Chapter 2, continuation of basic material:
sets, functions, sequences, and sums

here:

1. brief review of basic set-related concepts
2. brief mention of functions
3. focus on sequences and sums

1&2 (sets and functions)
if not thoroughly familiar with this material, carefully read Chapter 2

using un-axiomatic treatment: a **set** is an **unordered collection of distinct objects**

A is the set of primes less than 13:

$A = \{2,3,5,7,11\}$

$= \{3,7,11,5,2\} = \{2,2,3,5,5,5,7,11\}$

$2, 5 \in A$: 2 and 5 *belong to A*, are *elements* of A

B is the set of non-negative integers at most 100:

$B = \{0, 1, 2, \ldots, 100\}$

note usage of "{", "}" and "…" (*ellipses*)

be unambiguous: $A = \{2, 3, \ldots, 11\}$ is inadequate

Set builder notation:

for propositional function $P(x)$

"$S = \{x \mid P(x)\}$" and "$S = \{x : P(x)\}$"

are both short-hands for

$\forall x\ (x \in S \leftrightarrow P(x))$

$\Rightarrow$ S is the set of **all** x such that $P(x)$ holds (in some implicit domain that is often omitted)

examples:

$A = \{p \mid p \text{ prime and } p < 13\}$

$B = \{n \mid n \text{ integer and } 0 \le n \le 100\}$

$D = \{n \mid n = 2m \text{ for an integer } m\}$ (even integers)

again: always be clear and unambiguous

Common sets

- $\mathbf{N}$ is the set of natural numbers
    - for some $0 \in \mathbf{N}$, others prefer $0 \notin \mathbf{N}$ no big deal, as long as you're clear
    - $B = \mathbf{N}_{\leq 100}$
- $\mathbf{Z}$ is the set of the integers ($D = 2\mathbf{Z}$)
- $\mathbf{Q}$ is the set of the rational numbers
- $\mathbf{R}$ is the set of the real numbers
- $\mathbf{C}$ is the set of the complex numbers

Cardinality of a set S, denoted $|S|$ or $\#S$

$|S| = \#S$ = number of distinct elements of S

$|A| = \#A = 5$

$|B| = \#B = 101$

A and B are examples of *finite* sets

examples of *infinite* sets:

$\#\mathbf{N} = \#\mathbf{Z} = \#\mathbf{Q} = \infty$

$\#\mathbf{R} = \#\mathbf{C} = \infty$

and: $\#\mathbf{N} = \#\mathbf{Z} = \boldsymbol{\#\mathbf{Q} \neq \#\mathbf{R}} = \#\mathbf{C}$

empty set, the set without elements: $\varnothing$ $(=\{\})$

singleton set, a set with a single element

example: $\{\varnothing\}$, set containing the empty set

equality between sets A **and** B:

$A = B$ if and only if $\forall x\,(x \in A \leftrightarrow x \in B)$

subset: set A is subset of set B

if and only if $\forall x\,(x \in A \rightarrow x \in B)$

notation: $A \subseteq B$ (similar: $A \supseteq B \leftrightarrow \forall x\,(x \in B \rightarrow x \in A)$)

proper subset: set A is proper subset of set B

if and only if $A \subseteq B$ and $A \neq B$

notation: $A \subset B$ (careful with $\subseteq$ versus $\subset$)

thm: for every set A: $\varnothing \subseteq A$ and $A \subseteq A$

(prove $\varnothing \subseteq A$ using a vacuous proof)

Power set $P(A)$ of set A: set of all subsets of A

for every set A: $\varnothing \subseteq A$ and $A \subseteq A$,
thus $\varnothing \in P(A)$ and $A \in P(A)$

Let $A = \{1,2,3\}$, then $P(A)=$
$\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$
note: elements of $P(A)$ are (sub)sets, elements of these (sub)sets may again be (sub)sets:

Let $B = \varnothing$, then $P(B) = \{\varnothing\}$, so $P(\varnothing) = \{\varnothing\}$

Let $C = P(\varnothing) = \{\varnothing\}$,
$P(C) = \{\varnothing, \{\varnothing\}\}$, so $P(P(\varnothing)) = \{\varnothing, \{\varnothing\}\}$

Let $D = P(P(\varnothing)) = \{\varnothing, \{\varnothing\}\}$, so $P(D) =$
$P(P(P(\varnothing))) = \{\varnothing,\{\varnothing\},\{\{\varnothing\}\},\{\varnothing,\{\varnothing\}\}\}$

fye, **power set** of $P(P(P(\varnothing))) = \{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$:

$P(P(P(P(\varnothing)))) = \{$

$\varnothing,$

$\{\varnothing\},\ \{\{\varnothing\}\},\ \{\{\{\varnothing\}\}\},\ \{\{\varnothing, \{\varnothing\}\}\},$

$\{\varnothing, \{\varnothing\}\},\ \{\varnothing, \{\{\varnothing\}\}\},\ \{\varnothing, \{\varnothing, \{\varnothing\}\}\},$
$\{\{\varnothing\}, \{\{\varnothing\}\}\},\ \{\{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},$
$\{\{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\},$

$\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}\},\ \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\},$
$\{\varnothing, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\},\ \{\{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\},$

$\{\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\varnothing, \{\varnothing\}\}\}$

$\}$

Cartesian product $A \times B$ of sets A and B:

set of all ordered pairs (a,b), $a \in A$ and $b \in B$:

$$A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$$

example:

$A = \{\mathrm{H,L,S}\}$, $B = \{\mathrm{A,B,L',P}\}$:

$$\begin{aligned} A \times B = \{\ & (\mathrm{H,A}),(\mathrm{H,B}),(\mathrm{H,L'}),(\mathrm{H,P}), \\ & (\mathrm{L,A}),(\mathrm{L,B}),(\mathrm{L,L'}),(\mathrm{L,P}), \\ & (\mathrm{S,A}),(\mathrm{S,B}),(\mathrm{S,L'}),(\mathrm{S,P})\ \} \end{aligned}$$

$$\#(A \times B) = \#A \times \#\, B \ = \ 3 \times 4 = 12,$$

relation from A to B: a subset of $A \times B$

example:

$$\{(\mathrm{H,B}),(\mathrm{H,L'}),(\mathrm{H,P}),(\mathrm{L,P})\} \subset A \times B$$

for sets A, B, C

$$A \times B \times C = \{(a,b,c) \mid a \in A \wedge b \in B \wedge c \in C\}$$

but

$$(A \times B) \times C = \{(d,c) \mid d \in A \times B \wedge c \in C\}$$

Set operations

to create new sets from existing sets (similar to using logical operators to create compound propositions from existing propositions)

complement: $\overline{A} = \{x \mid x \notin A\} = \{x \mid \neg(x \in A)\}$

(always with respect to some universe U)

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

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

(A and B *disjoint* if $A \cap B = \emptyset$)

difference: $A - B = A \backslash B = \{x \mid x \in A \wedge \neg(x \in B)\}$

symmetric difference:

$$A \oplus B = A \,\Delta\, B = \{x \mid x \in A \oplus x \in B\}$$

Note: correspondence with logical operations (and "$\subseteq$" $\leftrightarrow$ "$\rightarrow$")

set operations lead to **set identities** (page 132 (124))
such as

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$ (distributive law)

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

(De Morgan's laws)

…

which can proved

1. with membership tables
2. using **both** $\subseteq$ and $\supseteq$
3. "directly"

example: Prove $\overline{A \cup B} = \overline{A} \cap \overline{B}$

1. with membership table (i.e., truth table for $x \in A$, etc.):

A	B	$A \cup B$	$\overline{A \cup B}$	$\overline{A}$	$\overline{B}$	$\overline{A} \cap \overline{B}$
0	0	0	1	1	1	1
0	1	1	0	1	0	0
1	0	1	0	0	1	0
1	1	1	0	0	0	0

2. using both $\subseteq$ and $\supseteq$, thus proving:

   $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ and $\overline{A \cup B} \supseteq \overline{A} \cap \overline{B}$

3. directly

using $\subseteq$ and $\supseteq$ to prove that $\overline{A \cup B} = \overline{A} \cap \overline{B}$

$\subseteq$: let $x \in \overline{A \cup B}$

$$\rightarrow x \notin A \cup B$$

$$\rightarrow \neg(x \in A \cup B)$$

$$\rightarrow \neg(x \in A \vee x \in B)$$

$$\rightarrow \neg(x \in A) \wedge \neg(x \in B)$$

$$\rightarrow (x \notin A) \wedge (x \notin B)$$

$$\rightarrow x \in \overline{A} \wedge x \in \overline{B}$$

$$\rightarrow x \in \overline{A} \cap \overline{B}$$

it follows that $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$

all "$\rightarrow$" can be replaced by "$\leftrightarrow$" (or "$\equiv$"), from which "$\supseteq$" follows as well

direct proof of $\overline{A \cup B} = \overline{A} \cap \overline{B}$

$$
\begin{aligned}
\overline{A \cup B} &= \{x \mid x \notin A \cup B\} \\
&= \{x \mid \neg(x \in (A \cup B))\} \\
&= \{x \mid \neg(x \in A \vee x \in B)\} \\
&= \{x \mid \neg(x \in A) \wedge \neg(x \in B)\} \\
&= \{x \mid (x \notin A) \wedge (x \notin B)\} \\
&= \{x \mid x \in \overline{A} \wedge x \in \overline{B}\} \\
&= \{x \mid x \in \overline{A} \cap \overline{B}\} \\
&= \overline{A} \cap \overline{B}
\end{aligned}
$$

prove $A \cup (A \cap B) = A$ by showing $\subseteq$ and $\supseteq$

- $A \cup (A \cap B) \subseteq A$:

  if $x \in A \cup (A \cap B)$, then $x \in A$ or $x \in A \cap B$,

  so:

  $x \in A$

  or

  ($x \in A$ and $x \in B$)

  in either case $x \in A$

  it thus follows that $A \cup (A \cap B) \subseteq A$

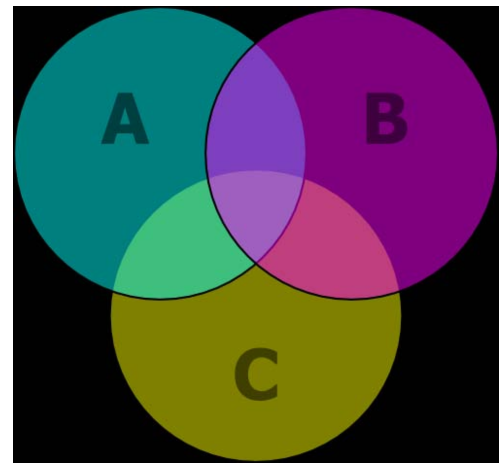
- $A \cup (A \cap B) \supseteq A$:

  if $x \in A$, then $x \in A \cup (A \cap B)$

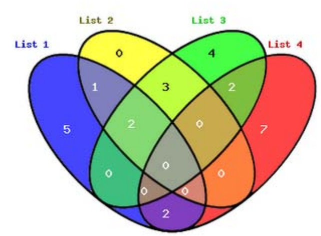
  it thus follows that $A \cup (A \cap B) \supseteq A$

Note on Venn diagrams

- Venn diagrams are pictures of sets, drawn as subsets of some universal set U
- may be used *for pictorial purposes*
  *but **never** for proofs*
- three sets intersecting in all possible ways:

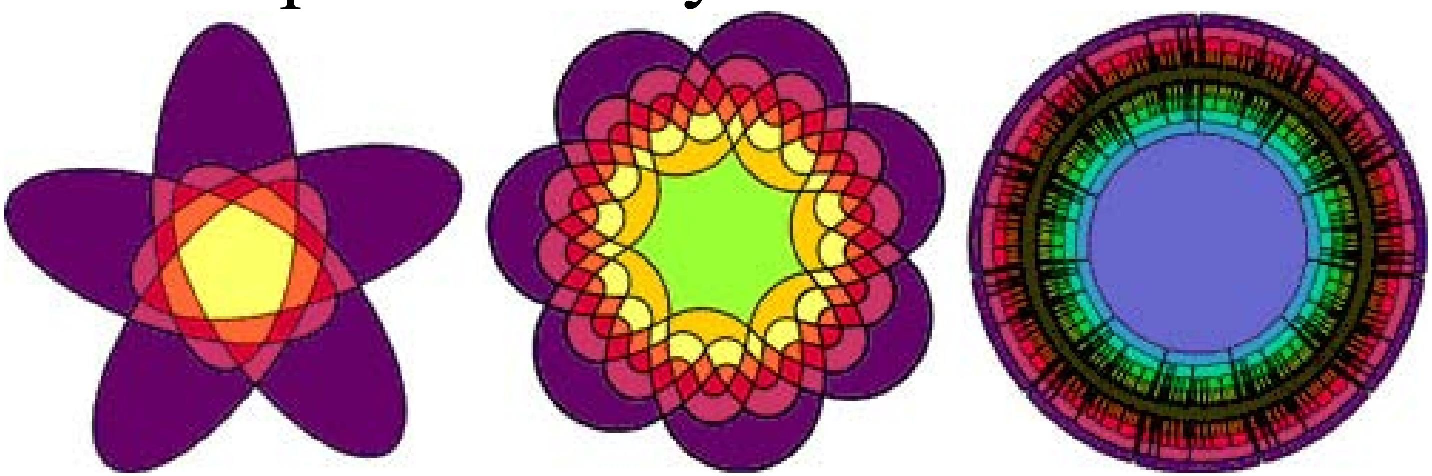


- four sets:



Note on Venn diagrams

- Venn diagrams are pictures of sets, drawn as subsets of some universal set U
- may be used *for pictorial purposes*
  *but **never** for proofs*
- 5, 7, and 11 sets intersecting in all possible ways:



Returning to sets, a note on cardinalities

given **finite** sets A and B, what is $|A \cup B|$?

$|A|$ is the cardinality of A

$|B|$ is the cardinality of B

$|A| + |B|$ is the cardinality of the union $A \cup B$ of A and B, where *all elements that belong to <u>both A and B</u> are counted twice*

thus: $|A| + |B| = |A \cup B| + |A \cap B|$

equivalently: $|A \cup B| = |A| + |B| - |A \cap B|$

known as

the principle of inclusion and exclusion

(and an example of “proof by intimidation”; how to really prove this?)

Inclusion/exclusion example

$A = \{n \in \mathbf{Z} : 0 \le n \le 100, n \text{ multiple of } 5\}$

$\quad = \{n \in \mathbf{Z} : 0 \le n \le 100, 5|n\}$

$B = \{n \in \mathbf{Z} : 0 \le n \le 100, 7|n\}$

$\Rightarrow |A| = 21, |B| = 15$

what is $|A \cup B|$?

$A \cup B = \{n \in \mathbf{Z} : 0 \le n \le 100, 5|n \text{ or } 7|n\}$

$|A| + |B| = 21 + 15 = 36$

counts multiples of **both** 5 **and** 7 twice:

$A \cap B = \{n \in \mathbf{Z} : 0 \le n \le 100, 5|n \text{ and } 7|n\}$

$\quad = \{0, 35, 70\}$

$|A \cup B| = |A| + |B| - |A \cap B| = 21 + 15 - 3 = 33$

more complicated

$A = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 5|n\},\ \ |A| = 21$

$B = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 7|n\},\ \ |B| = 15$

$C = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 3|n\},\ \ |C| = 34$

what is $|A \cup B \cup C|$?

$$|A\cup B\cup C| = |A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|$$

Proof: Let $D = B\cup C$, then

$$\begin{aligned}
|A\cup B\cup C| &= |A\cup D| \\
&= |A|+|D|-|A\cap D| \\
&= |A|+|B\cup C| - |A\cap(B\cup C)| \\
&= |A|+|B|+|C|-|B\cap C| - |(A\cap B)\cup(A\cap C)|
\end{aligned}$$

The result now follows from

$$\begin{aligned}
|(A\cap B)\cup(A\cap C)| &= |A\cap B|+|A\cap C|-|(A\cap B)\cap(A\cap C)| \\
&= |A\cap B|+|A\cap C|-|A\cap B\cap C|
\end{aligned}$$

more complicated

$A = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 5|n\},\ |A| = 21$

$B = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 7|n\},\ |B| = 15$

$C = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 3|n\},\ |C| = 34$

what is $|A \cup B \cup C|$?

$A \cap B = \{0, 35, 70\}: |A \cap B| = 3$

$A \cap C = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 3|n \text{ and } 5|n\}$

$\quad = \{0, 15, 30, 45, 60, 75, 90\}: |A \cap C| = 7$

$B \cap C = \{n \in \mathbf{Z} : 0 \le n \le 100,\ 3|n \text{ and } 7|n\}$

$\quad = \{0, 21, 42, 63, 84\}: |B \cap C| = 5$

$A \cap B \cap C = \{0\}: |A \cap B \cap C| = 1$

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$

$= 21 + 15 + 34 - 3 - 7 - 5 + 1 = 56$

Questions?

Concludes 2nd section of Chapter 2

Functions

given nonempty sets A and B,
a function f from A to B is an assignment of *exactly one* element of B to *each* element of A

What does that mean? Can't we do better?

Functions

first an unusually complicated definition

reminder: a relation from A to B is
an arbitrary subset of $A \times B$

A and B nonempty sets, function f from A to B is:

a relation from A to B
such that $\forall a \in A\ \exists! b \in B\ (a,b) \in f$

thus, *for each element of A* there is
exactly one ordered pair in f whose
first element equals that element of A

note: no limitation on number of pairs in f
in which any $b \in B$ may appear

Functions, more traditionally:

given nonempty sets A and B,
a function f from A to B is an assignment of
exactly one element of B to *each* element of A

we say that f *maps* A *to* B and write:

- $f(a) = b$ (or $(a,b) \in f$ as on previous slide):
  - b is **the** *image* of a
  - a is **a** *preimage* of b
- for any element of B, there may be any number of elements of A mapping to it

function f from A to B

- f: $A \to B$
  (note: same arrow as before, different meaning)
- f goes from *domain* A to *codomain* B
- f has *range* $f(A) = \{b \in B \mid \exists a \in A\ f(a)=b\} \subseteq B$
  $\Rightarrow \forall b \in f(A)\ \exists a \in A\ f(a)=b$,
  a property that does not necessarily hold for B
- for $S \subseteq A$, the *image* of S under f is defined as

$$f(S) = \{b \mid b \in B \text{ and } \exists s \in S\ f(s)=b\}$$
$$= \{f(s) \mid s \in S\} \subseteq f(A)$$

Operations on functions

- sum and product of two functions $f, g: A \to \mathbf{R}$:

  sum: $f+g: A \to \mathbf{R}$: $(f+g)(x) = f(x)+g(x)$

  product: $fg: A \to \mathbf{R}$: $(fg)(x) = f(x)g(x)$

- in general: $f, g: A \to B$ inherit operations on B
- composition of $f: A \to B$ and $g: B \to C$:

$$g \circ f : A \to C : (g \circ f)(x) = g(f(x))$$

Example

f: set of students $\to \mathbf{R}^3$, $g: \mathbf{R}^3 \to \{1, 1.5, 2, 2.5, \ldots, 5, 5.5, 6\}$

$f(\text{Amy}) = (H, M, F)$ is triple of Amy's average homework grade (H), midterm grade (M), and final grade (F)

$g(x,y,z) = [[0.3x+0.2y+0.5z]]$ (with [[.]] rounding to nearest half point)

then $(g \circ f)(\text{Amy})$ is Amy's overall grade

but $(f \circ g)(\text{Anna})$ is not defined

Simple properties of functions

$f\colon A \to \mathbf{R}$

- f is *increasing*:

  $$\forall\, x \in A\ \forall\, y \in A\ \ x > y \to f(x) \geq f(y)$$

- f is *strictly increasing*:

  $$\forall\, x \in A\ \forall\, y \in A\ \ x > y \to f(x) > f(y)$$

- f is *decreasing*:

  $$\forall\, x \in A\ \forall\, y \in A\ \ x > y \to f(x) \leq f(y)$$

- f is *strictly decreasing*:

  $$\forall\, x \in A\ \forall\, y \in A\ \ x > y \to f(x) < f(y)$$

Interesting properties of functions, $f: A \to B$

- f is ***one-to-one*** or ***injective*** or an ***injection***
  iff $\forall a_1, a_2 \in A \;\; f(a_1) = f(a_2) \to a_1 = a_2$
  iff $\forall a_1, a_2 \in A \;\; a_1 \neq a_2 \to f(a_1) \neq f(a_2)$:
  no “collisions”
- f is ***onto*** or ***surjective*** or a ***surjection***
  iff $f(A) = B$
  iff $\forall b \in B \; \exists a \in A \; f(a) = b$:
  everything in B is reached
- f is ***one-to-one correspondence*** or ***bijection***
  iff f is one-to-one and onto
  iff $\forall b \in B \; \exists! a \in A \; f(a) = b$
- injection $f: A \to B$ is bijection $f: A \to f(A)$

inverse of a function

injection $f: A \to B$, thus bijection $f: A \to f(A)$

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

let $g = \{(b,a): b \in f(A), a \in A, f(a) = b\} \subseteq f(A) \times A$

then g is relation $\subseteq f(A) \times A$ such that

$\forall b \in f(A)\ \exists! a \in A\ (b,a) \in g$ (i.e., $g(b) = a$)

where $(b,a) \in g \leftrightarrow f(a) = b$

thus g is a function from $f(A)$ to A such that

$g(b) = a$ if and only if $f(a) = b$

this g is called the ***inverse*** f^{-1} of f:

function $f^{-1}: f(A) \to A$ such that

$f^{-1}(b) = a$ if and only if $f(a) = b$

remarks on inverse

injection f: $A \to B$, bijection f: $A \to f(A)$,
the latter's inverse f^{-1}: $f(A) \to A$
with $f^{-1}(b) = a$ if and only if $f(a) = b$

- $\forall a \in A \quad f^{-1}(f(a)) = a$
  $\Rightarrow f^{-1} \circ f : A \to f(A) \to A$, the *identity* on A
- $\forall b \in f(A) \quad f(f^{-1}(b)) = b$
  $\Rightarrow f \circ f^{-1} : f(A) \to A \to f(A)$, identity on $f(A)$
- it may be the case that f can be computed while computing f^{-1} is *intractable*, or vice versa

examples

f: $\mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^2$ $\quad (f : x \mapsto x^2)$:

- f not injective: $f(1) = f(-1) = 1$
- "same" f: $\mathbf{R}_{\geq 0} \to \mathbf{R}$ is injective
- "same" f: $\mathbf{R}_{\leq 0} \to \mathbf{R}$ is injective too
- f not surjective: $\exists y \in \mathbf{R}\ \forall x \in \mathbf{R}\ f(x) \neq y \quad (y < 0)$
  $\equiv \neg\ (\ \forall y \in \mathbf{R}\ \exists x \in \mathbf{R}\ f(x) = y\ )$
- "same" f: $\mathbf{R} \to \mathbf{R}_{\geq 0}$ is surjective
- "same" f: $\mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$ is bijection
  with inverse f^{-1}: $\mathbf{R}_{\geq 0} \to \mathbf{R}_{\geq 0}$: $f^{-1}(y) = \sqrt{y}$
- or "same" f: $\mathbf{R}_{\leq 0} \to \mathbf{R}_{\geq 0}$ is bijection
  with inverse f^{-1}: $\mathbf{R}_{\geq 0} \to \mathbf{R}_{\leq 0}$: $f^{-1}(y) = -\sqrt{y}$

more examples

- g: $\mathbf{R} \to \mathbf{R}$, $g(x) = x^{2k+1}$ for $k \in \mathbf{N}$ $\left(g : x \mapsto x^{2k+1}\right)$:

  g is injective and surjective, and thus bijective

  example of simple non-trivial bijective correspondence between $\mathbf{R}$ and $\mathbf{R}$

- h: $\mathbf{R} - \{\pi/2 + k\pi : k \in \mathbf{Z}\} \to \mathbf{R}$, $h(x) = \tan(x)$

  h surjective, not injective: $\forall k \in \mathbf{Z}\ h(k\pi) = 0$

  "same" h: $(-\pi/2, \pi/2) \to \mathbf{R}$ (open interval notation!)

  is injective while staying surjective:

  h: $(-\pi/2, \pi/2) \to \mathbf{R}$, $h(x) = \tan(x)$, is bijection

  implies bijection between $(-\pi/2, \pi/2)$ and $\mathbf{R}$

  $\Rightarrow$ arctan $= \tan^{-1}$ is bijection $\mathbf{R} \to (-\pi/2, \pi/2)$

More on cardinalities

sets A and B have by definition the

same cardinality if there is a

bijection between A and B

a set S is **countable** if S is **finite** or has

the same cardinality as N

if S countable and infinite: $|S| = \aleph_0$: "aleph null"

$\Rightarrow$ countability of S implies that S can be

"enumerated": S is finite, or if not

there exists a bijection f: $\mathbf{N} \rightarrow S$,

$S = \{f(i) : i \in \mathbf{N}\} = \{f(0), f(1), f(2), \ldots\}$

a set that is not countable is **uncountable**:

any enumeration will miss (infinitely many) elements

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ are countable

to prove this, establish bijections between

- $\mathbf{N}$ and $\mathbf{N}$:

  the identity map

- $\mathbf{Z}$ and $\mathbf{N}$:

  define $f : \mathbf{Z} \to \mathbf{N}$:

  stretch all "non-negatives" to "even":

  if $z \geq 0$ then $f(z) = 2z$

  fill the odd holes with the negatives:

  if $z < 0$ then $f(z) = -(2z + 1)$

  this f is "obviously" a bijection

  with $f^{-1} : \mathbf{N} \to \mathbf{Z}$, $n \mapsto (-1)^n[(n+1)/2]$

- $\mathbf{Q}$ and $\mathbf{N}$: next slide

More on cardinalities

sets A and B have by definition the

same cardinality if there is a

bijection between A and B

a set S is **countable** if S is **finite** or has

the same cardinality as N

if S countable and **infinite**: $|S| = \aleph_0$: "aleph null"

$\Rightarrow$ countability of S implies that S can be "enumerated": S is finite, or if not

there exists a bijection f: $\mathbf{N} \to S$,

$S = \{f(i) : i \in \mathbf{N}\} = \{f(0), f(1), f(2), \ldots\}$

a set that is not countable is **uncountable**:

any enumeration will miss (infinitely many) elements

$\mathbf{N}$, $\mathbf{Z}$, $\mathbf{Q}$ are countable

to prove this, establish bijections between

- $\mathbf{N}$ and $\mathbf{N}$:

  the identity map

- $\mathbf{Z}$ and $\mathbf{N}$:

  define $f : \mathbf{Z} \to \mathbf{N}$:

  stretch all "non-negatives" to "even":

  if $z \geq 0$ then $f(z) = 2z$

  fill the odd holes with the negatives:

  if $z < 0$ then $f(z) = -(2z + 1)$

  this f is "obviously" a bijection

  with $f^{-1} : \mathbf{N} \to \mathbf{Z},\; n \mapsto (-1)^n[(n+1)/2]$

- $\mathbf{Q}$ and $\mathbf{N}$: next slide

Q is countable – less hand-waving

surjection $\mathbf{N}_{\geq 0} \to \mathbf{Q}_{>0}$ suffices (hold breath at duplicate)

Let $I_k = \{(k-1)k/2, 1+(k-1)k/2, \ldots, k(k+1)/2-1\}$
for $k = 1, 2, 3, \ldots$

then $|I_k| = k(k+1)/2 - 1 - (k-1)k/2 + 1 = k$

$I_1 = \{0\}, I_2 = \{1,2\}, I_3 = \{3,4,5\}, I_4 = \{6,7,8,9\}, \ldots$

$\Rightarrow \bigcup_{k=1}^{\infty} I_k = \mathbf{N}_{\geq 0}$ and $k \neq \ell \to I_k \cap I_\ell = \varnothing$

$\Rightarrow \forall n \in \mathbf{N}_{\geq 0}\ \exists! k\ \ n \in I_k$; denote this k by $k(n)$ $(=[(1+\sqrt{(1+8n)})/2])$

$(k(0)=1, k(1)=k(2)=2, k(3)=k(4)=k(5)=3, k(6)=k(7)=k(8)=k(9)=4)$

define $i(n) = n - (k(n)-1)k(n)/2$: $0 \leq i(n) < k(n)$

$$g : \mathbf{N}_{\geq 0} \to \mathbf{Q}_{>0} \quad n \mapsto \frac{k(n)-i(n)}{i(n)+1} \text{ is surjective}$$

R is uncountable – not too precisely

Proof by contradiction: assume **R** is countable,

implying countability of $\mathbf{R}_1 = \{x \in \mathbf{R}: 0 < x < 1\}$

$\Rightarrow \exists$ bijection $h : \mathbf{N}_{>0} \rightarrow \mathbf{R}_1$:

$h(1) = x_1, h(2) = x_2, \ldots, h(i) = x_i, \ldots$

and $\{x_1, x_2, \ldots, x_i, \ldots\} = \mathbf{R}_1$

$x_i = 0.d_{i1}d_{i2}d_{i3}\ldots d_{ii}\ldots$ is x_i's decimal expansion

for $i = 1, 2, 3, \ldots$, let $\delta_i \neq d_{ii}$, $\delta_i \in \{0,1,\ldots,9\}$

("**Cantor diagonalization argument**")

and let $y = 0.\delta_1\delta_2\delta_3\ldots\delta_i\ldots$

$\Rightarrow y \in \mathbf{R}_1$ and $\forall i \ y \neq x_i$

$\Rightarrow$ contradiction with $\{x_1, x_2, \ldots, x_i, \ldots\} = \mathbf{R}_1$

(un)countability examples

- the set of real numbers with decimal representation consisting of just digits "7" and possibly a single decimal point:
  7,   77, 7.7,   777, 77.7, 7.77,   7777, 777.7, 77.77, 7.777, …
  first list the single one consisting of a single digit, then the two consisting of two digits, followed by the three consisting of three digits, etc. ⇒ countable
- as above, but allow digits 8 as well: use Cantor's diagonalization to show that for any enumeration an element can be found that will not be enumerated by picking 7 if d_{ii}=8 and 8 if d_{ii}=7 (see previous slide) ⇒ uncountable
- the set of all finite length bit strings:
  0,1, 00,01,10,11, 000,001,010,011,100,101,110,111, …
  for k =1, 2, 3, … in succession list the 2^k bit strings of length k (by counting in binary from 0 to 2^k-1 and using leading zeros) ⇒ countable

Special functions

- rounding:
  $\mathbf{R} \to \mathbf{Z}$, $x \mapsto \lfloor x \rceil$, the integer nearest to x
  (halves rounded down; $-\lfloor -x \rceil$ goes up)
- floor:
  $\mathbf{R} \to \mathbf{Z}$, $x \mapsto \lfloor x \rfloor$, the largest integer $\leq x$
- ceiling:
  $\mathbf{R} \to \mathbf{Z}$, $x \mapsto \lceil x \rceil$, the smallest integer $\geq x$
- entier:
  $\mathbf{R}_{\geq 0} \to \mathbf{Z}$, $x \mapsto [x]$, the integer part of x
- factorial:
  $\mathbf{N} \to \mathbf{Z}$, $n \mapsto n!$, with $n! = \prod_{i=1}^{n} i$; **note that 0!=1**

example

$$\lfloor 3x \rfloor = \lfloor x \rfloor + \lfloor x+1/3 \rfloor + \lfloor x+2/3 \rfloor$$

Proof. let $x = n + \varepsilon$, with $n \in \mathbf{Z}$ and $0 \le \varepsilon < 1$
case analysis:

- if $0 \le \varepsilon < 1/3$, then $3x = 3n + \delta$, $0 \le \delta < 1$, $\lfloor 3x \rfloor = 3n$ and $\lfloor x \rfloor = \lfloor x+1/3 \rfloor = \lfloor x+2/3 \rfloor = n$
- if $1/3 \le \varepsilon < 2/3$, then $3x = 3n+1+\delta$, $0 \le \delta < 1$, $\lfloor 3x \rfloor = 3n+1$ and $\lfloor x \rfloor = \lfloor x+1/3 \rfloor = n$,
  but $\lfloor x+2/3 \rfloor = n+1$
- if $2/3 \le \varepsilon < 1$, then $3x = 3n+2+\delta$, $0 \le \delta < 1$, $\lfloor 3x \rfloor = 3n+2$ and $\lfloor x \rfloor = n$,
  but $\lfloor x+1/3 \rfloor = \lfloor x+2/3 \rfloor = n+1$

Another example

$\lceil 2x \rceil = \lceil x \rceil + \lceil x - ½ \rceil$

normally, one takes $x = m - \varepsilon$, with $0 \leq \varepsilon < 1$

instead, let $x = n + \varepsilon$, with $n \in \mathbf{Z}$ and $0 < \varepsilon \leq 1$,

then $\lceil x \rceil = n + 1$

- if $0 < \varepsilon \leq ½$, then $2x = 2n + 2\varepsilon$ with $0 < 2\varepsilon \leq 1$,
  so $\lceil 2x \rceil = 2n + 1$;
  $\lceil x - ½ \rceil = n$ then implies $\lceil 2x \rceil = \lceil x \rceil + \lceil x - ½ \rceil$
- if $½ < \varepsilon \leq 1$, then $2x = 2n + 2\varepsilon$ with $1 < 2\varepsilon \leq 2$,
  so $\lceil 2x \rceil = 2n + 2$;
  $\lceil x - ½ \rceil = n+1$ then implies $\lceil 2x \rceil = \lceil x \rceil + \lceil x - ½ \rceil$

Any questions?

Concludes 3rd section of Chapter 2

Introduction to sequences and summations

informally:
a sequence is a possibly infinite ordered list with a first, a second, a third, a fourth, … element

slightly more formally:

a sequence is a function f from a subset of the set of natural numbers (with or without 0) to some other set S:

$$a_1, a_2, a_3, \ldots \in S$$

or

$$a_0, a_1, a_2, \ldots \in S$$

where $a_i = f(i)$

common sequences

- 0, 1, 2, 3, 4, …
  sequence of natural numbers, $n_i = i,\ i \geq 0$
- 0, 2, 4, 6, 8, …
  sequence of even numbers ≥ 0, $m_i = 2i$, $i \geq 0$
- 1, 1, 2, 6, 24, 120, 720,…
  sequence of factorials, $f_i = i!$, $i \geq 0$
- 2, 3, 5, 7, 11, 13, 17, 19, …
  sequence of primes, p_i is ith prime, $i \geq 1$
- 0, 1, 1, 2, 3, 5, 8, 13, 21,…
  Fibonacci sequence:
  $F_i = i$ for $i = 0, 1$, $\quad F_i = F_{i-2} + F_{i-1}$ for $i \geq 2$

crazy sequences

- 2, 2, 3, 3, 4, 4, 5, 5, 5, 5, 5, 6, …

  $b_i =$ bitlength of p_i, $i \geq 1$
- 4, 3, 3, 5, 4, 4, 3, 5, 5, 4, 3, 6, …

  (in French: 4, 2, 4, 5, 6, 4, 3, 4, 4, 4, 3, 4, …)
- 5, 6, 5, 6, 5, 5, 7, 6, 5, 5, 8, 7, …

  (in French: 7, 8, 9, 9, 9, 7, 8, 8, 8, 7, 7, 8, ...)
- given an integer sequence
  (such as 171, 277, 367, 561, 567, 18881,…),
  how to find *what* it is?

  encyclopedia of integer sequences

  http://oeis.org/

Remarks on sequences

sequences do not necessarily consist of integers:

- $x_i = 1/i$ ($i>0$)
- $y_i = r^i$ for $r \in \mathbf{R}$

sequences are not necessarily infinite:

- s_i = ith SD student (lexicographically or sciper-wise)

sequences are not necessarily well understood

- 3, 5, 17, 257, 65537, …, primes $2^{2^i}+1$ (are there more than five *Fermat primes*?)
- 3, 5, 7, 11, 13, 17, 19, 29, 31, 41, 43, … (are there infinitely many twin primes?)
- primes 123456789101112131415…: any?

Common sequences

arithmetic progression: a sequence of the form

$a, a+d, a+2d, a+3d, \ldots, a+kd, \ldots$ for $a, d \in \mathbf{R}$

with *initial term a* and *common difference d*:

ith term a_i equals $a+id$ $\quad (\forall i{>}0\ a_i - a_{i-1} = d)$

geometric progression: a sequence of the form

$g, gr, gr^2, gr^3, \ldots, gr^k, \ldots$ for $g, r \in \mathbf{R}$

with *initial term g* and *common ratio r*.

ith term g_i equals gr^i $\quad (\forall i{>}0\ g_i/g_{i-1} = r)$

Often needed: summations of sequences

- sum of elements of arithmetic progression

  $a, a+d, a+2d, a+3d, \ldots , a+kd$
- sum of elements of geometric progression

  $g, gr, gr^2, gr^3, \ldots , gr^k,$
- and sums of elements of similar sequences

for $a_i = a+id$ determine $a_0 + a_1 + \ldots + a_k = \sum_{i=0}^{k} a_i$

for $g_i = gr^i$ determine $g_0 + g_1 + \ldots + g_k = \sum_{i=0}^{k} g_i$

$\Rightarrow$ **need to be familiar with methods to calculate such sums**

Sum of an arithmetic progression

$$a_i = a + id, \text{ then } a_0 + a_1 + a_2 + \ldots + a_k = \sum_{i=0}^{k} a_i$$

$$= \sum_{i=0}^{k} (a + id) = \sum_{i=0}^{k} a + \sum_{i=0}^{k} id$$

$$= (k+1)a + d\sum_{i=0}^{k} i$$

here we use:

$$= (k+1)a + d\,\frac{k(k+1)}{2} = (k+1)(a + \frac{dk}{2})$$

$$\sum_{i=1}^{k} i = \left(\sum_{i=1}^{k} i + \sum_{i=1}^{k} i\right)/2$$

let $j=k+1-i$, thus $i=k+1-j$; $j=k$ when $i=1$ and $j=1$ when $i=k$; thus

$$\sum_{i=1}^{k} i = \left(\sum_{i=1}^{k} i + \sum_{j=1}^{k} (k+1-j)\right)/2$$

$$= \left(\sum_{j=1}^{k} j + \sum_{j=1}^{k} (k+1-j)\right)/2 = \left(\sum_{j=1}^{k} (j + (k+1-j))\right)/2$$

$$= \left(\sum_{j=1}^{k} (k+1)\right)/2 = \frac{k(k+1)}{2}$$

Often needed: summations of sequences

- sum of elements of arithmetic progression

  $a, a+d, a+2d, a+3d, \ldots, a+kd$:

  for $a_i = a+id$ determine $a_0 + a_1 + \ldots + a_k = \sum_{i=0}^{k} a_i$

- sum of elements of geometric progression

  $g, gr, gr^2, gr^3, \ldots, gr^m$:

  for $g_j = gr^j$ determine $g_0 + g_1 + \ldots + g_m = \sum_{j=0}^{m} g_j$

- sums of elements of related progression

  $r, 2r^2, 3r^3, 4r^4, \ldots, nr^n$:

  for $t_\ell = \ell r^\ell$ determine $t_1 + t_2 + \ldots + t_n = \sum_{\ell=1}^{n} t_\ell$

$\Rightarrow$ **need to be familiar with those sums and with the methods to calculate them**

Sum of a geometric progression, I

$g_i = gr^i$, then $g_0 + g_1 + g_2 + \ldots + g_k = \sum_{i=0}^{k} g_i = \sum_{i=0}^{k} gr^i = g\sum_{i=0}^{k} r^i$

let $S = \sum_{i=0}^{k} r^i$; if $r = 0$ then $S = 1$

assume $r \neq 0$, then $S = r\sum_{i=0}^{k} r^{i-1}$, thus $S/r = \sum_{i=0}^{k} r^{i-1} = 1/r + \sum_{i=1}^{k} r^{i-1}$

let $i - 1 = j$, then $j = 0$ if $i = 1$, and $j = k - 1$ if $i = k$, thus

$$S/r = 1/r + \sum_{j=0}^{k-1} r^j = 1/r + \left(\sum_{j=0}^{k} r^j\right) - r^k = 1/r + S - r^k$$

with $r \neq 0$ it follows that $S = 1 + rS - r^{k+1}$ and thus, if $r \neq 1$, that

$$S = \frac{r^{k+1} - 1}{r - 1}$$ (also valid for $r = 0$; if $r = 1$, then $S = k + 1$)

note : for $0 \leq r < 1$ it follows that $\sum_{i=0}^{\infty} r^i = \frac{1}{1-r}$

Sum of a geometric progression, II

another way to compute $S=\sum_{i=0}^{k} r^i$

let $f(X)=1+X+X^2+\ldots+X^k$ (then $f(r)=S$)

$Xf(X)= \quad X+X^2+\ldots+X^k+X^{k+1}$

thus $Xf(X)-f(X)=X^{k+1}-1$ and $f(X)=\dfrac{X^{k+1}-1}{X-1}$ (if $X\neq 1$)

cleaner (without dots) : $f(X)=\sum_{i=0}^{k} X^i$, then

$$(X-1)f(X)=(X-1)\sum_{i=0}^{k} X^i = X\sum_{i=0}^{k} X^i - \sum_{i=0}^{k} X^i$$

$$=\sum_{i=0}^{k} X^{i+1} - \sum_{i=0}^{k} X^i = \sum_{j=1}^{k+1} X^j - \sum_{i=0}^{k} X^i = \sum_{i=1}^{k+1} X^i - \sum_{i=0}^{k} X^i$$

$$= X^{k+1} + \sum_{i=1}^{k} X^i - X^0 - \sum_{i=1}^{k} X^i = X^{k+1}-1$$

Sum of an arithmetic progression

$$a_i = a + id, \text{ then } a_0 + a_1 + a_2 + \ldots + a_k = \sum_{i=0}^{k} a_i$$

$$= \sum_{i=0}^{k}(a+id) = \sum_{i=0}^{k} a + \sum_{i=0}^{k} id$$

$$= (k+1)a + d\sum_{i=0}^{k} i$$

here we use:

$$= (k+1)a + d\,\frac{k(k+1)}{2} = (k+1)(a + \frac{dk}{2})$$

$$\sum_{i=1}^{k} i = \left(\sum_{i=1}^{k} i + \sum_{i=1}^{k} i\right)/2$$

let j=k+1–i, thus i=k+1–j; j=k when i=1 and j=1 when i=k; thus

$$\sum_{i=1}^{k} i = \left(\sum_{i=1}^{k} i + \sum_{j=1}^{k}(k+1-j)\right)/2$$

$$= \left(\sum_{j=1}^{k} j + \sum_{j=1}^{k}(k+1-j)\right)/2 = \left(\sum_{j=1}^{k}(j+(k+1-j))\right)/2$$

$$= \left(\sum_{j=1}^{k}(k+1)\right)/2 = \frac{k(k+1)}{2}$$

Similar sum $T(r)=\sum_{i=0}^{k} ir^{i-1}$, determined in two ways (for $r \neq 1$)

1 differentiating $S(r)=\sum_{i=0}^{k} r^{i} = \dfrac{r^{k+1}-1}{r-1}$ leads to $T(r)=S'(r)$:

$$T(r)=S'(r)=\frac{(k+1)r^{k}(r-1)-(r^{k+1}-1)}{(r-1)^{2}}=\frac{kr^{k+1}-(k+1)r^{k}+1}{(r-1)^{2}}$$

2 directly:

$$\begin{aligned}
T(r) &= \sum_{i=1}^{k} ir^{i-1} &&= \sum_{i=1}^{k} r^{i-1}+\sum_{i=1}^{k}(i-1)r^{i-1}\\
&= \sum_{i=0}^{k-1} r^{i}+r\sum_{i=1}^{k}(i-1)r^{i-2} &&= \sum_{i=0}^{k-1} r^{i}+r\sum_{i=0}^{k-1} ir^{i-1}\\
&= \frac{r^{k}-1}{r-1}+r(T(r)-kr^{k-1}) &&\Rightarrow \quad T(r) \text{ follows}
\end{aligned}$$

(page 166/157 : more summations, will be proved later)

Section 2.6/3.8: matrices

- if you're not familiar with matrices: read it
- $k \times m$ rectangles of numbers:
  k rows, m columns
- originally to represent linear
  transformations from $\mathbf{R}^m$ to $\mathbf{R}^k$
- wide variety of applications

Matrix product, traditional computation

$\forall\ k, m, n \in \mathbf{Z}_{>0}$:

$k \times m$ matrix $A = (a_{ij})_{i=1,\ j=1}^{k,\ \ m}$,

$m \times n$ matrix $B = (b_{j\ell})_{j=1,\ell=1}^{m,\ \ n}$,

$AB = C$ is $k \times n$ matrix $C = (c_{i\ell})_{i=1,\ell=1}^{k,\ \ n}$

with $c_{i\ell} = \sum_{j=1}^{m} a_{ij} b_{j\ell}$:

$c_{i\ell}$ is inner product of A's ith row and B's ℓth column

- computation in $k \times m \times n$ multiplications (disregarding additions)
- not commutative: even if AB and BA both defined, they are not necessarily equal

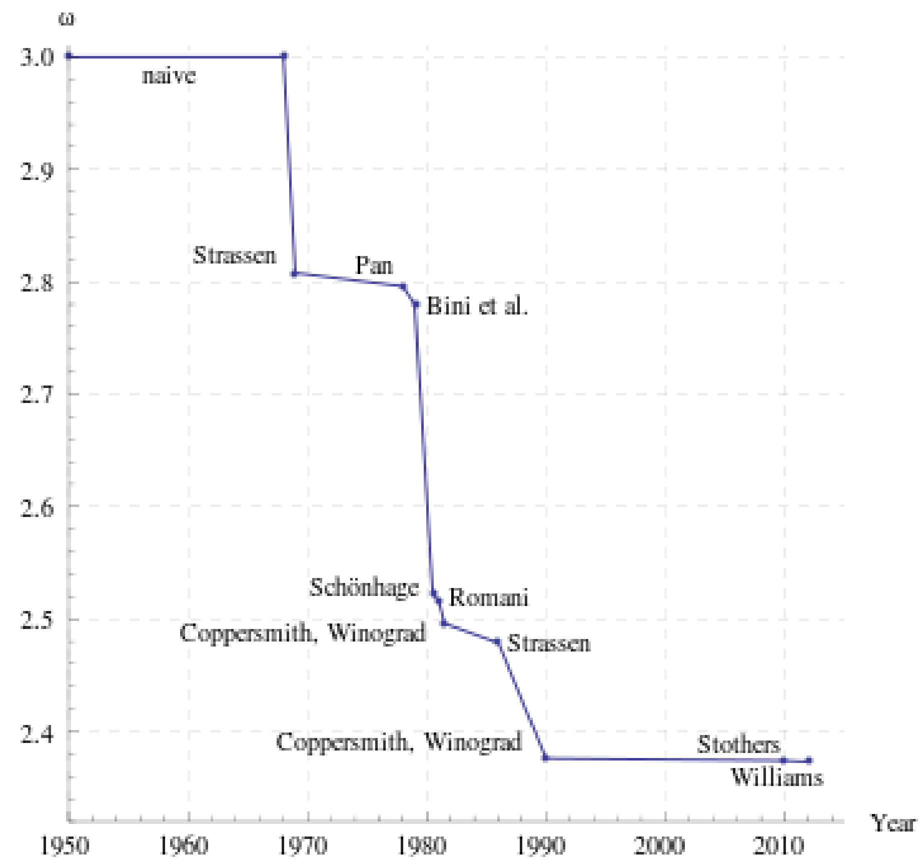
fye, matrix multiplication exponent

- traditional: $n \times n$ matrices A and B, computation of AB in n^3 multiplications
- can it be done faster?

yes, but no one knows how fast:

$\sim n^{2.3727}$ best so far

(compare to integer multiplication...)



(picture shamelessly copied from wikipedia)