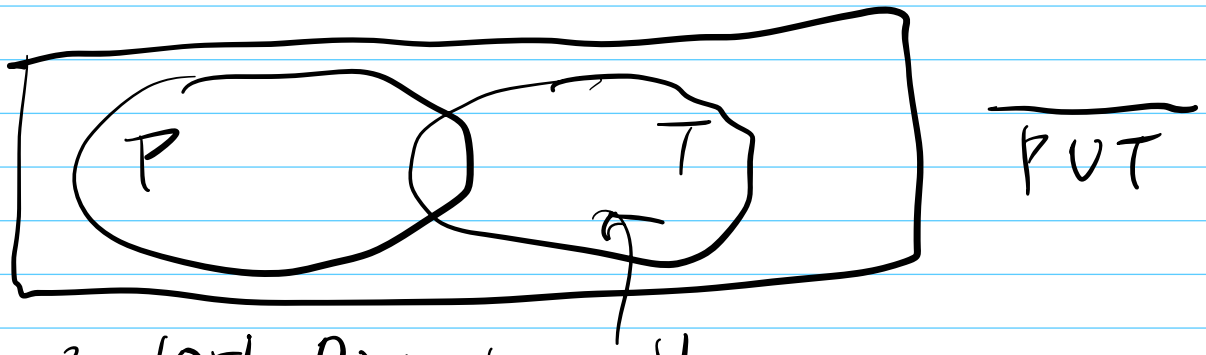
P: coding, hand-on

T: theory / math, pfs



250/251 Discrete math

Typical topics

250	251	others
□ Set theory	○ Logic	△ Combinatorics
□ math pfs (e.g. induction)	☆ Algebraic structure (aka. abstract) algebra	☆ Number theory
△ Graph theory.		◇ linear algebra
◇ Probability theory		

- why bother?

□: foundations

△: algorithm design.

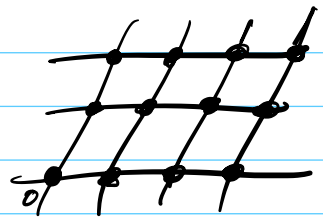
◇: ML / Data Science

○: PL

☆: cryptography / Communication / deep learning.

b. A few motivating Problems.

- Factoring // Given: $n = p \cdot q$ (p, q prime) Find: p. ($n = 33$, $p = 3$, $q = 11$)
- Pell's eqn: Given: d integer
  Find: integer soln's x, y s.t. $x^2 - dy^2 = 1$
  e.g. $d = 2$, $x = 3$, $y = 2$
  $\{(s,t) : s + \sqrt{2}\cdot t = (3 + \sqrt{2}\cdot 2)^n\}$
- SVP (shortest vector problem): Given: Lattice Λ Find: $v \in \Lambda$, $v \neq 0$ s.t. $\|v\|$ min.



Lattic Λ (格)

All fundemental to modern cryptograph!

↓

3. Diophantine eqn's: find integer soln's to eqn's.
   - linear: $ax + by = c$
     x, y unknown, a, b, c integers
   - quadratic $ax^2 + by^2 = c$
   - $x^n + y^n = z^n$
     - $n = 1$: $x + y = z$ easy!
     - $n = 2$: $x^2 + y^2 = z^2$ (Pythagorean) 勾股定理
     - $n \geq 3$: no int. soln's

Fermat's last theorem

- Hilbert's 10th problem:

Is there an algorithm deciding if a D! eqn has a soln?

$\Downarrow$

Halting Problem ✗

uncomputable

$\exists$ problems uncomputable by any computer.

1. Algebraic structures.

a. what is an algebra?

set + operation

- $(\mathbb{R}, +)$
- $(\mathbb{R}, \cdot)$

$\rightarrow (\mathbb{R}, +, \cdot)$

- X : set. $\mathcal{P}(X) := \{Y \subseteq X\}$ power set (冪集)
- $(\mathcal{P}(X), \cup)$

Abstract $\longleftrightarrow$ Concrete.

develop generic properties/techniques. gain intuition sanity check

- what's common in examples above?

$3+5=8 \in \mathbb{R}$

$\sqrt{2} \cdot e = \sqrt{2}e \in \mathbb{R}$

$S_1 \subseteq X$, $S_2 \subseteq X$, $S_1 \cup S_2 \subseteq X$ i.e. $S_1 \cup S_2 \in \mathcal{P}(X)$

☆: set closed under the operation.

$\forall x, y \in S,\ x \circ y \in S.$

- DEF: An algebraic structure/system (algebra) consists of a set $A \neq \emptyset$, and operations $f_1, \dots f_k$ s.t. for all i, A is closed under f_i.

  i.e. $\forall i$, $f_i : \underbrace{A \times \dots \times A}_{n_i} \to S_i$

  $\forall x_1 \dots x_{n_i} \in A.\ f_i(x_1 \dots x_{n_i}) \in A$

  (in an algebra : $S_i \subseteq A\ \forall i$)

  - usually consider binary op's : $f_i : A \times A \to A$
  - Notation : $\begin{pmatrix} \circ \\ \cdot \\ + \\ * \end{pmatrix}$

b. Special algebras

- Commutative algebra: $\forall a, b \in A$
  $a * b = b * a$
- DEF: [Semigroup] $(A, *)$ algebra is called a semigroup, if $*$ is associative.
  $\forall x, y, z \in A,\ (x*y)*z = x*(y*z)$

→ can define (abstract) exponentiation:

$$a^n := \underbrace{a * a * \dots * a}_{n \text{ times}}$$

Ex. $(\mathbb{R}, \cdot)$ a^n is ordinary exp.
$(\mathbb{R}, +)$ $a^n = a + \dots + a = na$.

· DEF [monoid (獨幕點.)]

semigroup + identity (單位元)

$\exists\ e \in A$, s.t. $\forall x \in A$, $x * e = e * x = x$

Eg: $(\mathbb{R}, +)$: $e = \underline{0}$

$(\mathbb{R}, \cdot)$: $e = \underline{1}$

$(\mathcal{P}(S), \cup)$: $e = \underline{\emptyset}$

· Thm: If $(S, *)$ is a semigroup.
& S is finite set.
then $(S, *)$ has an element b
w/ $b^k = b$ $\forall\ k \geq 1$.

· Pf: $\forall a \in S$, consider

$a^1, a^2, a^3, \cdots a^i, \cdots, a^j, \cdots$

B/C $|S|$ is finite, must repeat

[Pigeonhole principle 鴿籠原理]

say $a^i = a^j$ $(i < j)$

Let $\ell = j - i$

$a^j = a^\ell * a^i = a^i$

$\forall\ q \geq i$, $a^q = a^i * a^{q-i}$

$= (a^\ell * a^i) * a^{q-i} = a^\ell * a^q$

B/c. $\ell \geq 1$ $\exists$ integer $k > 0$, s.t. $k\ell \geq i$

$$a^{k\ell} = a^{\ell} * a^{k\ell}$$

$$= a^{\ell} * (a^{\ell} * a^{k\ell})$$

k times $\left\{ \right.$ $\vdots$

$$= \underbrace{a^{\ell} * a^{\ell} \cdots * a^{\ell}}_{k} * a^{k\ell}$$

$$= a^{k\ell} * a^{k\ell}$$

$b = a^{k\ell}$, $b = b * b * b * b \cdots$

$= b^{k}$

(QED)

c. subalgebra

- DEF: $(A, *)$ algebra.

  $S \subseteq A$, if $(S, *)$ is an algebra.

  then call it a subalgebra of $(A, *)$.

  $\Updownarrow$

  S closed under $*$: $x, y \in S$, $x * y \in S$.

Ex: $(\mathbb{Z}, +)$ is subalgebra $(\mathbb{R}, +)$