanics (analytical mechanics).
- 1739, *Tentamen novae theoriae musicae*: Physical nature of sound, pleasure and physiology of audio perception, generation of sound by string and wind instruments.
- 1744, *Methodus inveniendi lineas curvas maximi...*: Creates a new branch of mathematics, ‘calculus of variation’ and derives the Euler-Lagrange equation.
- 1748, *Introductio in analysin infinitorum*: Develops the concept of a function, introduces real and complex functions, infinite series and products, continued fractions and partitions, uses the fundamental theorem of algebra but without proof.
- 1749, *Scientia navalis*: Naval science, hydrostatics, equilibrium and oscillations about equilibrium of bodies submerged in water.
- 1753, *Theoria motus lunae*: Euler’s first lunar theory, provided astronomers with formulae needed to prepare lunar tables that served navigation for over a century.
- 1755, *Institutiones calculi differentialis...*: Textbook on calculus with power series and summation formulae, contains the first example of a Fourier series.

- 1765, *Theoria motus corporum solidorum...*: "Second Mechanics", motion of rigid bodies, two coordinate systems, Euler angles and motion of spinning tops.
- 1768-1770, *Institutionum calculi integralis...*(3 volumes): Textbook on calculus with indefinite integration, differential equations, linear 2nd order diff. eq., and linear PDE.
- 1768,1772, *Lettres a une princesse d'Allemagne sur divers sujets...*: Written in 1760-1762, contains Euler's views on physics, science, philosophy, ethics and religion.
- 1769-1771, *Dioptricae* (3 volumes): Optical instruments.
- 1770, *Vollständige Anleitung zur Algebra*: Comprehensive introduction to algebra.
- 1772, *Theoria motuum lunae*: Second lunar theory, deals with the three-body problem for the sun-earth-moon system.
- 1776, *Nova methodus motum corporum rigidorum determinandi*:
Seminal work on mechanics with formulations of linear and angular momentum.
- 1911-, *Opera omnia*: Complete works of Euler, fills 74 volumes and 16 more are planned. Euler's works have a chronological index made by G. Eneström stretching from E1 to E866.

Achievements

- 1727 Euler's number $e \equiv \lim_{n \rightarrow \infty} (1 + 1/n)^n = 2.71828...$ The constant was discovered by Jakob Bernoulli but Euler chose the symbol e for it.
- 1729 Euler's integral of the first kind $B(x, y) = \int_0^1 t^{x-1}(1-t)^{y-1} dt$ (Beta function) and of the 2nd kind $\Gamma(t) = \int_0^\infty x^{t-1} e^{-x} dx$ (Gamma function $\Gamma(n) = (n-1)!$)
- 1730 Improved on earlier work on infinite series.
- 1734 Modern notion of a mathematical function with notation $f(x)$.
- 1735 Solved the Basel problem $\sum_{k=1}^\infty 1/k^2 = \pi^2/6$
- 1735 Euler's constant $\gamma \equiv \lim_{n \rightarrow \infty} (1^{-1} + 2^{-1} + \dots + n^{-1} - \ln n) = 0.57721$
Euler showed its existence and calculated it to 16 decimal places.
- 1735 Solved and generalized the bridge problem of Königsberg. The start of graph theory. Eulerian path, a path that visits every edge exactly once. Euler tour technique for traversing binary trees and Euler tour representation useful for parallel computation.
- 1736 Proof of Fermat's little theorem $a^p \equiv a \pmod{p}$ with $a \in \mathbb{Z}, p \in \mathbb{P}$
- 1736 Proved the Euler-Maclaurin formula connecting integrals and sums,

$$I = \int_m^n f(x) dx \quad S = f(m+1) + \dots + f(n-1) + f(n)$$

$$S - I = \sum_{k=1}^p \frac{B_k}{k!} (f^{(k-1)}(n) - f^{(k-1)}(m)) + R \quad \text{with } |R| \leq \frac{2\zeta(p)}{(2\pi)^p} \int_m^n |f^{(p)}(x)| dx$$
- 1737 Popularized π as a symbol for the ratio of the circumference and diameter of a circle.
- 1737 Used analytic methods for number theory and continued fractions.
- 1737 Proved $\sum_{p \in \mathcal{P}} 1/p$ is divergent where $\mathcal{P} = \{2, 3, 5, 7, 11, 13, \dots\}$ is the set of primes.
- 1737 Proof of Euler's product formula $\zeta(s) = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}$
- 1739 Proves $\zeta(2n) = 2^{2n-1} |B_{2n}| \pi^{2n} / (2n)!$ for Riemann's zeta function $\zeta(s) \equiv \sum_{k=1}^\infty n^{-s}$.
- 1740 Calculus of variation and Euler-Lagrange equations, $q(t)$ is a stationary point of the functional $S(q) = \int_a^b L(t, q(t), \dot{q}(t)) dt$ if $\frac{\partial L}{\partial q_i}(t, q, \dot{q}) = \frac{d}{dt} \frac{\partial L}{\partial \dot{q}_i}(t, q, \dot{q})$, $i = 1, \dots, n$
- 1743 Euler's formula $e^{i\varphi} = \cos \varphi + i \sin \varphi$ (published 1748)
- 1743 Euler's identity $e^{i\pi} + 1 = 0$
- 1744 First to use a Fourier series. (published 1755)
- 1744 Euler spiral with curvature \propto length, found its limit in 1781. Reinvented by Fresnel.
- 1745 Studied hyperbolic trigonometric functions.
- 1747 Proof of Fermat's conjecture $p = x^2 + y^2, p \in \mathcal{P} \setminus \{2\} \wedge x, y \in \mathbb{Z} \Leftrightarrow p \equiv 1 \pmod{4}$
- 1747 Proved the Euclid-Euler theorem in both directions (Euclid proved \Leftarrow)
 N is a perfect number $\Leftrightarrow N = 2^{n-1}(2^n - 1)$ with $n \in \mathbb{Z}^+$ and $M_n = 2^n - 1$ prime.
 A perfect number equals the sum of its proper divisors
 A Mersenne prime M_n is a prime of the form $M_n = 2^n - 1$ with $n \in \mathbb{Z}^+$
- 1748 The four-square law $(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = x^2 + y^2 + z^2 + t^2$
- 1748 Euler's continued fraction formula for $a_0 + a_0 a_1 + \dots + a_0 a_1 \dots a_n$.

- 1748 Euler's criterion for determining if an integer is a quadratic residue modulo a prime.
- 1748 Euler function $\phi(q) = \prod_{k=1}^{\infty} (1 - q^k)$ for number theory and modular forms.
- 1749 Euler polynomials $E_n(x)$ and Euler numbers, E_n appear in the Taylor expansion of $1/\cosh t$ closely related to Bernoulli polynomials and Bernoulli numbers.
- 1750 Euler's polyhedron formula $V - E + F = 2$, his proof contained a small gap. Descartes had a similar formula in 1630. For other dimensions and shapes $2 \sim \chi$. The Euler characteristic χ , topological invariant and precursor to algebraic topology.
- 1750 Euler's laws of motion for continuous bodies.
First law with linear momentum and external forces, $\mathbf{p} = m\mathbf{v}_{cm} \rightarrow \mathbf{F}_{tot} = d\mathbf{p}/dt$
Second law with angular momentum and external moments, $\mathbf{M}_{tot} = d\mathbf{L}/dt$.
- 1750 Euler-Bernoulli beam theory for load and deflection characteristics of beams.
- 1751 Extends definition of e^x and $\ln x$ to complex numbers.
- 1752 Euler's pump-turbine equations used for performance of engines and power plants.
- 1755? The Euler transform $\sum_{k=0}^{\infty} (-1)^k a_k = \sum_{k=0}^{\infty} (-1)^k \Delta^k a_0 / 2^{k+1}$ to accelerate convergence of alternating series.
- 1755? Euler's homogeneous function theorem $f(\lambda \mathbf{x}) = \lambda^r f(\mathbf{x}) \Leftrightarrow \mathbf{x} \cdot \nabla f(\mathbf{x}) = kf(\mathbf{x})$.
- 1755 Introduced the Greek letter Σ for summation and Δ, Δ^2, \dots for finite differences.
- 1757 Critical buckling load of a column $F = (\pi^2 EI)/(KL)^2$ E, I, K, L material constants.
- 1757 Euler equations for fluid flow with zero viscosity:

$$\partial \rho / \partial t + \nabla \cdot (\rho \mathbf{u}) = 0$$

$$\partial (\rho \mathbf{u}) / \partial t + \nabla \cdot (\mathbf{u} \otimes \rho \mathbf{u}) + \nabla p = 0$$

$$\partial E / \partial t + \nabla \cdot (\mathbf{u}(E + p)) = 0$$
- 1757 Euler number (Eu), a dimensionless number used in fluid flow calculations.
- 1758 Euler's rotation equations describing rotation of a rigid body fixed to body's principle axis of inertia, $\mathbf{I} \cdot \dot{\boldsymbol{\omega}} + \boldsymbol{\omega} \times (\mathbf{I} \cdot \boldsymbol{\omega}) = \mathbf{M}$
 \mathbf{I} is the inertia matrix, $\boldsymbol{\omega}$ is the angular velocity and \mathbf{M} is applied torques.
- 1760 Euler's three-body problem, to find the movement of a particle acted on by the force of gravity from two point masses fixed in space. The problem is solvable.
- 1760 Euler-Lotka equation, describes age-structured population growth. Equation was based on original work of Euler and generalized by 20th century demographer Lotka.
- 1760 Proved existence of principal curvatures and principal directions on a surface.
- 1763 Introduced Euler's totient function $\phi(n) \equiv \#\{k \in \mathbb{N} | k \leq n \wedge (k, n) = 1\}$ and generalized Fermat's little theorem to Euler's theorem $a^{\phi(n)} \equiv 1 \pmod{n}$
- 1765 Euler line, a well-defined line for every non-equilateral triangle passing through the centroid, the orthocenter and the circumcenter of a given triangle.
- 1765 Euler angles (α, β, γ) sometimes (φ, θ, ψ) describing the orientation of a rigid body.
- 1767 Euler's geometric theorem $d^2 = R(R - 2r)$ where R and r are radii for inscribed and circumscribed circles of a triangle and d is the distance between their centers.
- 1768 Euler-Cauchy equation $\sum_{k=0}^n a_k x^k y^{(k)}(x) = 0$, a 2nd order ODE.
- 1768 Cauchy-Euler operator, an operator of the form $p(x) \cdot d/dx$ with a polynomial $p(x)$.
- 1768 The Euler method, numerical procedure for solving ordinary differential equations.
- 1768 Euler diagrams, visual aid in syllogistic reasoning and precursor of Venn diagrams.
- 1770 Eulerian integers, $m + n\omega$, $\omega = e^{2\pi i/3}$ used by Euler to study Fermat's last theorem.
- 1772 Showed $2^{31} - 1 = 2,147,483,647$ was a prime, the biggest known until 1867.
- 1775 Euler's rotation theorem, any rotation of a body with one point fixed is equivalent to a single rotation about some axis running through the fixed point.
- 1777 Studied Cauchy-Riemann's equations, used earlier by d'Alembert for hydrodynamics.
- 1777 Introduced symbol i for the imaginary unit.
- 1780 Showed existence of Graeco-Latin squares a.k.a Euler squares for $n=2k+1$ and $n=4k$. Euler conjectured that none exists for $n=4k+2$, a false proof of this was given 1922. Euler's efforts for $n=6$ resulted in a puzzle, the 36-officer problem with no solution. The conjecture was disproved in 1959, Euler squares actually exists for all $n > 6$.
- 1783 Conjectured the law of quadratic reciprocity which was later proved by Gauss.
- 1783 Showed that the tetration limit, $\lim_{n \rightarrow \infty} x \uparrow n$ is convergent for $e^{-e} \leq x \leq e^{1/e}$.

Euler’s formula can be expanded, not only from a spherical boundary to other shapes but also from three to higher dimensions. The next step after a planar graph would be a graph that can be drawn in three dimensions with no faces crossing each other. An n -dimensional polyhedron is called a polytope. It has cells of dimension $0, 1, \dots, n - 1$ and $\chi = c_0 - c_1 + \dots + (-1)^{n-1}c_{n-1}$ where c_k is the number of cells of dimension k .

Examples (All the regular convex polytopes from four dimensions)

4-cell (~ Tetrahedron)	$c_0 = 5$	$c_1 = 10$	$c_2 = 10$	$c_3 = 5$	$\chi = 0$
Tesseract (~ Cube)	$c_0 = 16$	$c_1 = 32$	$c_2 = 24$	$c_3 = 8$	$\chi = 0$
16-cell (~ Octahedron)	$c_0 = 8$	$c_1 = 24$	$c_2 = 32$	$c_3 = 16$	$\chi = 0$
24-cell	$c_0 = 24$	$c_1 = 96$	$c_2 = 96$	$c_3 = 24$	$\chi = 0$
120-cell	$c_0 = 600$	$c_1 = 1200$	$c_2 = 720$	$c_3 = 120$	$\chi = 0$
600-cell	$c_0 = 120$	$c_1 = 720$	$c_2 = 1200$	$c_3 = 600$	$\chi = 0$

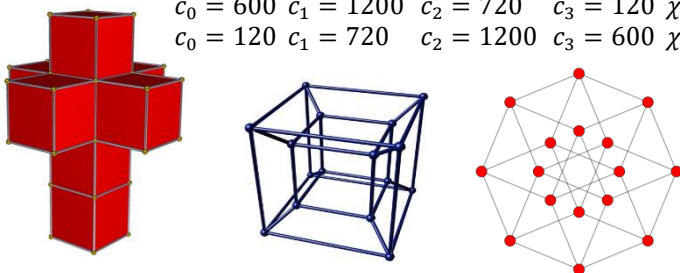


Fig. 3.4.13 Tesseract, unfolded / Schlegel diagram / ortographic projection.

Polytopes of every dimension and every shape of their boundary satisfies:

$$\sum_{k=0}^{n-1} (-1)^k c_k = \chi$$

Where χ is a topological invariant defined by the boundary. A sphere of n dimensions $S_n = \{x \in \mathbb{R}^{n+1} \mid |x| = 1\}$ has $\chi(S^n) = 1 + (-1)^n$ whereas a torus of n dimensions $T_n = \underbrace{S^1 \times \dots \times S^1}_{n \text{ factors}}$ always has $\chi(T^n) = 0$.

Euler’s characteristic is not the only use for χ in graph theory. There is a special branch that deals with different ways of labeling parts of a graph. The labels, usually integers are traditionally called colors.

Definition. A **coloring** of a graph is an assignment of colors to vertices such that adjacent vertices are colored differently. The smallest number of colors needed to color a graph G is called its **chromatic number**, $\chi(G)$.

Example. $\chi(K_n) = n$ and $\chi(K_{m,n}) = 2$ if $m, n > 0$.

Every drawing of a planar graph leads in a natural way to a new graph that has one vertex in each face of the old graph.

Definition. Every planar representation \tilde{G} of a planar graph G (or multigraph) has a **dual graph** \tilde{G}^d with vertices equal to the faces of \tilde{G} and with edges between faces that share a border edge in \tilde{G} .

The duality is reflected in a similar definition of duality between polyhedra.

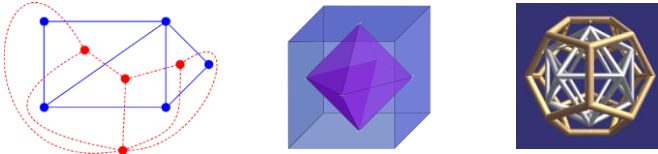


Fig. 3.4.14 Dual graphs and dual polyhedra.

The octagon and cube form a dual pair as does the dodecahedron and the icosahedron. The tetrahedron is its own dual. In higher dimensions there are similar dualities. The tesseract and 16-cell are dual as are the 120-cell and the 600-cell. The 4-cell (4-dimensional tetrahedron) and the 24-cell are self-dual.

The classical and most famous question in graph labeling was the four color map question. Given a partition of the plane into contiguous regions, is it possible to color the regions with no more than four colors so that no neighboring regions have the same color? Regions that only share a vertex are not considered to be neighbors. The question is now a theorem and by using our definitions and dualities it can be stated more shortly.

Theorem. (The four color theorem)
 If G is a planar graph then $\chi(G) \leq 4$.

The question was of interest to mapmakers. It was posed in the 1850s and a proof was published in 1879. It received a lot of attention but it took more than 10 years before several errors were found. A valid proof was first given by Appel and Haken in 1976. The proof was based on a reduction to a large number of individual maps that could be checked by a computer program. It was the first major theorem to be proved with the help of a computer. Computer-assisted proof was controversial, not every mathematician accepted a proof that could not be checked by hand. Today it is widely accepted, especially with the introduction of special proof-checking software.

The proof is actually easier for surfaces other than planes and spheres. A map on a closed orientable surface with genus g (sphere with g handles) requires

$$n = \lfloor 1/2 \cdot (7 + \sqrt{48g + 1}) \rfloor \text{ colors.}$$



Fig. 3.4.15 Torus map requiring 7 colors and plane with 4 country colors.

3.5 Equations, Algebra and Complex numbers

Solving **equations** is a common exercise in school mathematics. In this part the focus will be on equations with one unknown quantity often denoted x . Other variables that occur will usually be parameters that represent fixed but arbitrary numbers of some set. An example is $ax^2 + bx + c = 0$ or in its reduced form $x^2 + px + q = 0$.

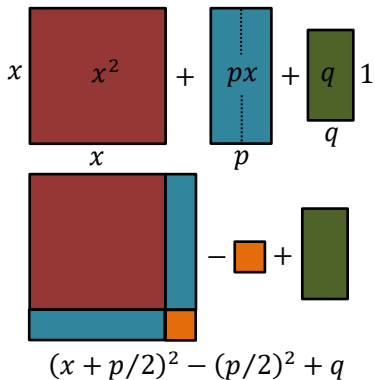
Equations have a left-hand side (LHS), a right-hand side (RHS) and an equals sign in between, $L(x) = R(x)$. The goal is to find the set of solutions (roots) $\{x|L(x) = R(x)\}$ and to express them as explicitly as possible. The sign for equality consisting of two equal lines was introduced by a mathematician from Wales in 1557. Some variations on '=' are:

- \neq not equal, $1 \neq 2$
- \approx almost equal, $\pi \approx 3.14159$
- $:=$ definition, $\tau := 2\pi$
- \cong congruence (geometry), $\triangle ABC \cong \triangle DEF$
- \equiv identity, congruence relation (arithmetic) or definition,
 $(x + y)^2 \equiv x^2 + 2xy + y^2$, $\sin^2 x + \cos^2 x \equiv 1$, $7 \equiv 1 \pmod{3}$

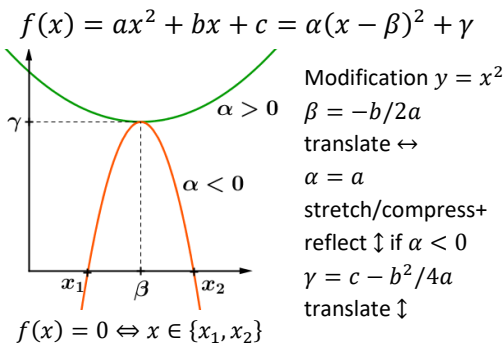
The domain of the variable(s) could be $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ or something else. It will affect what techniques to use, and if it is an easy or hard problem to solve. Diophantine equations with integer coefficients and solutions often lead to difficult and deep problems. The most interesting question is often if there is a solution and if so, how many. Approximating solutions with numerical methods is not unimportant. It's essential for applied mathematics in science and engineering.

To solve equations there are several techniques that need to be mastered. One is to apply identities (algebraic, trigonometric, etc.) that transform either side to a simpler or more suitable form.

Completing the square:



$$x^2 + px + q \equiv \left(x + \frac{p}{2}\right)^2 - \frac{p^2}{4} + q$$



- Modification $y = x^2$
- $\beta = -b/2a$
- translate \Leftrightarrow
- $\alpha = a$
- stretch/compress+
- reflect \Downarrow if $\alpha < 0$
- $\gamma = c - b^2/4a$
- translate \Downarrow

Another technique is variable substitution, divide and conquer. Solve a problem by dividing it into easier steps. For $x^2 + px + q = 0$ it could mean:

$$y = x + \frac{p}{2} \wedge r = \frac{p^2}{4} - q \rightarrow y^2 - r = 0$$

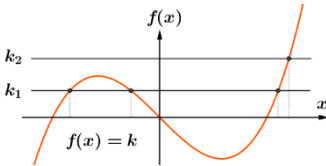
Applying a bijective function on both sides $f(L(x)) = f(R(x))$ will not alter the solution set. Doing it several times may give x alone on one side and a solution but care must be taken if f is only bijective on a limited domain D_f .

$f_\alpha(x) = x + \alpha$	$f_\alpha^{-1}(x) = x - \alpha$
$g_\beta(x) = \beta \cdot x \ (\beta \neq 0)$	$g_\beta^{-1}(x) = x/\beta$
$h_\gamma(x) = x^\gamma \ (\gamma \neq 0)$	$h_\gamma^{-1}(x) = x^{1/\gamma}$
$f(x) = e^x$	$f^{-1}(x) = \ln x$
$g(x) = \sin x \ (x \in [-\frac{\pi}{2}, \frac{\pi}{2}])$	$g^{-1}(x) = \arcsin x$
$bx - a = 0 \ (b \neq 0)$	$x = (g_{1/b} \circ f_a)(0) = \frac{a}{b}$

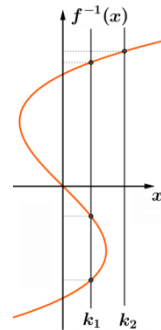
Applying non-injective functions (many-to-one) like $f(x) = x^2$ can lead to extraneous solutions that should be checked and discarded if necessary.

$$x = 1 \Rightarrow x^2 = 1^2 \Leftrightarrow \sqrt{x^2} = 1 \Leftrightarrow |x| = 1 \Leftrightarrow x \in \{-1, 1\}.$$

The “opposite” situation $f(x) = k$ where f is a non-injective function can lead to multiple solutions. The inverse of f if it existed would be a multi-valued function.



$$\begin{aligned} y^2 = r &\rightarrow y = \pm\sqrt{r} \rightarrow \\ x = -p/2 \pm \sqrt{p^2/4 - q} \\ &= \frac{1}{2}(-p \pm \sqrt{p^2 - 4q}) \end{aligned}$$



Multiplying with an expression $k(x)$, say an LCD to get rid of denominators can introduce extraneous solutions when $k(x_i) = 0$ and dividing with $k(x)$ can remove solutions when $k(x_i) = 0$, $k(x)q(x) = k(x) \neq q(x) = 1$. It is better to factorize than to divide, $k(x)(q(x) - 1) = 0$. If $h(x) = f(x)g(x)$ then $h(x) = 0$ whenever $x \in D_f \cap D_g$ and $f(x) = 0$ or $g(x) = 0$.

Imagine a culture that only recognizes integers as valid numbers. For them the equation $bx - a = 0 \ (a, b \in \mathbb{Z})$ is only solvable when $b|a$. There is an alternative, they could introduce a/b but it would require a leap of faith. Number systems can sometimes be extended with new numbers with partially preserved properties embedded among the old numbers.

$$\begin{aligned} x + 1 = 0 &\rightarrow \mathbb{N} \sim \mathbb{Z} \\ 2x = 1 &\rightarrow \mathbb{Z} \sim \mathbb{Q} \\ x^2 = 2 &\rightarrow \mathbb{Q} \sim \mathbb{R} \\ x^2 = -1 &\rightarrow \mathbb{R} \sim \mathbb{C} \end{aligned}$$

If $x^2 = -1$ has a solution, call it i or $\sqrt{-1}$ then it can't belong to \mathbb{R} since the order relation on \mathbb{R} requires $x^2 \geq 0$ (see p.97). An extended numbers system containing the real numbers, an imaginary unit i and operations for addition and multiplication must also contain the set $\mathbf{C} = \{a + b \cdot i \mid (a, b) \in \mathbb{R}^2\}$. The rules of arithmetic from page 79 suggests the following:

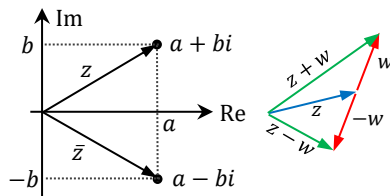
- Addition: $(a + bi) + (c + di) := (a + c) + (b + d)i$
- Multiplication: $(a + bi) \cdot (c + di) := (ac - bd) + (ad + bc)i$
- Additive identity: $0 + 0i \equiv 0$
- Multiplicative identity: $1 + 0i \equiv 1$
- Additive inverse: $-(a + bi) = (-a) + (-b)i \equiv -a - bi$
- Multiplicative inverse: $(a + bi)^{-1} = (a^2 + b^2)^{-1} \cdot (a - bi) \quad a + bi \neq 0$

complex numbers form a field $\mathbb{C} = (\mathbf{C}, +, \cdot, 0, 1)$ (check it!) with a natural embedding of the real numbers $a + 0i \equiv a$. (Pure imaginaries $0 + bi \equiv bi$). An alternative approach without reference to $i^2 = -1$ is to set $\mathbf{C} = \mathbb{R}^2$ with $(a, b) + (c, d) \equiv (a + c, b + d)$ and $(a, b) \cdot (c, d) \equiv (ac - bd, ad + bc)$.

• Complex plane

It is natural to look at the complex numbers as part of a 2-dimensional plane.

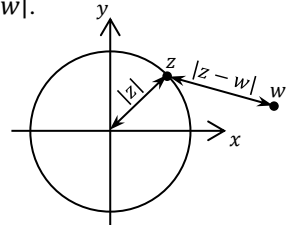
- Complex number: $z = a + bi, a, b \in \mathbb{R}$
- Real part: $a = \text{Re}(z) = \Re(z) = (z + \bar{z})/2$
- Imaginary part: $b = \text{Im}(z) = \Im(z) = (z - \bar{z})/2i$
- Conjugate: $\bar{z} = a - bi$



• Order

\mathbb{C} has no linear order compatible with its field operations (p.79.3). It can be ordered lexically and in other ways but of more interest is the norm $|z|$ that turns \mathbb{C} into a metric space with distance $d(z, w) = |z - w|$.

- $z = x + iy$
 - $|z| = \sqrt{x^2 + y^2}$
 - $|z|^2 = z \cdot \bar{z}$
1. $d(z, w) \geq 0$
 2. $d(z, w) = 0 \iff z = w$
 3. $d(z, w) = d(w, z)$
 4. $d(z, w) \leq d(z, v) + d(v, w)$



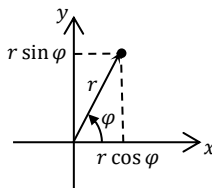
• Polar form

Complex numbers are defined by their absolute value r and argument φ .

$$z = \underbrace{r \cos \varphi}_x + i \cdot \underbrace{r \sin \varphi}_y$$

$$r = |z|$$

$$\varphi = \arg(z)$$



The argument φ (phase) is undefined for $z = 0$ and given up to a multiple of 2π by: $\cos \varphi = x/r$ and $\sin \varphi = y/r$. $\varphi \in (-\pi, \pi]$ is the natural choice.

- Exponential form

Taylor series of $\cos x$, $\sin x$ and e^x are absolutely convergent for complex as well as real arguments. Their domains can be expanded to all of \mathbb{C} .

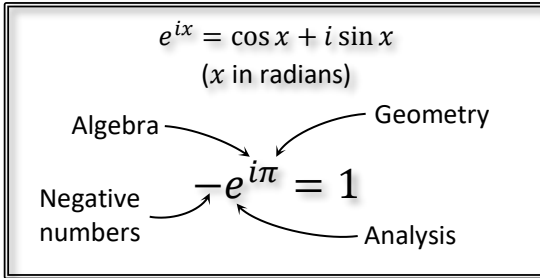
$$\cos z = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} z^{2n} \quad \sin z = \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} z^{2n+1} \quad e^z = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

$$i^n = (1, i, -1, -i) \text{ for } n \equiv (0, 1, 2, 3) \pmod{4} \rightarrow re^{i\varphi} = r(\cos \varphi + i \sin \varphi)$$

Complex trigonometric identities become easy to learn, $e^z \cdot e^w = e^{z+w} \rightarrow$

$$\begin{aligned} \cos(\alpha \pm \beta) &= \operatorname{Re}\{(\cos \alpha + i \sin \alpha)(\cos \beta \pm i \sin \beta)\} \\ \sin(\alpha \pm \beta) &= \operatorname{Im}\{(\cos \alpha + i \sin \alpha)(\cos \beta \pm i \sin \beta)\} \end{aligned}$$

It was Leonhard Euler who used complex analysis and power series to link trigonometric functions to the complex exponential function. His work was preceded by others who studied complex logarithms. The famous formula below was published in 1748. It is now known as Euler's formula.



Whenever there is a vote for the most beautiful formula in mathematics, this is the favorite. It brings together in a surprising and unifying way, constants and concepts from different times and branches that used to be separate.

- Multiplication, division, powers and roots

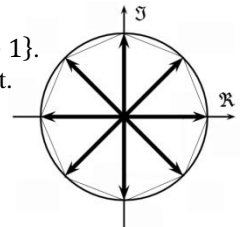
$$\begin{aligned} z \cdot w &= r_z e^{i\varphi_z} \cdot r_w e^{i\varphi_w} = r_z r_w e^{i(\varphi_z + \varphi_w)} && \text{multiply/divide magnitudes} \\ z/w &= r_z e^{i\varphi_z} / r_w e^{i\varphi_w} = r_z/r_w e^{i(\varphi_z - \varphi_w)} && \text{and add/subtract arguments.} \\ z^n &= [r(\cos \varphi + i \sin \varphi)]^n = r^n (\cos n\varphi + i \sin n\varphi) && \text{De Moivre's formula} \end{aligned}$$

$\omega^n = 1$ has n roots of unity, $\omega_k = e^{ik \cdot \frac{2\pi}{n}}$, $k \in \{0, 1, \dots, n-1\}$.

For a general LHS, $\omega^n = z$ there is no natural choice of root.

$\sqrt[n]{z}$ with $z = r e^{i\varphi}$ is a multi-valued function,

$$\sqrt[n]{z} = \sqrt[n]{r} \cdot e^{i(\varphi/n + k \cdot 2\pi/n)}, \quad k \in \{0, 1, \dots, n-1\}.$$

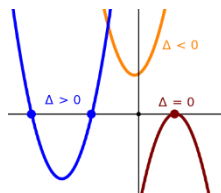


- Quadratic equation

The solution is found by completing the square, not by looking up formulas.

$$\begin{array}{llll}
 az^2 + bz + c = 0 & \Delta > 0 & z_{1,2} = (-b \pm \sqrt{\Delta})/2a & \text{Two real roots} \\
 a, b, c \in \mathbb{R} & \Delta = 0 & z_1 = -b/2a & \text{Real double root} \\
 \Delta = b^2 - 4ac & \Delta < 0 & z_{1,2} = (-b \pm i\sqrt{-\Delta})/2a & \text{Complex conjugates} \\
 a, b, c \in \mathbb{C} & \rightarrow & z = (-b + \Delta^{1/2})/2a &
 \end{array}$$

Quadratic polynomials $P_2(z) = az^2 + bz + c$ have two roots unless the discriminant $\Delta \equiv b^2 - 4ac = 0$. If so the root act as a double root $P(z) = a(z - z_1)^2$. With real coefficients the roots are either real or a conjugate pair (z_1, z_2) with $z_2 = \bar{z}_1$.



Methods for solving quadratic equations were known by Babylonian mathematicians as early as 2000 BC. Cubic and quartic equations were solved by Italian mathematicians in the 16th century. The formulas are long and not very useful. Despite centuries of efforts by many mathematicians, no general solution could be found for equations of degree five. A general solution is a formula of the coefficients that finds a root with a finite number of basic arithmetical operations and root extractions. Proofs of the non-existence of such a formula were given by Ruffini in 1799 (incomplete) and by Abel in 1824 (complete).

Definition.

A **polynomial function over** \mathbb{S} (a set such as $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ or \mathbb{C}) is a function $f: \mathbb{S} \rightarrow \mathbb{S}, x \mapsto a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ($a_n \neq 0$ if $n > 0$) with $n \in \mathbb{N}_0$ and **coefficients** $a_0, a_1, \dots, a_n \in \mathbb{S}$.

If $a_n \neq 0$ then n is the **degree** of the polynomial, $\deg(f) = n$.

$f = 0 \Rightarrow \deg(f)$ is undefined, -1 or $-\infty$. Conventions vary.

The shorter term polynomial is often used which can cause confusion with polynomials in algebra, a similar but slightly different concept.

Definition.

A **polynomial ring** $K[X]$ is a set of expressions P called **polynomials**

$$P = p_0 + p_1 X + p_2 X^2 + \dots + p_n X^n$$

with coefficients p_k in a ring K (usually a field F like \mathbb{Q}, \mathbb{R} or \mathbb{C})

and formal symbols X for which $X^0 = 1, X^1 = X$ and $X^k X^l = X^{k+l}$.

The setting of the polynomial matters. A polynomial like $x^2 - 2$ is prime when viewed over \mathbb{Q} but factorized over $\mathbb{R}, (x + \sqrt{2})(x - \sqrt{2})$. Polynomials will be assumed to be functions over \mathbb{R} or \mathbb{C} for the rest of this chapter. Polynomial rings will be treated in a later chapter on algebra.

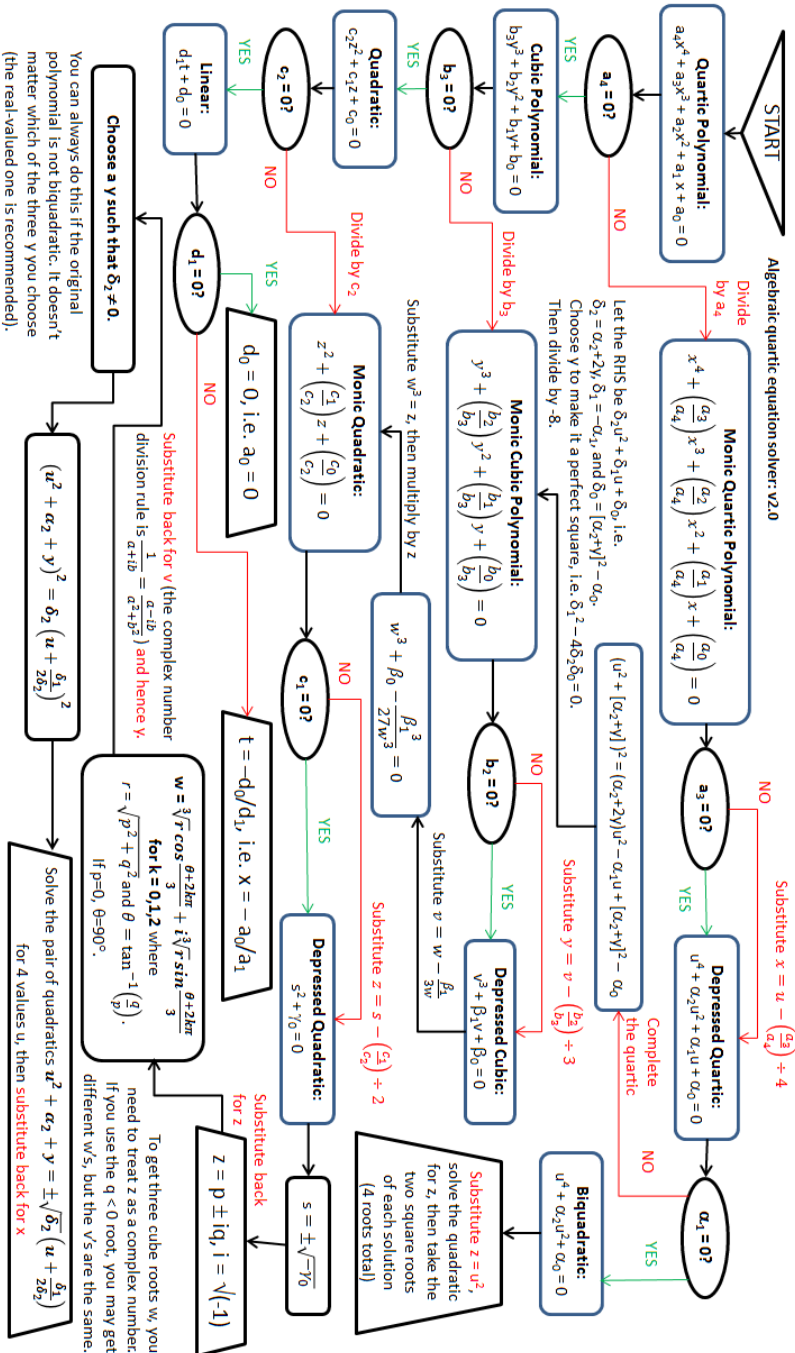


Fig. 3.5.1 How to find the roots of cubic and quartic polynomials

Integers and polynomials share many properties. They are both rings with all the familiar properties of addition and multiplication. Euclidean division of integers with quotient and remainder, $a = bq + r$ with $0 \leq r < |b|$, ($b \neq 0$), divisibility and the Euclidean algorithm can be generalized to polynomials if modulus, $|n|$ for integers is replaced by the degree, $\deg(f)$ for polynomials.

Theorem 10. (The division algorithm)

Let f and $g \neq 0$ be two polynomials then there is polynomials q and r s.t. $f = gq + r$, $0 \leq \deg(r) < \deg(g)$ or $r = 0$ ($f/g = q + r/g$)

Proof

q and r are found by polynomial long division, best described by a concrete example. Let $f = 2x^4 - 3x^2 + 7x - 6$ and $g = x^2 - 2x - 1$.

$$\begin{array}{r}
 \begin{array}{l} \square \\ \searrow \\ g \end{array} \quad \begin{array}{l} \square \\ \searrow \\ q \end{array} \\
 \hline
 x^2 - 2x - 1 \quad \left| \begin{array}{r} 2x^2 + 4x + 7 \\ 2x^4 + 0x^3 - 3x^2 + 7x - 6 \leftarrow f \\ \hline 2x^4 - 4x^3 - 2x^2 \\ \hline 4x^3 - x^2 + 7x \\ 4x^3 - 8x^2 - 4x \\ \hline 7x^2 + 11x - 6 \\ 7x^2 - 14x - 7 \\ \hline 25x + 1 \leftarrow r \end{array}
 \end{array}$$

$$\frac{2x^4 - 3x^2 + 7x - 6}{x^2 - 2x - 1} = 2x^2 + 4x + 7 + \frac{25x + 1}{x^2 - 2x - 1}$$

If f and g were polynomials over a field \mathbb{F} then so would q and r be since their coefficients are obtained by adding, subtracting, multiplying and all divisions are by the leading coefficient of g which is non-zero. ■

Definition.

The polynomial f is a **divisor** of the polynomial g iff there is a polynomial k such that $g = fk$. It is written $f|g$

Definition.

A polynomial k is a **greatest common divisor** GCD of two polynomials (not both zero-polynomials) iff k is a common divisor of f and g and there is no other common divisor of higher degree. The GCD is written (f, g)

(f, g) is uniquely defined up to a multiplicative constant. A natural choice is to use the unit as the coefficient of the highest degree. Polynomials are called coprime or relatively prime when $(f, g) = 1$.

Lagrange interpolation

$P(x) = (x - x_1)(x - x_2) \dots (x - x_n)$ passes through $(x_i, 0)$ for $i=1,2, \dots n$.

Is there a polynomial that passes through $(x_i, y_i)_{i=1}^n$ with $x_i \neq x_j$ if $i \neq j$?

$$l_k(x) = \prod_{i=1, i \neq k}^n \frac{(x - x_i)}{x_k - x_i} \text{ makes } l_k(x_m) = \begin{cases} 0 & \text{if } m = k \\ 1 & \text{if } m \neq k \end{cases} \quad (\text{Lagrange basis})$$

$$L(x) = \sum_{k=1}^n y_k l_k(x) \text{ is of degree } n - 1 \text{ and passes through } (x_i, y_i)_{i=1}^n$$

Definition. Let $f \neq 0$ be a polynomial. If $(z - \alpha)^k | f(z)$ but $(z - \alpha)^{k+1} \nmid f(z)$ then the root α is of **multiplicity** k .

This can also be expressed as $f(z) = (z - \alpha)^k g(z)$ for some polynomial g such that $g(\alpha) \neq 0$. Quadratic roots of multiplicity 2 has zero slope at the root. It suggests a definition based on derivation $D \sum_{i=0}^n a_i z^i = \sum_{i=1}^n i a_i z^{i-1}$. For a multiplicity k root: $D^{(i)} f(\alpha) = 0, i = 0, 1, \dots, k-1$ and $D^{(k)} f(\alpha) \neq 0$. Roots with $k = 1$ are called simple, $k = 2$ are double roots and $k > 1$ are multiple roots. $z^3 - z^2 = z^2(z - 1)$ has a simple root 1, and a double root 0. Counted with multiplicity there are 3 roots.

How many roots can a polynomial $P(z) = a_n z^n + \dots + a_1 z + a_0$ of degree n have if roots of multiplicity k are counted k times? Clearly not more than n , that would give a divisor of degree bigger than n . If $a_k \in \mathbb{R}$ and only real roots are counted then there can be fewer, $(x^2 + 1)^k$ has no real roots.

Theorem 12.

If P is a polynomial over \mathbb{R} with root $c = a + bi$ ($b \neq 0$) then $\bar{c} = a - bi$ is also a root and of the same multiplicity. Complex roots come in pairs c, \bar{c} .

Proof.

$$a_k \in \mathbb{R} \implies P(\bar{c}) = \overline{P(c)} = \bar{0} = 0,$$

divide with $(z - c)(z - \bar{c})$ and repeat if necessary.

Definition.

A field \mathbb{F} is **algebraically closed** if every non-constant polynomial in $\mathbb{F}[X]$ has at least one root in \mathbb{F} .

Theorem 13. (Fundamental theorem of algebra)

\mathbb{C} is an algebraically closed field.

Corollary. (A.k.a fundamental theorem of algebra)

Every polynomial f over \mathbb{C} of degree $n \geq 1$ has exactly n roots in \mathbb{C} if they are counted according to their multiplicity.

Proof. (Corollary, complex polynomials of degree n has n roots)

The corollary follows from assuming the existence of one root and induction over the degree. If $n = 1$ then $f(z) = az + b$, $a \neq 0$ with root $-b/a$.

F.T.A $\Rightarrow f(z) = (z - c)g(z)$ with $c \in \mathbb{C}$ and g of degree $n - 1$ and the same number of roots by assumption so $f(z)$ has n roots counted with multiplicity. ■

The fundamental theorem of algebra depends on the completeness of the real numbers which is a concept from analysis so ironically despite its name there is no purely algebraic proof of the fundamental theory of algebra.

Proof. (Every complex non-constant polynomial has at least one root)

Let $z_{R,\varphi} = Re^{i\varphi}$ then $0 \leq \varphi < 2\pi$ will parametrize one counter-clockwise lap around $z = 0$ at radius R .

Let $P(z) = a_n z^n + \dots + a_1 z + a_0$, $a_n, a_0 \neq 0$ then $P(z_{R,\varphi})$ will trace out a closed curve in the complex plane. $a_n = r e^{i\alpha} \rightarrow a_n z_{R,\varphi}^n = r R^n e^{i(n\varphi + \alpha)}$.

For R large enough $|a_n z^n| \gg |a_{n-1} z^{n-1} + \dots + a_1 z + a_0|$

$P(z_{R,\varphi})$ will loop around the origin n times, winding number $+n$.

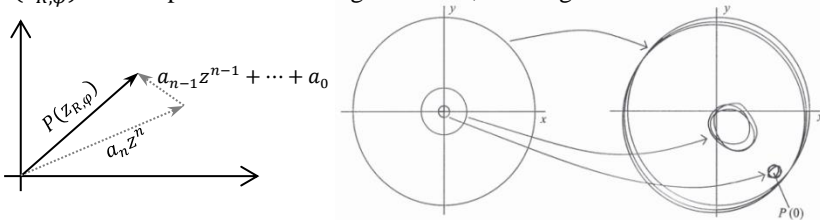


Fig. 3.5.2 Polynomial function in the complex plane.

As $R \rightarrow 0$ the image $P(z_{R,\varphi})$ will close in around $P(0) = a_0$ and for small enough R it is contained in a disc outside 0. ($a_0 = 0$ gives a trivial root)

During the shrinking the loops must cross the origin and then $P(z) = 0$.

If it never happened we could remove $z = 0$ and have a violation of winding number invariance around the origin, of a continuous deformation of a closed curve in a plane with the origin removed.

A general polynomial of degree n in $\mathbb{C}[X]$ with complex roots c_1, \dots, c_n can be factored into polynomials of degree one.

$$\frac{P(z)}{a_n} = (z - c_1) \dots (z - c_n)$$

A general polynomial of degree n in $\mathbb{R}[X]$ has real roots $(r_i)_{i=1}^j$ $j \geq 0$ and complex roots that come in conjugate pairs $(c_i, \bar{c}_i)_{i=1}^k$ $k \geq 0$, $n = j + 2k$. It can be factored into polynomials of degree one and two.

$$\frac{P(x)}{a_n} = (x - r_1) \dots (x - r_j)(x^2 - 2\text{Re } c_1 + |c_1|^2) \dots (x^2 - 2\text{Re } c_k + |c_k|^2)$$

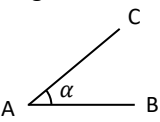

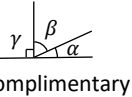
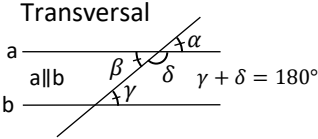
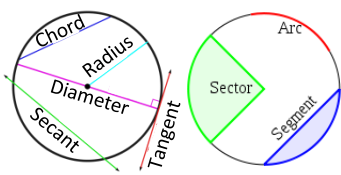
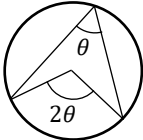
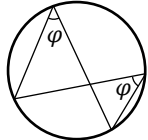
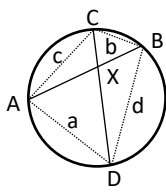
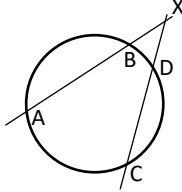
3.6 Geometry

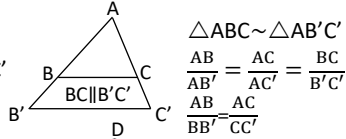
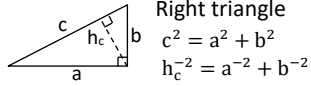
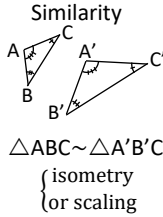
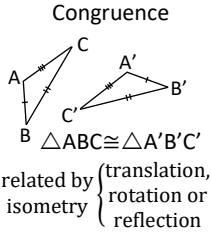
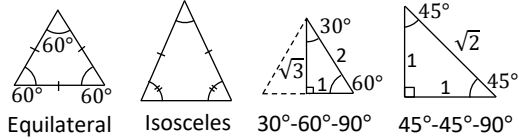
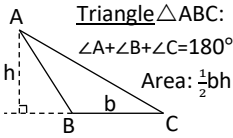
Geometry divides broadly into synthetic geometry and analytic geometry. Synthetic geometry, sometimes called axiomatic or pure geometry is the study of geometry without coordinates or formulas. The axiomatic form with primitives, axioms, rigorous deduction (synthesis) and construction with ruler and compass is described in Euclid's *Elementa*. With Descartes' introduction of coordinates came a new development that could take advantage of algebra and other analytic methods. The two branches are complementary; insights gained with one method can stimulate progress in the other branch.

School geometry starts with practical geometry, the kind of geometry that got mathematics started in most ancient civilizations. Practical geometry was intended for concrete applications, it contains terminology for geometric concepts and formulas for calculations of lengths, areas and volumes.

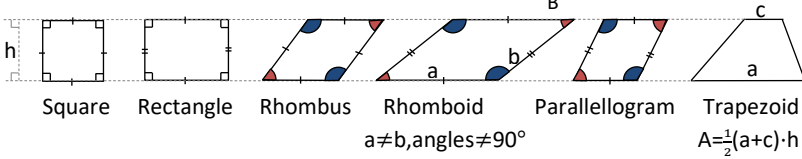
Practical Geometry

as a formula sheet

<p><u>Angles</u></p>  <p style="margin-left: 100px;">$\alpha: \angle BAC$</p> <p>Acute angle: $\alpha < 90^\circ$ Obtuse angle: $\beta > 90^\circ$ Straight angle: $\gamma = 180^\circ$</p>  <p>Right angle: $\gamma = 90^\circ$ Complimentary angles: $\alpha + \beta = 90^\circ$</p>  <p>Vertical angles: $\alpha = \beta$ Supplementary angles: $\alpha + \gamma = 180^\circ$</p> <p><u>Transversal</u></p>  <p>Corresponding angles: $\alpha = \gamma$ Alternate angles: $\beta = \gamma$</p>	<p><u>Circles</u></p>     <p style="text-align: center;">$AX \cdot XB = CX \cdot XD$</p>  <p style="text-align: center;">$AX \cdot BX = CX \cdot DX$</p> <p>Cyclic quadrilateral: ADBC Semiperimeter: $s = (a+b+c+d)/2$ Area: $\sqrt{(s-a)(s-b)(s-c)(s-d)}$</p>
---	---



Quadrilateral ABCD:



Diagonal (D), Perimeter (P), Arc (C), Area (A), Inner angle sum (S), Base area (B), Volume (V)

