Discrete Mathematics Midterm 2

2017-03-30

- **Statements**: declarative sentences that are either true or false, but not both.
- Non-primitive statements: *negation* (¬, not), *conjunction* (∧, and), *disjunction* (∨, or), *implication* (→, only if), *biconditional* (↔, if and only if).
- Truth table for $\rightarrow$:

p	q	$p \rightarrow q$
0	0	1
0	1	1
1	0	0
1	1	1

- **Logical connectives**: combine two or more statements into a compound statement, e.g. ∧, ∨, →, ↔.
- Proof based on $(p \rightarrow q) \leftrightarrow (\neg q \rightarrow \neg p)$
- Proof by **contradiction**: $(p \rightarrow q) \leftrightarrow (\neg p \vee q) \leftrightarrow \neg(p \wedge \neg q)$
- **Tuple**: an r-tuple is $(a_1, a_2, \ldots, a_r)$, where a_i is the i-th coordinate (component).
- **Cartesian product**: $A_1 \times A_2 \times \ldots \times A_r = \{(a_1, a_2, \ldots, a_r) | a_i \in A_i, 1 \leq i \leq r\}$
- **Ary relation**: a subset of $A_1 \times A_2 \times \ldots \times A_r$ is called an r-ary relation on $A_1, A_2, \ldots, A_r$
- Binary relations can be represented as a *relation matrix* or a *graph*.
- A *binary* relation on A can be ($\forall x, y, z \in A$):
  - **reflexive**: xRx
  - **irreflexive**: $\neg(xRx)$
  - **symmetric**: $(xRy) \rightarrow (yRx)$
  - **asymmetric**: $(xRy) \rightarrow \neg(yRx)$
  - **anti-symmetric**: $(xRy) \wedge (yRx) \rightarrow (x = y)$
  - **transitive**: $(xRy) \wedge (yRz) \rightarrow (xRz)$
- If $(x, y) \in R^k$, there is a path (or cycle as $x = y$) of length k from x to y in the graph representation of R
- Composition of relations:
  - R^0: $\{(x, x) | x \in A\}$, **identity relation**.
  - R^+: $\bigcup_{i=1}^{\infty} R^i$, **transitive closure**.
  - R^*: $\bigcup_{i=0}^{\infty} R^i$, **reflexive transitive closure**.

- $R^+ = R \circ R^* = R^* \circ R$
- $R^* = R^0 \bigcup R^+$
- $R = R^+$ if R is *transitive*.
- $R = R^*$ if R is both *reflexive* and *transitive*.

- **Equivalence relation**: a binary relation R on A is an *equivalence relation* iff it is *reflexive, symmetric and transitive*.
- A subset $E \subseteq A$ is an **equivalence class** with respect to R and A iff:
  - $(xRy) \forall x, y \in E$
  - $\neg(xRy) \forall x \in E, y \in A - E$
- The set of equivalence classes with respect to R and A forms a *partition* of A
- **Minimization** process of a *finite state machine (FSM)*:
  - The concept of FSM is widely used in software design (e.g. compiler design), logic circuit design, probability analysis (e.g. Markov model), etc.
  - An FSM can be represented by a *state table*, where ν denotes a state transition function and ω denotes an output function.
  - *Step 1*: partition the set of states so that s_i and s_j belong to the same subset iff $\omega(s_i, x) = \omega(s_j, x)$, where $x \in \{0, 1\}$
  - *Step 2*: partition each subset so that s_i and s_j belong to the same subset iff $\nu(s_i, x)$ and $\nu(s_j, x)$ fall into the same subset of the current partition, where $x \in \{0, 1\}$
- **Partial ordering**: a relation R on A is called a *partial ordering* iff it is *reflexive, anti-symmetric and transitive*, where A is called a **partially ordered set (poset)**.
- **Hasse diagram**: when A is finite, a *partial ordering* on A can be conveniently represented by an ordering diagram, called **Hasse diagram**.
  - Each element is a *vertex*.
  - A vertex a_i appears below another vertex a_j iff $a_i \preceq a_j$
  - An *edge* connects a_i with a_j iff $a_i \preceq a_j$ and there is no a_k such that $a_i \preceq a_k \preceq a_j$
- [x] Homework: #5-1, #5-2, #5-3, #5-4, #5-5, #5-6, #5-7, #5-8, #5-9
- Solutions: Solutions5.pdf

2017-04-06

- **Lattice**: every two elements of A have upper bounds and lower bounds in A
- **Topological order**: a linear presentation that preserves all *partial ordering*, or descending paths in *Hasse diagram*.
- **Total ordering**: a partial ordering $\prec$ on A is called a total ordering if for all $ai, aj \in A$, either

$ai \preceq aj$ or $aj \preceq ai$. The Hasse diagram for a total ordering is a *chain*.

- Properties of algebra:
  - **Closure** under + and ·: $a + b \in R$ and $a \cdot b \in R$
  - **Complement** for + and ·: $a + a' = 1$ and $a \cdot a' = 0$
  - **Identity** for + and ·: $a + 0 = a$ and $a \cdot 1 = a$.
    - Identity for +: $a + 0 = a$, where 0 is called **zero** or **additive identity**.
    - Identity for ·: $a \cdot 1 = a$, where 1 is called **unity** or **multiplicative identity**.
  - **Inverse** for + and ·: $a + (-a) = 0$ and $a \cdot a^{-1} = 1$.
    - Inverse for +: $a + (-a) = 0$, where a and $-a$ are called **additive inverses**.
    - Inverse for ·: $a \cdot a^{-1} = 1$, where a and a^{-1} are called **multiplicative inverses** or **units**.
  - **Proper divisor of zero**: $a \cdot b = 0$ given $a \neq 0$ and $b \neq 0$
  - **Associativity** of + and ·: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
  - **Commutativity** of + and ·: $a + b = b + a$ and $a \cdot b = b \cdot a$
  - **Distributivity** of + and ·:
    - $a + (b \cdot c) = (a + b) \cdot (a + c)$
    - $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
- Properties of **Boolean algebra** $(K, \cdot, +)$:
  - Closure under + and ·
  - Complement for + and ·
  - Identity for + and ·
  - Associativity of + and ·
  - Commutativity of + and ·
  - Distributivity of + and ·
- **Duals**: $(K, 0, 1, \cdot, +) \leftrightarrow (K, 1, 0, +, \cdot)$
- **Principle of duality**: If S is a theorem about a Boolean algebra, and can be proved, then its dual is likewise a theorem.
- Properties of **Ring** $(R, +, \cdot)$:
  - Closure under + and ·
  - Identity for +
  - Inverse for +
  - Associativity of + and ·
  - Commutativity of +
  - Distributivity of ·
- Ring with *commutativity* of · is called **commutative ring**.

- [x] Homework: #6-1, #6-2, #6-3, #6-4, #6-5, #6-6
- Solutions: [Solutions6.pdf]

2017-04-13

- **Integral domain** is a ring with:
  - Identity for $\cdot$
  - *No* zero divisor $\leftrightarrow$ **The cancellation law of multiplication**
  - Commutativity of $\cdot$
- **Field** is a ring with:
  - Identity for $\cdot$
  - Inverse for $\cdot \rightarrow$ **The cancellation law of multiplication**
  - Commutativity of $\cdot$
- Inverse under $\cdot \rightarrow$ **The cancellation law of multiplication** $\leftrightarrow$ *No* zero divisor.
  - $\mathbb{N}$ and $\mathbb{Z}$ are integral domains, but not fields.
  - $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are both integral domains and fields.
- Theorems of rings, integral domain, and field $(R, +, \cdot)$:
  - The zero z is unique.
  - The additive inverse of each $a \in R$ is unique.
  - **The cancellation law of addition**
  - $-(-a) = a$
  - $a \cdot (-b) = (-a) \cdot b =- (a \cdot b)$
  - $(-a) \cdot (-b) = a \cdot b$
  - If R has a unity u, then it is unique.
  - If x is a unit in ring R, then the multiplicative inverse of x is unique.
  - If x is a unit in ring R, then x cannot be a zero divisor.
  - No zero divisor $\leftrightarrow$ The cancellation law of multiplication
  - Inverse under $\cdot \rightarrow$ The cancellation law of multiplication
  - If $(R, +, \cdot)$ is a field, then it is an integral domain.
  - A finite integral domain $(R, +, \cdot)$ is a field.
- **Subring**: $(S, +, \cdot)$ is said to be a *subring* of a ring $(R, +, \cdot)$ if S is nonempty and $(S, +, \cdot)$ is also a ring.
- Given a ring $(R, +, \cdot)$, a nonempty subset S of R is a subring of R iff:
  - (1) $a + b \in S$ and $a \cdot b \in S$ for all $a, b \in S$, and (2) S is *finite*.
  - (1) $a + b \in S$ and $a \cdot b \in S$ for all $a, b \in S$, and (2) $-a \in S$ for all $a \in S$

- $a + (-b) \in S$ and $a \cdot b \in S$ for all $a, b \in S$
- Integer modulo n: $a \equiv b \pmod{n}$ iff $a - b$ is a multiple of n
- The relation aRb iff $a \equiv b \pmod{n}$ is an *equivalence relation* on $\mathbb{Z}$ and partition $\mathbb{Z}$ into $\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$, where $[i] = \{i + nx | x \in Z\}$
- Theorems of $\mathbb{Z}_n$:
  - For $n \in \mathbb{Z}^+$ and $n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring with unity $[1]$
  - $\mathbb{Z}_n$ is a field iff n is a *prime*.
  - $[a] \in \mathbb{Z}_n$ has a multiplicative inverse iff $\gcd(a, n) = 1$
  - For each integer $0 < a < n$, (1) $\gcd(a, n) = 1 \leftrightarrow [a]^{-1}$ exist, and (2) $\gcd(a, n) > 1 \leftrightarrow [a]$ is a zero divisor of $\mathbb{Z}_n$
- [x] Homework: #7-3, #7-4
- Solutions: Solutions7.pdf

2017-04-20

- The **Chinese remainder theorem**: find all x satisfying $x \equiv a_i \pmod{m_i}$ for all $1 \leq i \leq k$.
  - Define $M = m_1 m_2 \ldots m_{k-1} m_k$
  - Compute $M_i = M/m_i$ for all $1 \leq i \leq k$
  - Find x_i satisfying $M_i x_i \equiv 1 \pmod{m_i}$ for all $1 \leq i \leq k$
  - $[x] = [a_1 M_1 x_1 + \ldots + a_k M_k x_k]$ in $\mathbb{Z}_M$ is the set of solutions.
- A cryptosystem based on the Chinese remainder theorem:
  - Alice generates k relatively prime integers $m_1, m_2, \ldots, m_{k-1}, m_k$ (**decryption keys**)
  - Alice broadcasts M and $e_1, e_2, \ldots, e_{k-1}, e_k$ (**encryption keys**) to Bob as follows:
    - $M = m_1 m_2 \ldots m_{k-1} m_k$
    - $e_i = M_i x_i$ such that $M_i x_i \equiv 1 \pmod{m_i}$ for all $1 \leq i \leq k$
  - Bob *encrypts* p (**plaintext**) with M and e, and then broadcasts C (**ciphertext**) to Alice as follows: $C \equiv p_1 e_1 + \ldots + p_k e_k \pmod{M}$
  - Alice *decrypts* C to get p as follows: $p_i \equiv C \pmod{m_i}$ for all $1 \leq i \leq k$
  - It is extremely time-consuming for Trudy to obtain decryption keys from M
- **Ring homomorphism**: Let $(R, +, \cdot)$ and $(S, \oplus, \odot)$ be two rings. A function $f : R \to S$ is a *ring homomorphism* if $f(a + b) = f(a) \oplus f(b)$ and $f(a \cdot b) = f(a) \odot f(b)$ for all $a, b \in R$
- If $f : (R, +, \cdot) \to (S, \oplus, \odot)$ is a *ring homomorphism*, then
  - $f(z_R) = z_S$ where z_R and z_S are the zeros of R and S
  - $f(-a) = -f(a)$ for any $a \in R$
  - $f(na) = nf(a)$ for any $a \in R$ and $n \in \mathbb{Z}$

  - $f(a^n) = f(a)^n$ for any $a \in R$ and $n \in \mathbb{Z}^+$
  - If A is a subring of R, then $f(A)$ is a subring of S
- **Ring isomorphism**: Let $f : (R, +, \cdot) \to (S, \oplus, \odot)$ be a ring homomorphism. A function $f : R \to S$ is a *ring isomorphism* if f is one-to-one and onto. R and S are said to be two **isomorphic rings**.
- If $f : (R, +, \cdot) \to (S, \oplus, \odot)$ is a *ring homomorphism* and *onto*, then
  - If R has a unity u_R, then $f(u_R)$ is the unity of S
  - If R has a unity u_R and $a^{-1} \in R$, then $f(a^{-1}) = f(a)^{-1}$
  - If R is commutative, then S is commutative.
- $[n_1] \cdot [n_2] \in \mathbb{Z}_M$ can be computed as $f^{-1}f([n_1] \cdot [n_2])$ where
  - $M = m_1 m_2 \ldots m_{k-1} m_k$
  - $f : (\mathbb{Z}_M, +, \cdot) \to (\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k}, \oplus, \odot)$, which is a *ring isomorphism*.
  - $([a_1], \ldots, [a_k]) \oplus ([b_1], \ldots, [b_k]) = ([x_1 + y_1] \in \mathbb{Z}_{m_1}, \ldots, [x_k + y_k] \in \mathbb{Z}_{m_k})$
  - $([a_1], \ldots, [a_k]) \odot ([b_1], \ldots, [b_k]) = ([x_1 \cdot y_1] \in \mathbb{Z}_{m_1}, \ldots, [x_k \cdot y_k] \in \mathbb{Z}_{m_k})$
- [x] Homework: #7-5, #7-6
- Solutions: Solutions7.pdf

2017-04-27

- Properties of **Group** $(G, \cdot)$:
  - Closure under $\cdot$
  - Identity for $\cdot$
  - Inverse for $\cdot$
  - Associativity of $\cdot$
- Goup with commutativity of $\cdot$ is called **abelian group**.
- Given a group, the identity is denoted as $e\ (= a^0)$, and inverse is denoted as a^{-1}
- **Subgroup**: $(H, \cdot)$ is said to be a *subgroup* of a group $(G, \cdot)$ if H is nonempty and $(H, \cdot)$ is also a group.
- Given a group $(G, \cdot)$, a nonempty subset H of G is a subgroup of G iff:
  - (1) $a \cdot b \in H$ for all $a, b \in H$, and (2) H is *finite*.
  - (1) $a \cdot b \in H$ for all $a, b \in H$, and (2) $a^{-1} \in H$ for all $a \in H$
  - $ab^{-1} \in H$ for all $a, b \in H$
- **Group homomorphism**: Let $(G, \cdot)$ and $(H, \odot)$ be two groups. A function $f : R \to S$ is a *group homomorphism* if $f(a \cdot b) = f(a) \odot f(b)$ for all $a, b \in G$
- If $f : (G, \cdot) \to (H, \odot)$ is a *group homomorphism*, then
  - $f(e_G) = e_H$ where e_G and e_H are the identities of G and H

- $f(a^{-1}) = f(a)^{-1}$ for any $a \in G$
  - $f(a^n) = f(a)^n$ for any $a \in G$ and $n \in \mathbb{Z}$
  - If A is a subgroup of G, then $f(A)$ is a subgroup of H
- **Group isomorphism**: Let $f : (G, \cdot) \to (H, \odot)$ be a group homomorphism. A function $f : G \to H$ is a *group isomorphism* if f is one-to-one and onto. G and H are said to be two **isomorphic groups**.
- **Cyclic groups**: A group G is cyclic if there is a **generator** $a \in G$ such that for all $x \in G$, $x = a^k$ for some $k \in \mathbb{Z}$. G is denoted as $\langle a \rangle = \{a^i | i \in \mathbb{Z}\}$
- If G is a group and $a \in G$, the **order** of a, denoted by $o(a)$, is $|\langle a \rangle|$. If $|\langle a \rangle|$ is infinite, we say that a has **infinite order**.
- Theorems of *groups*, and *cyclic groups*:
  - The identity of G is unique.
  - The inverse of each element of G is unique.
  - If $a, b, c \in G$ and $a \cdot b = a \cdot c$, then $b = c$
  - If $a, b, c \in G$ and $b \cdot a = c \cdot a$, then $b = c$
  - G is abelian iff $(ab)^2 = a^2 \cdot b^2$ for all $a, b \in G$
  - Let G be a group. If for some $a \in G$ and $S = \{a^k | k \in Z\}$, then S is a subgroup of G and denoted as $\langle a \rangle$
  - Let a be an element in a group G, and suppose $a^n = e$ for some positive integer n. If m is the least positive integer such that $a^m = e$, then
    - $\langle a \rangle$ has the order m and $\langle a \rangle = \{e, a^1, a^2, \ldots, a^{m-1}\}$
    - $a^s = a^t$ iff $s \equiv t \pmod{m}$
  - If $(G, \cdot)$ is a cyclic group, then G is abelian.
  - Let G be a cyclic group.
    - If G is *infinite*, then G is isomorphic to $(\mathbb{Z}, +)$.
    - If $|G| = n$, then G is isomorphic to $(\mathbb{Z}_n, +)$.
  - Any subgroup of a cyclic group is cyclic.
- Examples of *groups* and *cyclic groups*:
  - Under ordinary addition, each of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ is an *abelian group*, but none of them are groups under multiplication.
  - If $(R, +, \cdot)$ is a ring, then $(R, +)$ is an abelian group, and $(R, \cdot)$ is a semigroup.
  - For each $n \in \mathbb{Z}^+$ and $n > 1$, $(\mathbb{Z}_n, +)$ is an abelian group. If n is a prime number, then $(\mathbb{Z}_n - [0], \cdot)$ is an abelian group.
  - U_n defined as $\{[a] | [a] \in \mathbb{Z}_n, [a]^{-1} \in \mathbb{Z}_n\}$ = $\{[a] | [a] \in \mathbb{Z}_n, \gcd(a, n) = 1\}$ is an abelian group, where $(\mathbb{Z}_n, +, \cdot)$ is a ring.

- $(U_9, \cdot)$ is a cyclic group with two generators [2] and [5].
- $(U_9, \cdot)$ is isomorphic to $(\mathbb{Z}_6, +)$
- The group $(\mathbb{Z}, +)$ is cyclic and denoted as $\langle 1 \rangle$ or $\langle -1 \rangle$.
- $G = \{\pi_0, \pi_1, \pi_2, r_1, r_2, r_3\}$ is not cyclic.

- **Lagrange's theorem**: If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.
- **Coset**: Suppose H is a subgroup of G. For any $a \in G$, the set $a \cdot H = \{a \cdot h | h \in H\}$ is a **left coset**, and $H \cdot a = \{h \cdot a | h \in H\}$ is a **right coset** of H in G.

2017-05-04

- If H is a subgroup of a finite group G, then for any $a, b \in G$,
  - $|aH| = |H|$
  - $|Ha| = |H|$
  - $aH = bH$ or $aH \cap bH = \emptyset$
  - $Ha = Hb$ or $Ha \cap Hb = \emptyset$
- Let H be a subgroup of a finite group G:
  - The distinct left cosets of H in G form a partition of G.
  - The distinct right cosets of H in G form a partition of G.
- If G is finite and $a \in G$, then $o(a)$ divides $|G|$.
- If $|G|$ is prime, then G is cyclic.
- **RSA** cryptosystem:
  - Alice arbitrarily generates two prime integers p, q and calculates $\varphi(pq)$, where φ is the Euler's phi function.
  - Alice arbitrarily generates a pair of e (**encryption key**) and d (**decryption key**) and broadcasts pq and e as follows:
    - e is relatively prime to $\varphi(pq)$.
    - $ed \equiv 1 \pmod{\varphi(pq)}$
  - Bob encrypts L (**plaintext**) with pq and e, and then broadcasts C (**ciphertext**) to Alice as follows: $C \equiv L^e \pmod{pq}$
  - Alice decrypts C to get L as follows: $L \equiv C^d \pmod{pq}$
- [x] Homework: #7-1, #7-2, #8
- Solutions: Solutions7.pdf, Solutions8.pdf