Logo

Discrete Mathematics

Dr. Han Huang

South China University of Technology


Logo

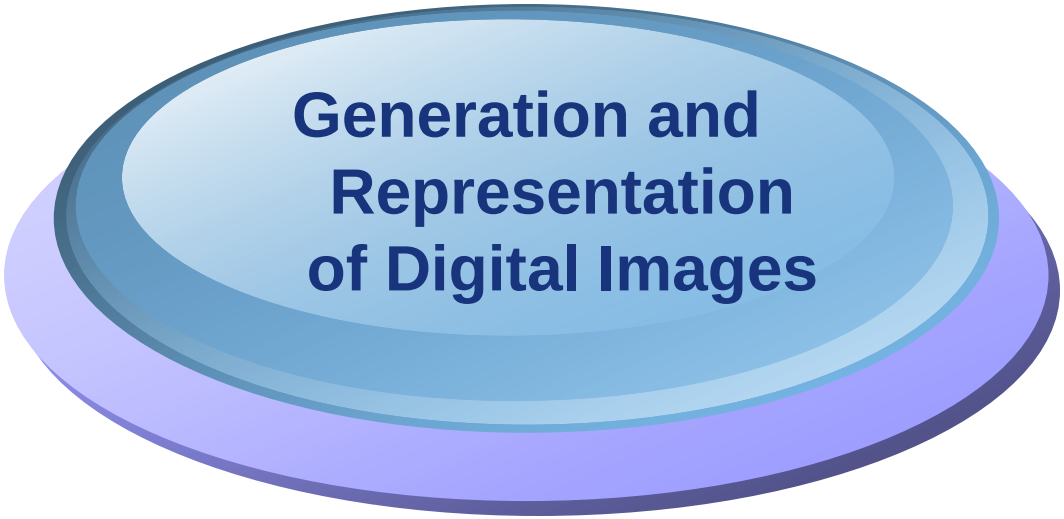
Chapter 2. Set model

Mathematical Modeling and Application

Section 2.3


Logo

Contents

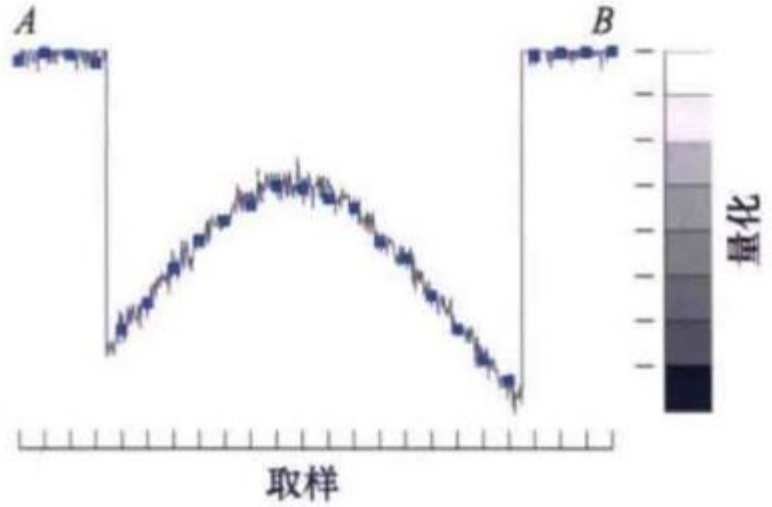

Generation and
Representation
of Digital Images

Introduction

- **Point cloud model** is a representation of 3D image
- Point clouds can usually be obtained by scanning the target with devices such as RGB-depth (RGB-D) cameras and lidar
- **Point cloud registration**， for two frames of overlapping point clouds, by solving the transformation matrix, the overlapping point clouds are transformed to the same unified coordinate system
- A point cloud is a set of points with 3D coordinates in space. At present, the **iterative closest point** algorithm is the most widely used point cloud precise registration algorithm

Modeling

- Images acquired by sensors are sampled at regular intervals from the function. The vertical scale marks provide specific values assigned to brightness intervals, and by aligning each sample with the distance to the vertical scale marks, one of the values can be assigned to quantize the continuous brightness.



Modeling

- We represent an image using the two-dimensional function f: (x, y) → z, where z ∈ R is a scalar, and (x, y) ∈ R × R are spatial coordinates. The image can also be represented as {(x, y, f(x, y)) | (x, y) ∈ R × R}.
- The physical meaning of z is the radiative energy from the physical source, making z non-negative with a value range of $0 \le z < \infty$. The range of values for (x, y) depends on the choice of the origin.
- The sampling function can be represented as:
  - I: (x, y) → (i, j), (i, j) ∈ Z × Z,
- defined as I((x, y)) = (⌊x⌋, ⌊y⌋). The quantization function can be represented as:
  - q: z → a, a ∈ A,
- where A represents the set of brightness intervals. The digital image can be represented as:
  - {(i, j, a) | (i, j) = I(x, y), a = q(f(x, y))}, or f: (i, j) → a.


Representation and
Registration of
Point Clouds

Introduction

- **Point cloud model** is a representation of 3D image
- Point clouds can usually be obtained by scanning the target with devices such as RGB-depth (RGB-D) cameras and lidar
- **Point cloud registration**， for two frames of overlapping point clouds, by solving the transformation matrix, the overlapping point clouds are transformed to the same unified coordinate system
- A point cloud is a set of points with 3D coordinates in space. At present, the **iterative closest point** algorithm is the most widely used point cloud precise registration algorithm

Principle of algorithm

- The closest point in the two point clouds is selected as the corresponding point, the rotation and translation transformation matrix is solved through all the corresponding point pairs, and the registration error between the two point clouds is smaller and smaller through continuous iteration, until it meets the threshold requirements or the number of iterations set in advance.

算法的具体步骤：

(1) 计算源点云中的每一个点在目标点集中的对应近点。

(2) 求得使上述对应点对平均距离最小的刚体变换，并求得平移参数和旋转参数。

(3) 对求得的平移和旋转矩阵进行空间变换，得到新的变换点集。

(4) 如果新的变换点集与参考点集满足两点集的平均距离小于某一给定阈值，或者迭代次数达到设定的最大值，则停止迭代计算，否则新的变换点集作为新的源点云继续迭代，直到达到目标函数的要求。

Modeling

- As shown in the figure, the image before registration is displayed with the target point cloud on top and the source point cloud at the bottom.

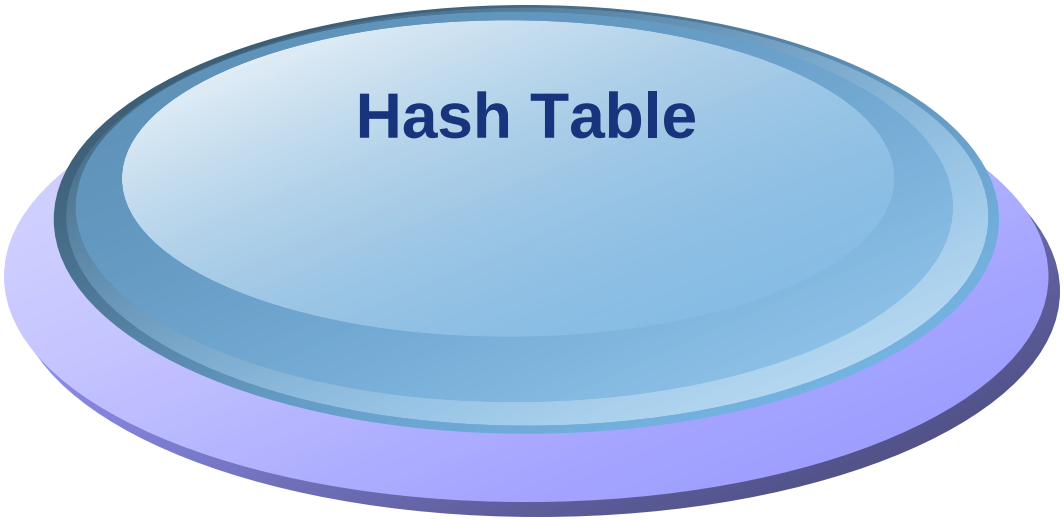
(a) 未配准，红色点云是目标点 (b) 已配准，蓝色是配准结果云，绿色是源点云

Modeling

- As shown in the figure, the image before registration is displayed with the target point cloud on top and the source point cloud at the bottom.

(a) 未配准，红色点云是目标点 (b) 已配准，蓝色是配准结果云，绿色是源点云

- Let Pt denote the target point cloud, Ps represent the source point cloud, and f denote the ICP (Iterative Closest Point) algorithm. Then f is a function and is non-analytic, defined as f: p → q, where p ∈ Ps and q ∈ Pt


Hash Table

Introduction

A hash function/hash function is a way to create small digital "fingerprints" from any kind of data. A hash function compresses a message or data into a digest so that the amount of data is small and the data format is fixed.

Properties of Hash Functions:

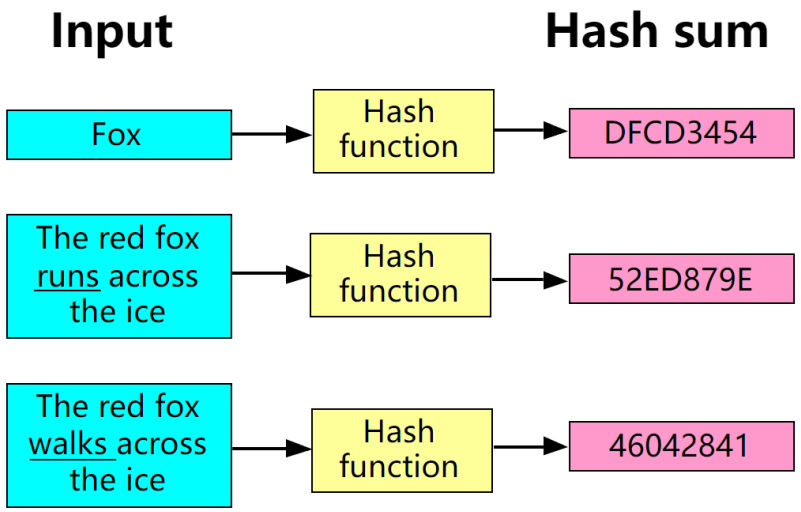
•If two hash outputs are different, then their original inputs are also different.

•Irreversible: It is not possible to obtain the original input from the hash output.

•Strong avalanche effect: A small change in the original input is likely to result in a completely different hash output.

However, there is an exception to property 2, known as hash collisions:

Different inputs may result in the same output (pigeonhole principle). To minimize this, hash function outputs should be as random and uniformly distributed as possible.



Example

Application: Password authentication; File integrity authenticity verification; Tamper proof

Modeling

- Using perfect hashing technique to store the set of keywords *K = {10, 22, 37, 40, 52, 60, 70, 72, 75}*. The outer hash function is h(k) = ((ak + b) mod p) mod m, where a = 3, b = 42, p = 101, m = 9.
- The hash functions for the secondary hash tables are hj(k) = ((ajk + bj) mod p) mod mj, where a0 to a9 are respectively 0, 0, 10, 11, 14, 0, 5, 23, 4, and b0 to b9 are respectively 0, 0, 18, 11, 14, 0, 5, 88, 4, and m0 to m9 are respectively 1, 0, 9, 11, 14, 1, 5, 16, 4.

- **The generation process of this hash table is ?**

Modeling

$$h(10) = ((10 * 3 + 42) mod 101) mod 9 = 0, h_0(10) = ((0 * 10 + 0) mod 101) mod 1 = 0,$$

$$h(22) = ((22 * 3 + 42) mod 101) mod 9 = 7, h_7(22) = ((23 * 22 + 88) mod 101) mod 16 = 9,$$

$$h(37) = ((37 * 3 + 42) mod 101) mod 9 = 7, h_7(37) = ((23 * 37 + 88) mod 101) mod 16 = 14,$$

$$h(40) = ((40 * 3 + 42) mod 101) mod 9 = 7, h_7(40) = ((23 * 40 + 88) mod 101) mod 16 = 7,$$

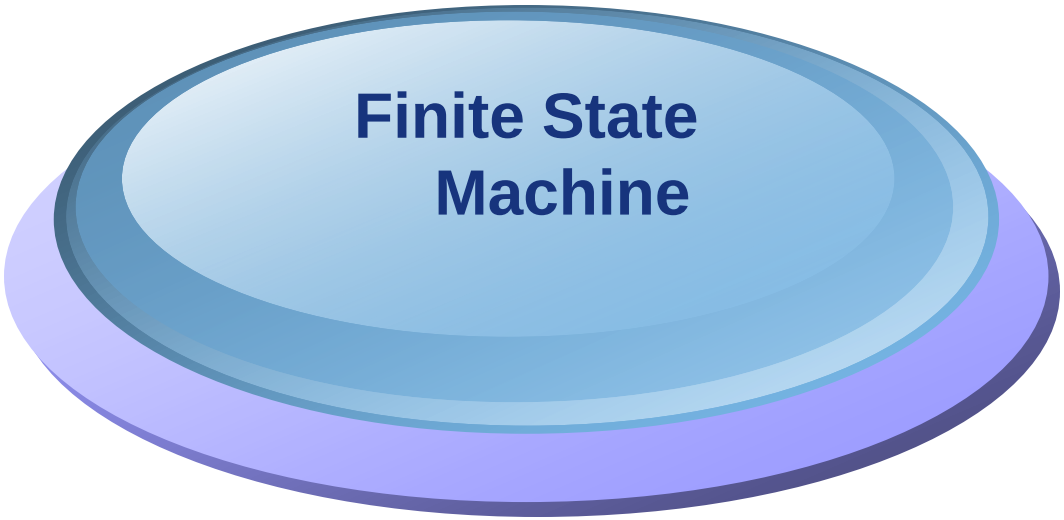
$$h(52) = ((52 * 3 + 42) mod 101) mod 9 = 7, h_7(52) = ((23 * 52 + 88) mod 101) mod 16 = 8,$$

$$h(60) = ((60 * 3 + 42) mod 101) mod 9 = 3, h_3(60) = ((10 * 60 + 18) mod 101) mod 9 = 2,$$

$$h(70) = ((70 * 3 + 42) mod 101) mod 9 = 5, h_5(70) = ((0 * 70 + 0) mod 101) mod 1 = 0,$$

$$h(72) = ((72 * 3 + 42) mod 101) mod 9 = 2, h_2(72) = ((10 * 72 + 18) mod 101) mod 9 = 4,$$

$$h(75) = ((75 * 3 + 42) mod 101) mod 9 = 2, h_2(75) = ((10 * 75 + 18) mod 101) mod 9 = 7,$$


Finite State
Machine

Introduction

- Mathematicians Established the roots of automata in the 20th century, began developing machines that mimicked certain characteristics of humans
- An automaton is an abstract model of a machine that performs computations on inputs by transitioning through a series of states or configurations.
- *An automaton with a finite number of states is called a finite state machine also known as a finite automaton*

Defition

- The formal definition of a finite automaton can be represented by a 5-tuple $M = (Q, \Sigma, \delta, q_0, F)$, where:

- Q —— Non-empty finite set of states. $\forall q \in Q$ is called a state of M.
- Σ ——The input alphabet. All input strings are strings over Σ.
- δ —— The state transition function, $\delta: Q \times \Sigma \rightarrow Q$. For $\forall(q, a) \in Q \times \Sigma$, $\delta(q, a) = p$ means that M, when in state q and reading character a, transitions to state p and awaits the next input.
- q_0 is the initial state, with $q_0 \in Q$.
- F is the set of accepting (or final) states, with $F \subseteq Q$.

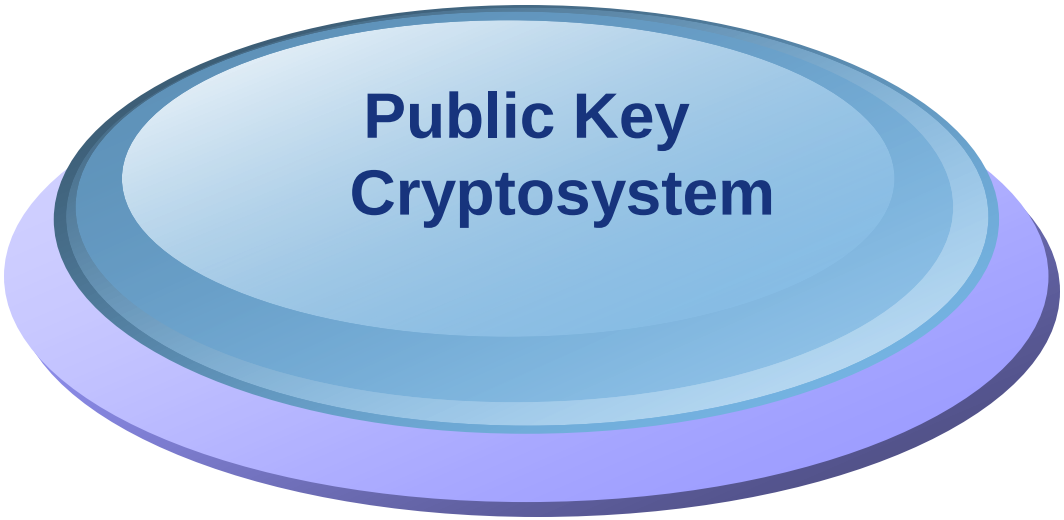
Modeling

- The finite state automaton M has states q0, q1, q2, with the start state as q0 and the accepting state as q2, and the input alphabet is {0}. When the input is 0 and the state is q0, the output is q1. When the input is 0 and the state is q1, the output is q2. When the input is 0 and the state is q2, the output is q1.

Modeling

- The finite state automaton M has states q0, q1, q2, with the start state as q0 and the accepting state as q2, and the input alphabet is {0}. When the input is 0 and the state is q0, the output is q1. When the input is 0 and the state is q1, the output is q2. When the input is 0 and the state is q2, the output is q1.

- The set of states is Q = {q0, q1, q2}, the alphabet set Σ = {0}, and the state transition function is δ(q0, 0) = q1, δ(q1, 0) = q2, δ(q2, 0) = q1. The state machine M = (Q, Σ, δ, q0, {q2}).


Public Key
Cryptosystem

Introduction

- **Public key cryptosystem**, abbreviated as public key encryption system, also known as asymmetric encryption system, the biggest feature is that encryption and decryption use different keys.
- Digital signatures are the foundation of public key infrastructures (PKI) and many network security mechanisms (SSL/TLS, virtual private networks, etc.).
- In a public key encryption system, each participant has a public key and a private key

Modeling

- Let D represent the allowed set of messages. For example, D is the set of all bit sequences of finite length. It is required that the public key and the private key specify a one-to-one correspondence function from D to itself. It should be possible to transform a message M successively using the two keys PA and SA, and still be able to obtain M in the end.

Modeling

- Let D represent the allowed set of messages. For example, D is the set of all bit sequences of finite length. It is required that the public key and the private key specify a one-to-one correspondence function from D to itself. It should be possible to transform a message M successively using the two keys PA and SA, and still be able to obtain M in the end.

- Case Modeling: The function of the public key PA is denoted by PA(), and the function of the private key SA is denoted by SA(). Therefore, both PA() and SA() are permutations of D. Let PA() and SA() be inverse functions of each other. That is, for any message M ∈ D, we have:

$$M = S_A(P_A(M))$$

$$M = P_A(S_A(M))$$

- In either order, after successive transformations of M using the two keys PA and SA, the original message M can still be obtained.


True Positive Rate

Introduction

- Ebola virus a kind of rare virus， for some patients with very low specific antibody titers in acute phase serum, viral antigen or nucleic acid detection should be performed.

- True positive rate (TPR), also known as sensitivity (SEN), is the percentage of patients who are actually sick but are correctly classified as sick according to the criteria of the screening test. It reflects the ability of a screening test to find a patient. It is calculated as,

$$TPR = \frac{TP}{TP + FN},$$

- TP ——the person whose test result says positive,
- FN ——the person who is actually positive, but whose test result says negative

Modeling

- Suppose there are 50 individuals in a certain epidemic area, and antibody testing indicates that 27 people are infected with the virus. Through nucleic acid testing, it was discovered that 3 out of the 27 individuals were not actually infected with the virus, and additionally, there were 4 individuals who were infected but not detected. What is the true positive rate of the antibody test?

Modeling

- Suppose there are 50 individuals in a certain epidemic area, and antibody testing indicates that 27 people are infected with the virus. Through nucleic acid testing, it was discovered that 3 out of the 27 individuals were not actually infected with the virus, and additionally, there were 4 individuals who were infected but not detected. What is the true positive rate of the antibody test?

- Let TP be the set of individuals who tested positive in the antibody test and are indeed infected, with |TP| = 24. Let FN be the set of individuals who tested negative in the antibody test but positive in the nucleic acid test, with |FN| = 4. According to the calculation formula, the true positive rate of the antibody test is 24 / (24 + 4) × 100% = 86%.

Logo

End of Section 2.3