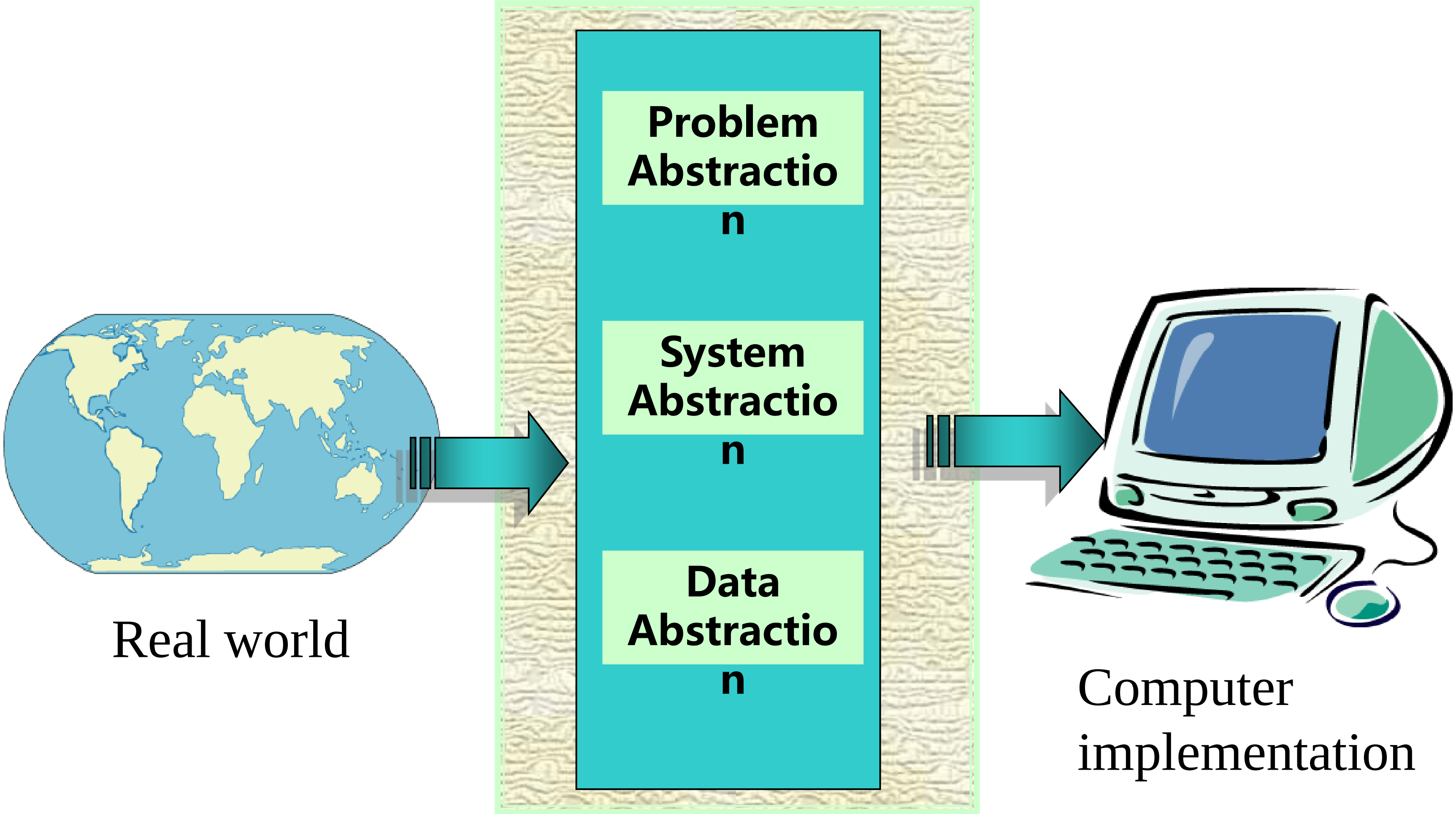
Basic Models and Tools

Lecture 1

Discrete Mathematical Structures

Scenario



Problem Abstraction

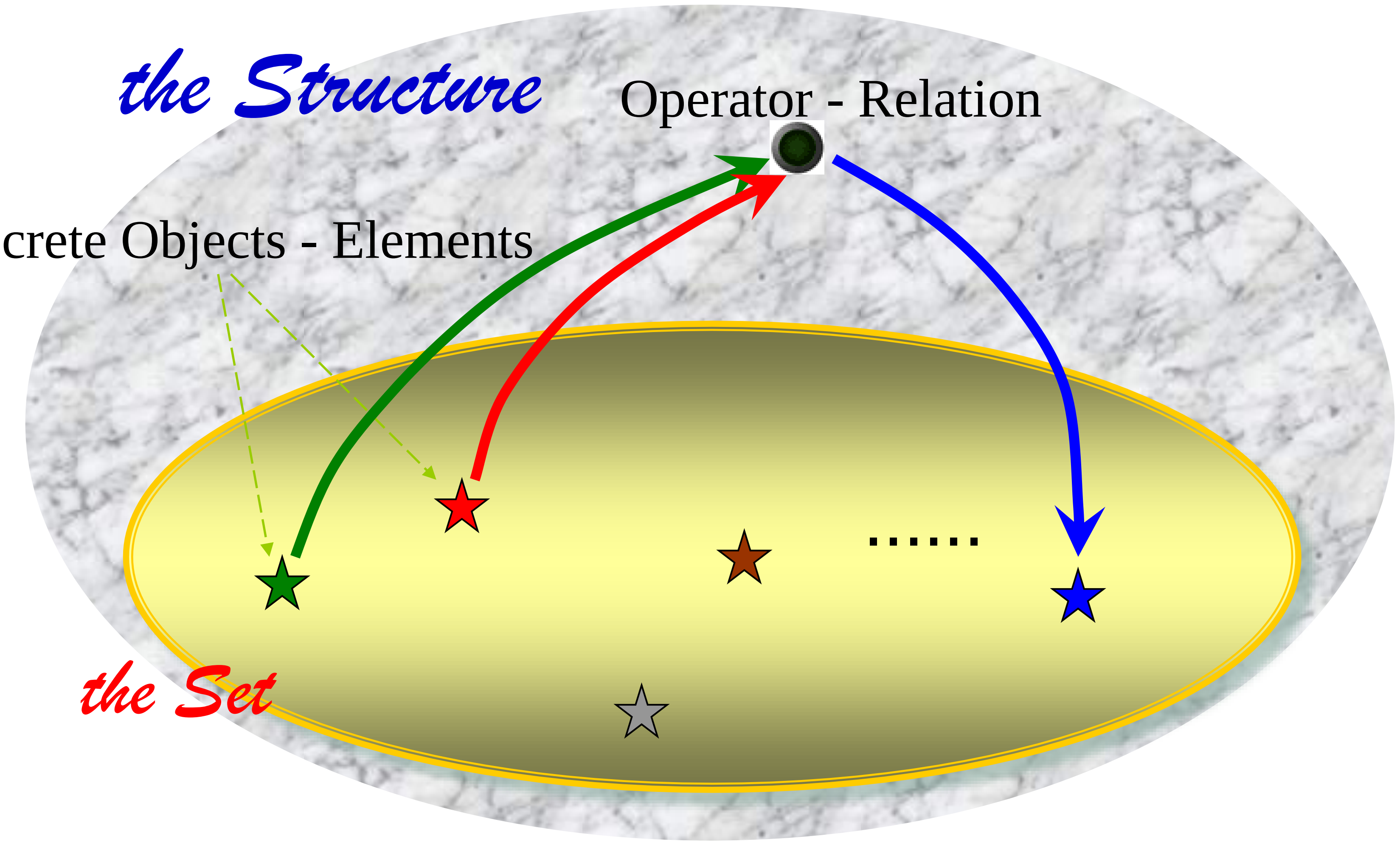
System Abstraction

Data Abstraction

Real world

Computer implementation

Modeling the Real World



What We Look at

Structures in General

Specific Structures

Details of Obs & Ops

Discrete Math Model – an Example

- Two-player game using 9 matches
  - Each player in turn can take one, or two, or three matches away,
  - BUT cannot take the same number as the other player took in the last run.
  - The player lost the game if he can not take away any more match.
- The first player wins if he is smart enough!
  - Take away 1 match first: 8 matches left, the choices of second player: 2,3
  - If 2nd player takes away 2 matches:
    - Take away 3 matches: 3 matches left, the choices of 2nd player: 1,2.
  - If 2nd player takes away 3 matches:
    - Take away 1 matches: 4 matches left, the choices of 2nd player: 2,3 …
- A more general problem:
  - Is the first player guaranteed to win if the game starts with N matches?

Modeling The Game

- The model should specify all the aspects concerned
- To record the current situation (configuration).
  - Next player,
  - The number of matches left,
  - Forbidden move
  - (X, m, k)
- Possible move: taking away i matches, where
  - i = 1,2,or 3;
  - i != k
  - i <= m

Solve the problem by algorithm

- Win(X, m, k)
  - Can player X win if m matches left, and he can not take away k matches from the rest matches?
- Losing configurations:
  - (X, 1, 1), (X, 0, *)

```
Win(X, m, k)
{
        if(m == 1 && k == 1 || m == 0)
                return false;

        for(i = 1,2,3)
        {
                if(i > m || i == k)    continue;
                if(!Win(1-X, m-i, i))
                        return true;
        }
        return false;
}
```

The first player wins if Win(0, N, -1) return true

Generalize More !

- Can the algorithm be generalized to solve other kinds of games?
- Specify Configurations and Moves

Conditions

- Either win or lose
- Each move results in a “smaller” configuration.

Abstract configurations details not concerned.

```
Win(Configuration cfg)
{
        if(LosingConfiguration(cfg))
                return false;

        for(each possible move m)
        {
                cfg’ = m(cfg);
                if(! Win(cfg’))
                        return true;
        }
        return false;
}
```

Basic Models and Tools

- Part I: Sets, Sequences and Structures
  - Sets: fundamental model in mathematics
  - Sequences: elements and order
  - Structures: sets with operations
- Part II: Some Useful Tools
  - Division, prime and algorithm

Concept of Set

- No exact definition
  - a variety of different objects as being bound together by some common property, the property may be nothing more than the ability to think of these objects (as being) together
- Description by Cantor
  - A set is a collection into a whole of definite, distinct objects of our intuition or our thought. The objects are called elements (member) of the set.

Representation of Set

- Enumeration: {element$_1$, element$_2$, …, element$_n$}

- {x | **P**(x)}, **P** must be a mathematically definite property
  - "There exists no Y $\in$ X" is a well-defined property about X

- There may be more than one representation for one set:
  - {2, 3, 5}
  - {x | x >= 1 AND x < 7 AND isPrime(x)}
    - All prime numbers in [1, 7)
  - {x | x^3-10x^2+31x-30=0}
    - All real roots of the equation x^3-10x^2+31x-30=0。

is a member of

- An object x is an element of a set A (or x is in A) is denoted as $x \in A$
- An object x is not an element of a set A (or x is not in A) is denoted as $x \notin A$
- Examples
  - □ $2 \in \{2, 3, 5\}$
  - □ $6 \notin \{2, 3, 5\}$

Subset

- “ is a subset of ” is a relation between two sets:
  - $A \subseteq B$ is defined as: for all x, $x \in B$ if $x \in A$
  - So, $A \not\subset B$ means that: There exists at least an x, satisfying $x \in A$ and $x \notin B$

- A is a true subset of B if and only if
  - $A \subseteq B$ and $B \not\subset A$

Equality of Sets

- Two sets A,B are equal (A=B) if they have the same elements.

- For any two sets A,B, A=B if and only if:
  - $A \subseteq B$, and
  - $B \subseteq A$

Empty Set

- A set without any element in it is called empty set
  - Ex. A = {x | x is an integer and x>x}
  - {x | P(x)}, where P(x) is unsatisfable

- Property : Empty set is a subset of any set.
  - If A is a set, "For all x, x is in A if x is in Ø" is always true.

- Property : There is a unique empty set
  - If there are two empty sets $Ø_1$, $Ø_2$, then both $Ø_1 \subseteq Ø_2$ and $Ø_2 \subseteq Ø_1$ are true.
  - Empty set is denoted as Ø

Power Set

- $\rho(A) = \{x \mid x \subseteq A\}$, where A is a set.

- $\rho(\{a,b\}) = \{\varnothing,\{a\},\{b\},\{a,b\}\}$
- $\rho(\varnothing) = \{\varnothing\}$

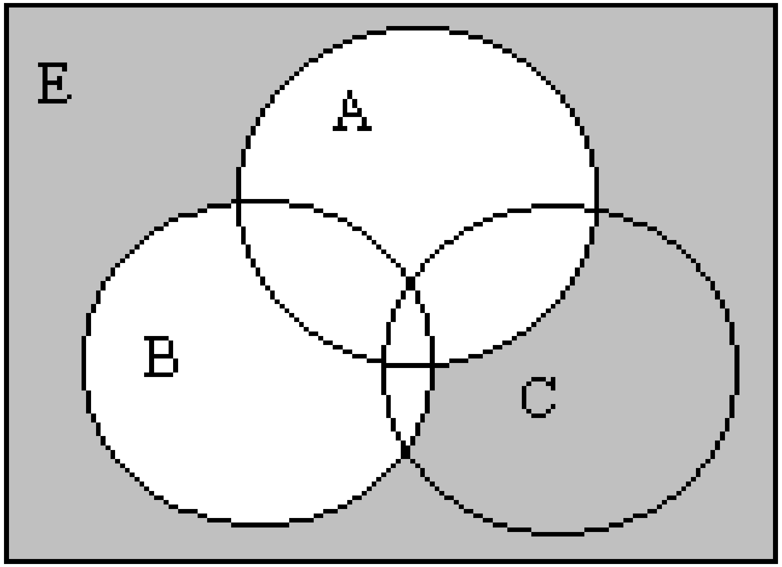
- If $|A|=n$, then $|\rho(A)|=2^n$
  - So, another denotation for power set: 2^A

Fundamental Set Operations

- Union and intersection
  - $A \cup B = \{x | x \in A \text{ or } x \in B\}$
  - $A \cap B = \{x | x \in A \text{ and } x \in B\}$
- Complement (with respect to a universal set)
  - $\sim A = \{x \mid x \notin A\}$
- Complement with respect to a given set
  - $A - B = \{x | x \in A \text{ and } x \notin B\} = A \cap \sim B$
- Symmetric difference
  - $A \oplus B = (A - B) \cup (B - A)$

Venn’s Digram: Example 1

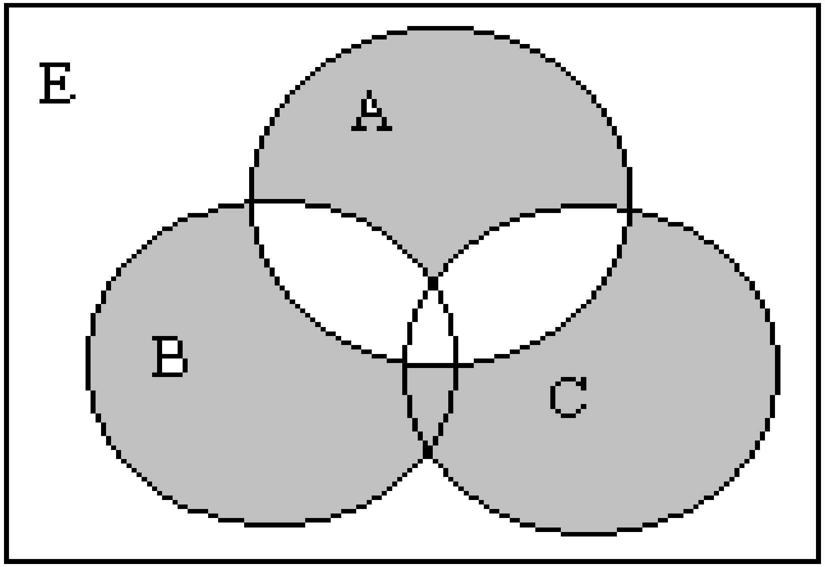
- $\sim A \cap \sim B$
- $\sim(A \cup B)$



Venn’s Digram：Example 2

- $(A-(B\cup C))\cup((B\cup C)-A)$

- $\mathrm{A} \oplus (B\cup C)$



Properties of Set Operations （1）

- Least upper bound and greatest lower bound under inclusion relation
  - $A \subseteq A \cup B$, $B \subseteq A \cup B$
  - For any X， if $A \subseteq X$, $B \subseteq X$, then $A \cup B \subseteq X$
  - $A \cup B$ is the least upper bound of A and B

  - $A \cap B \subseteq A$, $A \cap B \subseteq B$
  - For any X， if $X \subseteq A$, $X \subseteq B$, then $X \subseteq A \cap B$
  - $A \cap B$ is the greatest lower bound

Properties of Set Operations （2）

- Subset relation and set operations
  1. $A \subseteq B \Leftrightarrow$
  2. $A \cup B = B \Leftrightarrow$
  3. $A \cap B = A \Leftrightarrow$
  4. $A - B = \phi$

Properties of Set Operations（3）

- Properties of Union and Intersection
  - Idempotent properties
  - Associative properties
  - Commutative properties
  - Distributive properties
  - Properties related to empty and universal set
  - Properties related to complement
  - Absorptive properties
  - de Morgan’s Law

Properties of Set Operations（4）

- Properties of the relative complement
  - $A-B \subseteq A$
  - $A-B = A \cap \sim B$

Properties of Set Operations（5）

- Properties of the symmetric difference
  - Commutation and Association
  - Idempotention
  - $A \oplus A = \phi$
  - Cancellation

True or False?

✘ (1) $A \in \{\{A\}\}$

✓ (2) $\{A\} \in \{\{A\}\}$

✓ (3) $x \in \{x\} - \{\{x\}\}$

✓ (4) $\{x\} \subseteq \{x\} - \{\{x\}\}$

✘ (5) $A - B = A \quad \Leftrightarrow \quad B = \emptyset$

✘ (6) $A - B = \emptyset \quad \Leftrightarrow \quad A = B$

✘ (7) $A \oplus A = A$

✓ (8) $A - (B \cup C) \quad = \quad (A - B) \cap (A - C)$

✘ (9) If $A \cap B = B$, then $A = E$

✓ (10) $A = \{x\} \cup x$, then $x \in A$ and $x \subseteq A$

How to Prove（1）

- **Using definitions of equality or inclusion**
  - Ex： $A \cup B = B \Rightarrow A \subseteq B$
    - Prove “For any x, if $x \in A$, then $x \in B$”
  - Ex： $A \subseteq B \Rightarrow A \cap B = A$
    - Prove both:

      “For any x, if $x \in A \cap B$, then $x \in A$”

      “For any x, if $x \in A$, then $x \in A \cap B$”

How to Prove（2）

- **Using definition of operations**
  - Ex： $A-(B\cup C) = (A-B) \cap (A-C)$

$A-(B\cup C)=\{x|x\in A, \text{ but } x\notin B\cup C)$

$=\{x| x\in A, \text{ but } (x\notin B \text{ and } x\notin C)\}$

$=\{x| (x\in A, \text{ but } x\notin B) \text{ and } (x\in A, \text{ but } x\notin C)\}$

$= (A-B) \cap (A-C)$

How to prove（3

- **Algebraic reduction**
  - □ Ex： $A\cap B=A \Leftrightarrow A-B=\phi$
  - □ Ex： $A\cup(A\cap B) = A$
  - □ Ex： If $A\oplus B=A\oplus C$, prove $B=C$
  - □ A more complicated example：
    - Using $A \cap B=A \Leftrightarrow A\subseteq B$ to prove：

$((A\cup B\cup C) \cap (A\cup B))-((A\cup(B-C)) \cap A)=B-A$

$A\cap B=A\Rightarrow A-B=\phi$:

$= A\cap\sim(A\cap B) = A\cap\sim A = \phi$

$A-B=\phi\Rightarrow A\cap B=A$:

$A\cap B=(A\cap B)\cup(A\cap\sim B)$

$=A\cap(B\cup\sim B)=A\cap E=A$

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

$(A\cup(B-C)) \cap A)=A$, so $(A\cup B)-A=B-A$

How to prove（4）

- **Prove a sequence of logically equivalent expression**
  - □ $A\cup B=B \Leftrightarrow A\subseteq B \Leftrightarrow A\cap B=A \Leftrightarrow A-B=\phi$，
    - Using the results above, we only need prove $A-B=\phi \Rightarrow A\cup B=B$。
    - Note：$A\cup B= (A\cup B) \cap E=(A\cup B) \cap(\sim B\cup B)$

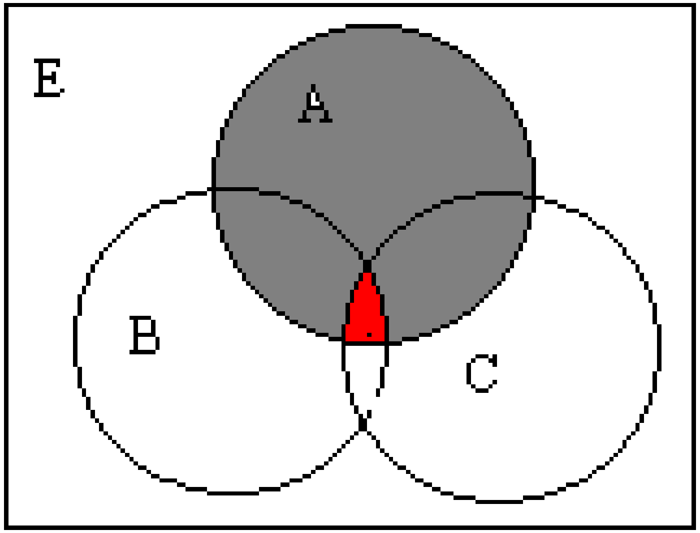
More about Venn’s Diagram

- Venn’s digram and proof
- Ex：
  - Give the condition for

    $(A-B)\cup(A-C)=A$

    the sufficient and
    necessary condition
    is preferred

    $A\cap B\cap C=\phi$



Counting for Finite Sets

- Addition Principle (inclusion-exclusion principle)
  - Two sets
    - $|A \cup B| = |A|+|B|-|A \cap B|$
  - Three sets
    - $|A \cup B \cup C| = |A|+|B|+|C|-|A \cap B|-|A \cap C|-|B \cap C|+|A \cap B \cap C|$

Using Addition Principle

- Among 260 students，64 select Math，94 select Computing，58 select Finance，28 select both Math and Finance，26 select both Math and Computing，22 select both Computing and Finance，14 select all three.
- Problem: How many select none, and how many select only one course?

Solution

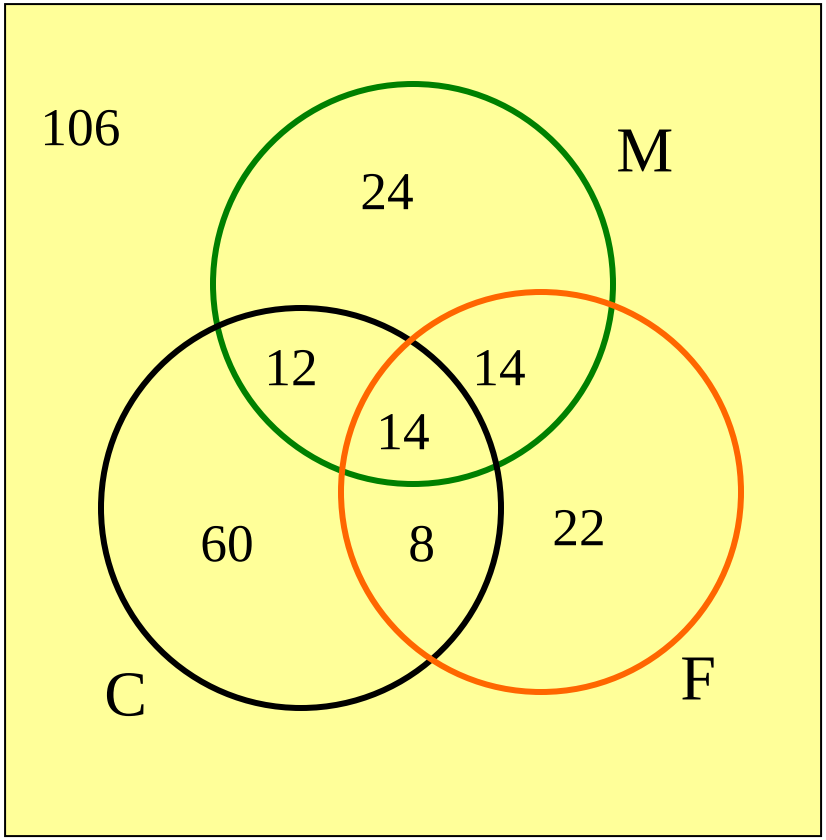
- Addition principle

|M∪C∪F|=|M|+|C|+|F|-|M∩F|-|M∩C|-|C∩F|+|M∩C∩F|

=64+94+58-28-26-22+14

=154

So, 106 select none.



Generalized Union and Intersection

- Generalized union
  - $\cup A = \{x | \text{exists some } z \in A, \text{such that } x \in z\}$
  - $\cup Ø = ?$
- Generalized intersection
  - $\cap A = \{x | \text{for any } z, \text{ if } z \in A, \text{ then } x \in z\}$
  - $\cap Ø = ?$

Examples on the Set of Real Number

- Generalized union
  - $A_0=\{a|a<1\}$， $A_i=\{a|a\leq 1-1/i\}$,
  - then: $\cup\{A_i|i=1,2,3,...\} = A_0$

- Generalized intersection
  - $B_0=\{b|b\leq 1\}$， $B_i=\{b|b<1+1/i\}$,
  - then: $\cap\{B_i|i=1,2,3,...\} = B_0$

Inside or Outside

- Characteristic Functions

$$f_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A \end{cases}$$

For any subset *A* of a universal set *U*

- Examples:
  - □ A={1,2}; f_A(x)=1-|sign((x-1)(x-2))|

Characteristic Functions and Set Operations

$$f_{A \cap B} = f_A f_B$$

Both

$$f_{A \cup B} = f_A + f_B - f_A f_B$$

Either

$$f_{A \oplus B} = f_A + f_B - 2 f_A f_B$$

Either, but not Both

What about $f_{\text{A-B}}$?

With Ordering Added

- Sequence
  - □ A list of objects **arranged** in a definite order
- The ordering number can be looked as a integral part of the object
- Defining a sequence by formular
  - □ By explicit formular: $s_n = (-4)^2$
  - □ By recursive formula: $f_1 = 0;\ f_2 = 1;\ f_n = f_{n-1} + f_{n-2}$

String – Sequence of symbols

- Alphabet
  - A set of symbols, usually finite, such as A={a,b,c}
- Word (string)
  - A finite sequence of elements of the alphabet, such as ‘bcaabbcca’
  - A string of length zero is defined: Λ
- All words on A consists the set A*
- Defining an operation on A*: ‘·’(catenation)
  - $w_1 \cdot w_2$ is just a longer string with w_2 following w_1

Regular Expression

- The regular expression over an alphabet A is defined as following:
  - □ RE1. the symbol **Λ** is a regular expression
  - □ RE2. for any symbol x in A, **x** is a regular expression
  - □ RE3. If α,β are regular expressions, then **$\alpha\beta$** is
  - □ RE4. If α,β are regular expressions, then **$\alpha\vee\beta$** is
  - □ RE5. If α are regular expressions, then **$(\alpha)^*$** is
- Priority:* > catenation > $\vee$

Regular Expressions

- Given an alphabet A, a subset of A* is a language over A*
- **Language represented by a regular expression.**

Λ	:	$\emptyset$
x	:	{x}
$\alpha\beta$	:	$L(\alpha).L(\beta)$
$\alpha\vee\beta$	:	$L(\alpha)$ U $L(\beta)$
$(\alpha)^*$	:	$L(\alpha)^*$

Defining a Language

- A language specified by a RE called a regular set.
- Let A and B be two regular sets, $A \cup B$, $A \cap B$, ~A are still regualr sets.
- Given a Regular Expression r, and a string s, whether s is in the language of r can be decided automatically.

Examples of Regular Languages

- Let the alphabet be A={0,1}
  - □ 0*(0∨1)*:

    Simply the A* itself
  - □ 00*(0∨1)*1:

    Beginning with a “0”, and ended with a “1”
  - □ (01)*(01∨1*):
    - Note: (01∨1*) corresponds to {01, 1,11,111,1111,...}

Structures in General

- Discrete mathematical structures, or systems
  - □ A collection of objects: the set
  - □ One or more operations defined on the set
  - □ The accompanying properties
    - Properties most commonly discussed:

      closure

      commutative, associative, distributive

      identity and inverse

Operation Table

- Operation table can be used to define unary or binary operations on a finite set (usually only with several elements)

*	a	b	c	d
a	1	®	✱	M
b	&	6	K	M
c	7	6	Q	0
d	G	#	~	□

Closed Operations

- A structure is closed with respect to an operation if that operation always produces another member of the collection of object.

- Arithmatic operations on sets of numbers
- Set A={1,2,3,...,10}, gcd is closed, but lcm is not.
- Is the common addition closed on the following set:
  - {n | there exists a positive integer *k*, such that $16|n^k$}
  - {n | 9 divides 21n}

Identity

- 1*x=x*1=x for any real number x, (* is the common multiplication)
- If, in a structure with a binary operation *, there is a specific element *e*, satisfying x**e*=*e**x=x for any x in the collection, then *e* is called an identity.
- In fact, such *e* is unique in the structure

Inverse

- In the set of positive real number, for any x, there is an element x’, satisfying x*x’=1, the identity. (x’ is 1/x)
- If a binary operation * has an identity e, we say y is a *-inverse of x if x*y=y*x=e
- If fact, if * is associative, and x has a *-inverse y, then y is unique
  - Suppose x has two *-inverse, say, y and z, then

    y = e*y = (z*x)*y = z*(x*y) = z*e = z

Details about Integer Division

- If n and m are integers and n>0, we can write $m=qn+r$ for uniquely determined integers q and r with $0 \le r \le n$.
- "n divedes m" is a relation on integers
  - □ If $a|b$ and $a|c$, then $a|(mb+nc)$ for any integers m,n
- Prime number

Greatest Common Divisor(GCD)

- If d is GCD(a,b), then $d=sa+tb$ for some integer s and t
  - □ Let x be **the smallest positive integer** that can be written as **sa+tb**.
  - □ For any common divisor c of a,b, $c|(sa+tb)$, which means that ***x* is no less than any common divisor of *a,b.***

  Let $a=qx+r$ ($r<x$), then $r = a-q(sa+tb) = (1-qs)a-qtb$. Since r is also of the form of $s'a+t'b$, r can not be positive, and must be 0. So, $a=qx$, that is, $x|a$. Similarly, $x|b$.

  Conclusion: $x=sa+tb$ is the largest common divisor of a and b. And it is a multiple of any other common divisors.

- If a and b are relatively prime, we can always find two integers s,t, satisfying $sa+tb=1$

Euclidean Algorithm

- Euclid (a,b) [a,b are arbitrary nonnegative integers]

  -
    ```
    **if** $b$=0 **then return** $a$
              **else** Euclid ($b$, $a$ mod $b$)
    ```
- Correctness of Euclid Algorithm
  - The algorithm must terminate
  - Note: Let $a=k_1b+r_1$ (that is, r_1 is a mod b), then $r_1=a-k_1b$. It is easy to see that any common divisor of b,r_1 must divide a, and any common divisor of a,b must divide r_1 as well. So, GCD(a,b)=GCD(b,r_1)

Home Assignments

- To be checked
  - pp.4-5: 5, 10, 16, 30-31, 34, 36
  - pp.11-13: 1, 6, 10, 23-24, 34, 36, 39
  - pp.19-20: 19, 20, 22, 25, 29, 32, 34, 37
  - p.30-31: 24-29
  - p.39-41: 6,9, 16, 17, 23, 29, 41
  - P.44-45: 24-29, 35

- Self tests