University of Warwick
Department of Computer Science

CS131

Mathematics for Computer Scientists II

Cem Yilmaz

January 14, 2022

Contents

1 Number System

1.1 Binary

Definition 1.1. Binary number system

The binary number system uses the digits $0, 1$ to express itself. In particular the positive integers are represented as:

$$\sum_{i=0}^{n} a2^i \tag{1}$$

where $a \in \mathbb{B}$ and $\mathbb{B} = \{0, 1\}$. Different number systems are usually expressed with subscripts. E.g. 100101_{two}.

1.2 Converting to base n

We can utilise the division algorithm to achieve this. That is, for some base n to convert from base 10 we divide by n to get remainders.

Example 1.1. Division of binary

$$19 \div 2 = 9R1 \tag{2}$$
$$9 \div 2 = 4R1 \tag{3}$$
$$4 \div 2 = 2R0 \tag{4}$$
$$2 \div 2 = 1R0 \tag{5}$$
$$1 \div 2 = 0R1 \tag{6}$$

1.3 The division algorithm

Theorem 1.1. *The division algorithm*

Given any integers $a, b \in \mathbb{Z}$ and $b \neq 0$, there are unique integers $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < |b|$.

1.4 The Euclidean algorithm

The euclidean algorithm utilises the division algorithm to find $gcd(m, n) = b$ where $m, n, b \in \mathbb{Z}$.

Definition 1.2. Greatest Common Divisor

The greatest common divisors of two numbers m, n where $m, n \in \mathbb{Z}$ is the greatest number ζ such that $\zeta \mid m$ and $\zeta \mid n$. It is denoted as $gcd(m, n)$.

Then, through division, observe that $n = mb + r$ In particular, the key observation would be $gcd(r, m) = gcd(n, m) = b$. Repeat this process until one of the numbers reaches 0.

1.5 Modular Arithmetic

Modular arithmetic ensures that the two numbers have the same remainder.

Example 1.2. Modular Arithmetic

The numbers 19 and 21 are congruent to modulo 2. That is, they both have remainder 1.

$$19 \equiv 21 \bmod 2 \tag{7}$$

The notation $a \bmod n$ can also be used as a notation to denote the remainder of the integer a. Furthermore, the modular arithmetic can be subtracted, added and multiplied as usual. In particular,

Example 1.3. Properties of Modular Arithmetic

Consider the following examples

$$x \equiv 3 \bmod n \tag{8}$$
$$y \equiv 5 \bmod n \tag{9}$$
$$x + y \equiv 8 \bmod n \tag{10}$$
$$x \times y \equiv 15 \bmod n \tag{11}$$

Because of these properties, indeed

Corollary. *Power of modular arithmetic*

Then, from multiplication property, the following holds true. If for some integers x, y the property $x \equiv y \bmod n$ holds, then

$$x^k \equiv y^k \bmod n \tag{12}$$

also holds.

1.6 Use of Modular Arithmetic

Let N represent the number of bits used in a system. Then, there are 2^N bits of string length N can be used to represent the numbers in the integer range $[-2^{N-1}, 2^{N-1} - 1]$. In modular arithmetic, the integer x can be then represented as $x \bmod 2^N$. This is two's complement. For example,

Example 1.4. Two's Complement

Table 1: Two's Complement

x	$x \bmod 2^3$	String	x	$x \bmod 2^3$	String
0	0	000	-4	4	100
1	1	001	-3	5	101
2	2	010	-2	6	110
3	3	011	-1	7	111

1.7 Real Numbers

Real numbers consist of every possible numbers that are not complex. There are an infinite amount of real numbers in the interval $[0, 1]$. See CS 130 for this.

1.8 Rational Numbers

A rational number has the form $\frac{m}{n}$ where $m, n \in \mathbb{Z}$ and $n \neq 0$. We can always choose m and n s.t. $n \geq 1$ and $gd(m, n) = 1$.

1.9 Irrational Numbers

An algebraic number is a real number such as $\sqrt{2}$ and $-\sqrt{2}$. It is a solution of a polynomial equation with rational coefficients

Definition 1.3. Transcendental numbers

Transcendental numbers are real numbers which cannot be solutions of polynomial equations with rational coefficients. Examples include π and e.

2 Axioms

2.1 Algebraic Axioms

Axiom 1. Commutativity

It follows that

$$x + y = y + x \land x \times y = y \times x \tag{13}$$

Axiom 2. Associativity

It follows that

$$x + (y + z) = (x + y) + z \land x \times (y \times z) = (x \times y) \times z \tag{14}$$

Axiom 3. Distrubitivity of $\times$ over +

It follows that

$$x \times (y + z) = x \times y + x \times z \tag{15}$$

Axiom 4. Additive Identity

$\exists x . y + x = y$

$$\text{In particular, } x = 0 \tag{16}$$

Axiom 5. Multiplicative Identity

$\exists x . yx = y$

$$\text{In particular, x=1} \qquad dotted \tag{17}$$

Axiom 6. Distinction

Multiplicative and additive identities are distinct. That is,

$$1 \neq 0 \tag{18}$$

So far, all the above axioms hold for $\mathbb{N}$. However, once we add the following axiom:

Axiom 7. Additive Inverse

$\exists - x.x + (-x) = 0$

So far, all above axioms hold for $\mathbb{Z}$. However, once we add the following axiom:

Axiom 8. Multiplicative Inverse

If $x \neq 0$, then $\exists x^{-1}.x \times x^{-1} = 1$

2.2 Ordering Axioms

Axiom 9. Transitivity of ordering

$$x < y \land y < z \implies x < z \tag{19}$$

Axiom 10. The trichotomy law

Exactly one of the following is true:

$$x < y \lor y < x \lor x = y \tag{20}$$

Axiom 11. Preservation of ordering under addition

If $x < y$, then

$$x + z < y + z \tag{21}$$

Axiom 12. Preservation of ordering under multiplication

If $0 < z$ and $x < y$ then

$$x \times z < y \times z \tag{22}$$

So far, all the above axioms hold for $\mathbb{Q}$. However, once we add the following axiom:

Axiom 13. Completeness

Every non-empty subset that is bounded above has a least upper bound.

2.3 Ordering

Definition 2.1. Upper bound

A real number u is an upper bound of S if $u \geq x \; \forall x \in S$

Definition 2.2. Lower bound

A real number u is a lower bound of S if $l \geq x \; \forall x \in S$

Definition 2.3. Supremum

A real number U is supremum of S if U is an upper bound of S and $U \leq u$ for every upper bound u of S. That is, it is the first upper bound.

Definition 2.4. Infimum

A real number L is the infimum of S if L is a lower bound of S and $L \geq l$ for every lower bound l of S. That is, it is the first lower bound.

2.4 Archimedes Property of Real

Theorem 2.1. *Archimedes Property of Reals*

Given any $\varepsilon \in \mathbb{R}^+$, $\exists n \in \mathbb{N}. n\varepsilon > 1$

Proof. Assume $n\varepsilon \leq 1$. Then,

$$\begin{aligned}
& \forall n \text{ that } \{n\varepsilon | n \in \mathbb{N}\} \text{ has an upper bound} && (23)\\
& \text{By completeness it has a least upper bound } l && (24)\\
\implies & \forall n, n\varepsilon \leq l && (25)\\
\implies & (n+1)\varepsilon \leq l && (26)\\
\iff & (n+1)\varepsilon - \varepsilon \leq l - \varepsilon && (27)\\
\iff & n\varepsilon \leq l - \varepsilon && (28)\\
\implies & l - \varepsilon \text{ is also an upper bound} && (29)
\end{aligned}$$

However, this is a contradiction since we already assumed that l is the least upper bound when clearly $l - \varepsilon < l$ □