Appendix Mathematical Background

Sum Formulas

Each sum of the form

$$\sum_{k=1}^{n} x^{k} = 1^{k} + 2^{k} + 3^{k} + \dots + n^{k},$$

where k is a positive integer has a closed-form formula that is a polynomial of degree k + 1. For example, ¹

$$\sum_{r=1}^{n} x = 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$$

and

$$\sum_{r=1}^{n} x^2 = 1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

An *arithmetic progression* is a sequence of numbers where the difference between any two consecutive numbers is constant. For example,

is an arithmetic progression with constant 4. The sum of an arithmetic progression can be calculated using the formula

$$\underbrace{a + \dots + b}_{n \text{ numbers}} = \frac{n(a+b)}{2}$$

¹There is even a general formula for such sums, called *Faulhaber's formula*, but it is too complex to be presented here.

[©] Springer International Publishing AG, part of Springer Nature 2017

²⁶⁹

where a is the first number, b is the last number, and n is the amount of numbers. For example,

$$3 + 7 + 11 + 15 = \frac{4 \cdot (3 + 15)}{2} = 36.$$

The formula is based on the fact that the sum consists of n numbers and the value of each number is (a + b)/2 on average.

A *geometric progression* is a sequence of numbers where the ratio between any two consecutive numbers is constant. For example,

is a geometric progression with constant 2. The sum of a geometric progression can be calculated using the formula

$$a + ak + ak^2 + \dots + b = \frac{bk - a}{k - 1}$$

where a is the first number, b is the last number, and the ratio between consecutive numbers is k. For example,

$$3+6+12+24=\frac{24\cdot 2-3}{2-1}=45.$$

This formula can be derived as follows. Let

$$S = a + ak + ak^2 + \dots + b.$$

By multiplying both sides by k, we get

$$kS = ak + ak^2 + ak^3 + \dots + bk.$$

and solving the equation

$$kS - S = bk - a$$

yields the formula.

A special case of a sum of a geometric progression is the formula

$$1 + 2 + 4 + 8 + \dots + 2^{n-1} = 2^n - 1.$$

A *harmonic sum* is a sum of the form

$$\sum_{x=1}^{n} \frac{1}{x} = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n}.$$

An upper bound for a harmonic sum is $log_2(n) + 1$. Namely, we can modify each term 1/k so that k becomes the nearest power of two that does not exceed k. For example, when n = 6, we can estimate the sum as follows:

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} \le 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}.$$

$$= k$$
for number n:
$$n = 1 + 2 + 4 + \dots + 2^{N}(k-1) = 2^{N}k - 1$$

This upper bound consists of $\log_2(n) + 1$ parts $(1, 2 \cdot 1/2, 4 \cdot 1/4, \text{ etc.})$, and the value of each part is at most 1.

Sets

A set is a collection of elements. For example, the set

$$X = \{2, 4, 7\}$$

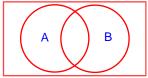
contains elements 2, 4, and 7. The symbol \emptyset denotes an empty set, and |S| denotes the size of a set S, i.e., the number of elements in the set. For example, in the above set, |X| = 3. If a set S contains an element x, we write $x \in S$, and otherwise we write $x \notin S$. For example, in the above set, $4 \in X$ and $5 \notin X$.

New sets can be constructed using set operations:

- The intersection $A \cap B$ consists of elements that are in both A and B. For example, if $A = \{1, 2, 5\}$ and $B = \{2, 4\}$, then $A \cap B = \{2\}$.
- The union $A \cup B$ consists of elements that are in A or B or both. For example, if $A = \{3, 7\}$ and $B = \{2, 3, 8\}$, then $A \cup B = \{2, 3, 7, 8\}$.
- The *complement* \bar{A} consists of elements that are not in A. The interpretation of a complement depends on the *universal set*, which contains all possible elements. For example, if $A = \{1, 2, 5, 7\}$ and the universal set is $\{1, 2, ..., 10\}$, then $\bar{A} = \{3, 4, 6, 8, 9, 10\}$.
- The difference $A \setminus B = A \cap B$ consists of elements that are in A but not in B. Note that B can contain elements that are not in A. For example, if $A = \{2, 3, 7, 8\}$ and $B = \{3, 5, 8\}$, then $A \setminus B = \{2, 7\}$.

If each element of A also belongs to S, we say that A is a *subset* of S, denoted by $A \subset S$. A set S always has $2^{|S|}$ subsets, including the empty set. For example, the subsets of the set $\{2, 4, 7\}$ are how to calculate the number of subset

Some often used sets are \mathbb{N} (natural numbers), \mathbb{Z} (integers), \mathbb{Q} (rational numbers), and \mathbb{R} (real numbers). The set \mathbb{N} can be defined in two ways, depending on the situation: either $\mathbb{N} = \{0, 1, 2, ...\}$ or $\mathbb{N} = \{1, 2, 3, ...\}$.



Appendix A: Mathematical Background

| Table A.1 | Logical op | erators | not | and | or | imply not or | x nor |
|-----------|------------|----------|----------|--------------|------------|-------------------|-----------------------|
| A | В | $\neg A$ | $\neg B$ | $A \wedge B$ | $A \vee B$ | $A \Rightarrow B$ | $A \Leftrightarrow B$ |
| bit 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |

There are several notations for defining sets. For example,

$$A = \{2n : n \in \mathbb{Z}\}$$

consists of all even integers, and

$$B = \{x \in \mathbb{R} : x > 2\}$$

consists of all real numbers that are greater than two.

Logic

The value of a logical expression is either *true* (1) or *false* (0). The most important logical operators are \neg (*negation*), \wedge (*conjunction*), \vee (*disjunction*), \Rightarrow (*implication*), and \Leftrightarrow (*equivalence*). Table A.1 shows the meanings of these operators.

The expression $\neg A$ has the opposite value of A. The expression $A \wedge B$ is true if both A and B are true, and the expression $A \vee B$ is true if A or B or both are true. The expression $A \Rightarrow B$ is true if whenever A is true, also B is true. The expression $A \Leftrightarrow B$ is true if A and B are both true or both false.

A *predicate* is an expression that is true or false depending on its parameters. Predicates are usually denoted by capital letters. For example, we can define a predicate P(x) that is true exactly when x is a prime number. Using this definition, P(7) is true but P(8) is false.

A quantifier connects a logical expression to the elements of a set. The most important quantifiers are \forall (for all) and \exists (there is). For example,

$$\forall x (\exists y (y < x))$$
 min(y)< min(x)

means that for each element x in the set, there is an element y in the set such that y is smaller than x. This is true in the set of integers, but false in the set of natural numbers.

Using the notation described above, we can express many kinds of logical propositions. For example,

$$\forall x((x>1 \land \neg P(x)) \Rightarrow (\exists a(\exists b(a>1 \land b>1 \land x=ab))))$$

means that if a number x is larger than 1 and not a prime number, then there are numbers a and b that are larger than 1 and whose product is x. This proposition is true in the set of integers.

Functions

floor

The function $\lfloor x \rfloor$ rounds the number x down to an integer, and the function $\lceil x \rceil$ rounds the number x up to an integer. For example,

$$|3/2| = 1$$
 and $[3/2] = 2$.

The functions $\min(x_1, x_2, \dots, x_n)$ and $\max(x_1, x_2, \dots, x_n)$ give the smallest and largest of values x_1, x_2, \dots, x_n . For example,

$$min(1, 2, 3) = 1$$
 and $max(1, 2, 3) = 3$.

The factorial n! can be defined by

$$\prod_{x=1}^{n} x = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$$

or recursively

$$0! = 1$$

$$n! = n \cdot (n-1)!$$

The *Fibonacci numbers* arise in many situations. They can be defined recursively as follows:

$$f(0) = 0$$

 $f(1) = 1$
 $f(n) = f(n-1) + f(n-2)$

The first Fibonacci numbers are

There is also a closed-form formula for calculating Fibonacci numbers, which is sometimes called *Binet's formula*:

$$f(n) = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}.$$

Logarithms

The logarithm of a number x is denoted $log_b(x)$, where b is the base of the logarithm. It is defined so that $log_b(x) = a$ exactly when $b^a = x$. The natural logarithm ln(x) of a number x is a logarithm whose base is $e \approx 2.71828$.

A useful property of logarithms is that $\log_b(x)$ equals the number of times we have to divide x by b before we reach the number 1. For example, $\log_2(32) = 5$ because 5 divisions by 2 are needed:

$$32 \rightarrow 16 \rightarrow 8 \rightarrow 4 \rightarrow 2 \rightarrow 1$$

The logarithm of a product is

$$\log_b(xy) = \log_b(x) + \log_b(y),$$

and consequently,

$$\log_b(x^n) = n \cdot \log_b(x).$$

In addition, the logarithm of a quotient is

$$\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y).$$

Another useful formula is

$$\log_u(x) = \frac{\log_b(x)}{\log_b(u)},$$

using which it is possible to calculate logarithms to any base if there is a way to calculate logarithms to some fixed base.

Number Systems

Usually, numbers are written in base 10, which means that the digits $0, 1, \ldots, 9$ are used. However, there are also other number systems, like the base 2 binary system that has only two digits 0 and 1. In general, in a base b system, the integers $0, 1, \ldots, b-1$ are used as digits.

We can convert a base 10 number to base b by dividing the number by b until it becomes zero. The remainders in reverse order correspond to the digits in base b. For example, let us convert the number 17 to base 3:

- 17/3 = 5 (remainder 2)
- 5/3 = 1 (remainder 2)
- 1/3 = 0 (remainder 1)

Thus, the number 17 in base 3 is 122. Then, to convert a base b number to base 10, it suffices to multiply each digit by b^k , where k is the zero-based position of the digit starting from the right, and sum the results together. For example, we can convert the base 3 number 122 back to base 10 as follows:

$$1 \cdot 3^2 + 2 \cdot 3^1 + 2 \cdot 3^0 = 17$$

The number of digits of an integer x in base b can be calculated using the formula $\lfloor \log_b(x) + 1 \rfloor$. For example, $\lfloor \log_3(17) + 1 \rfloor = 3$.