零知识证明笔记

谢文进

2023 年 4 月 19 日

目录

1 TO-DO

- 线性变换
- 不可约多项式

2 基本概念

2.1 抽象代数

参考资料

- 《抽象代数》张贤科 清华大学出版社
- 《高等代数》（第三版）北京大学数学系几何与代数教研室

定理 1 (古典代数学基本定理)**.** *任意 n 次方程 $x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ 一定有复数解（这里 $a_1, \cdots, a_n$ 为任意复数，整数 $n \geq 1$）.*

一个**集合**就是一些互异的确定的对象全体，其中每个对象称为一个成员或元素，简称为元，有时也称为点。
映射三要素：定义域、值域、对应规则。对任意两个不同的原像，它们有不同的像，则为**单射**。
以 (a, b) 或 $\gcd(a, b)$ 记 a, b 的正的最大公因子。

引理 1. *若 $a = bq + r$，其中 a, b, r 为整数（不全为 0），则*

$$(a, b) = (r, b).$$

《高等代数》中有类似引理。

引理 2 (《高等代数》P13)**.** 如果有等式

$$f(x) = q(x)g(x) + r(x) \tag{1}$$

成立，那么 $f(x), g(x)$ 和 $g(x), r(x)$ 有相同的公因式。

引理1中的公式 $(a, b) = (r, b)$ 说明：余数 r 可作为原数 a 的“替身”去参与求最大公因子，以此类推，引出著名的**“辗转相除法”**。

定理 2. 任意两个整数 $a, b(b \neq 0)$ 的最大公因子 $d = (a, b)$ 是唯一存在的，即 $d = r_s$（就是 a 与 b 辗转相除的最后非零余数），而且存在整数 u, v 使

$$ua + vb = d \quad (\textbf{贝祖等式}, \textit{Bézout's identity}).$$

定义 1 (《抽象代数》张贤科 P17)**.** 一个**群**就是一个非空集合 G，且其元素之间有一种运算，此运算将 G 中任意元素 a，b（可以相等）对应于 G 中的一个元素（记为 $a \cdot b$ 或 ab），而且满足如下 4 个条件（称为**群的公理**）：

($G1$) （封闭性）ab 仍然在 G 中（对任意 a，$b \in G$）；

($G2$) （结合律）$a(bc) = (ab)c$（对任意 $a, b, c \in G$）；

($G3$) （存在单位元）存在元素 $e \in G$ 使 $ea = ae = a$（对任意 $a \in G$）；

($G4$) （可逆性）对每个元素 $a \in G$，存在 $a' \in G$ 使 $a'a = aa' = e$.

满足交换律的群称为**交换群**，或 **Abel 群**。
由一个元素 a 生成的子群，称为**循环子群**，记为 $\langle a \rangle$. 如果群 $G = \langle a \rangle$，则 G 称为**循环群**.

定理 3 (算术基本定理，参考维基百科)**.** 算术基本定理，又称为正整数的唯一分解定理，即：每个大于 1 的自然数，要么本身就是质数，要么可以写为 2 个或以上的质数的积，而且这些质因子按大小排列之后，写法仅有一种方式。

充分条件与必要条件

- 由条件能推出结论，但由结论推不出这个条件，这个条件就是充分条件。
- 如果能由结论推出条件，但由条件推不出结论，此条件为必要条件。
- 如果既能由结论推出条件，又能有条件推出结论，此条件为充要条件。

2.2 初等数论

2.2.1 原根

参考oi-wiki 原根，一些数学概念及定理如下：

定义 2. 阶：由欧拉定理可知，对 $a \in \mathbb{Z}$，$m \in \mathbb{N}^*$，若 $\gcd(a, m) = 1$，则 $a^{\varphi(m)} \equiv 1 \pmod{m}$。因此满足同余式 $a^n \equiv 1 \pmod{m}$ 的最小正整数 n 存在，这个 n 称作 a 模 m 的阶，记作 $\delta_m(a)$。

定义 3. 原根：设 $m \in \mathbb{N}^*$，$a \in \mathbb{Z}$。若 $\gcd(a, m) = 1$，且 $\delta_m(a) = \varphi(m)$，则称 a 为模 m 的原根。

定理 4 (原根判定定理)**.** *设 $m \geqslant 3$, $\gcd(a,m)=1$，则 a 是模 m 的原根的充要条件是，对于 $\varphi(m)$ 的每个素因数 p，都有 $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod m$。*

证明. 必要性显然，下面用反证法证明充分性。

当对于 $\varphi(m)$ 的每个素因数 p，都有 $a^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod m$ 成立时，我们假设存在一个 a，其不是模 m 的原根。因为 a 不是 m 的原根，则存在一个 $t<\varphi(m)$ 使得 $a^t \equiv 1 \pmod m$。

由裴蜀定理得，一定存在一组 k,x 满足 $kt = x\varphi(m)+\gcd(t,\varphi(m))$。又由欧拉定理得 $a^{\varphi(m)} \equiv 1 \pmod m$，故有：

$$1 \equiv a^{kt} \equiv a^{x\varphi(m)+\gcd(t,\varphi(m))} \equiv a^{\gcd(t,\varphi(m))} \pmod m$$

由于 $\gcd(t,\varphi(m)) \mid \varphi(m)$ 且 $\gcd(t,\varphi(m)) \leqslant t < \varphi(m)$。故存在 $\varphi(m)$ 的素因数 p 使得

$$\gcd(t,\varphi(m)) \mid \frac{\varphi(m)}{p}$$

则 $a^{\frac{\varphi(m)}{p}} \equiv a^{(t,\varphi(m))} \equiv 1 \pmod m$，与条件矛盾。

故假设不成立，原命题成立。 □

定理 5 (原根存在定理)**.** *一个数 m 存在原根当且仅当 $m=2,4,p^\alpha,2p^\alpha$，其中 p 为奇素数，$\alpha \in \mathbb{N}^*$。*

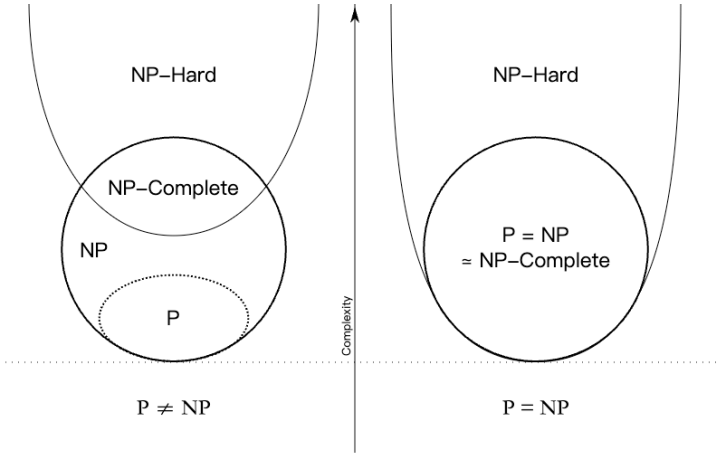
2.3 计算复杂度

参考P/NP 问题、NP 完全、P 问题、NP 问题、NP 完全问题和 NP 难问题：

- **P 问题**：复杂度类 P 即为所有可以由一个确定型图灵机在多项式表达的时间内解决的问题。
- **NP 问题**：类 NP 由所有可以在多项式时间内验证它的解是否正确的决定问题组成，或者等效的说，那些可以在非确定型图灵机上在多项式时间内找出解的问题的集合。
- **NPC 问题**：一个决定性问题 C 若是为 NPC（NP 完全），则代表它对 NP 是完全的，这表示：
  - 它是一个 NP 问题
  - 它是一个 NP 困难问题
  - 其他属于 NP 的问题都可在多项式时间内归约（reduce to）成它。

  可归约（reducible）在此意指对每个问题 L，总有一个多项式时间多对一变换，即一个决定性的算法可以将实例 $l \in L$ 转化成实例 $c \in C$ ，并让 c 回答 Yes 当且仅当此答案对 l 也是 Yes。为了证明某个 NP 问题 A 实际上是 NP 完全问题，证明者必须找出一个已知的 NP 完全问题可以归约成 A。
- **NP 难问题**：NP-Hard 问题是这样一种问题，它满足 NPC 问题定义的第二条但不一定要满足第一条（就是说，NP-Hard 问题要比 NPC 问题的范围广，NP-Hard 问题没有限定属于 NP），即所有的 NP 问题都能约化到它，但是它不一定是一个 NP 问题。

它们之间的关系如下：



3 零知识证明

3.1 交互式零知识证明

参考课程Zero Knowledge Proofs。

定义 4. *A language $\mathcal{L}$ is a set of binary strings x.*

定义 5. *$\mathcal{L}$ is an **NP**-language (or NP-decision problem), if there is a **poly**$(|x|)$ **time** verify V where*

- ***Completeness [True claims have (short) proofs].***
  if $x \in \mathcal{L}$,there is a poly$(|x|)$-long witness $w \in \{0,1\}^*$ s.t. $V(x,w) = 1$.
- ***Soundness [False theorems have no proofs].***
  if $x \notin \mathcal{L}$, there is no witness. That is, for all $w \in \{0,1\}^*, V(x,w) = 0$.

定义 6. *(P,V) is an interactive proof for L, if V is probabilistic poly $(|x|)$ time and*

- *Completeness: If $x \in L$, V always accepts.*
- *Soundness: If $x \notin L$, for all cheating prover strategy, V will not accept except with negligible probability.*

定义 7. *(P,V) is an interactive proof for L, if V is probabilistic poly $(|x|)$ and*

- *Completeness: If $x \in L$, $Pr[(P,V)(x) = accept] = 1$.*
- *Soundness: If $x \notin L$, for every P^*, $Pr[(P^*,V)(x) = accept] = negl(|x|)$ where $negl(\lambda) \leq \frac{1}{polynomial(\lambda)}$ for all polynomial functions.*

定义 8. *(P,V) is an interactive proof for L, if V is probabilistic poly $(|x|)$ and*

- *Completeness: If $x \in L$, $Pr[(P,V)(x) = accept] \geq c$*
- *Soundness: If $x \notin L$, for every P^*, $Pr[(P^*,V)(x) = accept] \leq s$*

Equivalent as long as $c - s \geq 1/poly(|x|)$.

定义 9. *class of languages IP = {L for which there is an interactive proof}.*

定义 10. *An Interactive Protocol (P,V) is **zero-knowledge** for a language L if there exists a PPT algorithm Sim (a simulator) such that for every $x \in L$, the following two probability distributions are poly-time indistinguishable:*

1. $view_V(P,V)[x,1^\lambda]$
2. $Sim(x,1^\lambda)$

定义 11. *(P,V) is a **zero-knowledge interactive protocol** if it is complete, sound and zero-knowledge.*

定义 12. *An Interactive Protocol (P,V) is zero-knowledge for a language L if for every PPT V^*, there exists a poly time simulator Sim s.t. for every $x \in L$,*

$$view_V(P,V)[x] \approx Sim(x,1^\lambda)$$

Flavors of Zero Knowledge

- Computationally indistinguishable distributions = CZK
- Perfectly identical distributions = PZK
- Statistically close distributions = SZK

Consider $L_R = \{x : \exists w \text{ s.t. } R(x,w) = accept\}$ for poly-time relation R.

定义 13. *(P,V) is a **proof of knowledge** (POK) for L_R if : $\exists$ PPT (knowledge) extractor algorithm E s. t. $\forall x$ in L, in expected poly-time $E^P(x)$ outputs w s.t. R(x,w)=accept. [if $Prob[(P,V)(x) = accept] > \alpha$, then $E^P(x)$ runs in expected poly$(|x|, 1/\alpha)$ time]*

定理 6 (GMW86,Naor)**.** *If one-way functions exist, then every L in NP has **computational zero knowledge interactive proofs**.*

Properties of a Bit Commitment Protocol (Commit, Decommit) between Sender S and Receiver R

- **Hiding**: $\forall$ receiver R^* , after commit stage $\forall b, b' \in 0,1$, view of sender R^* $\{View_{R^*}(Sender(b), R^*)(1^k)\}$ $\approx_c$ $\{View_{R^*}(Sender(b'), R^*)(1^k)\}$ [k = sec.param]
- **Binding**: $\forall$ sender S^*, after commit and decommit stage, Prob[R will accept two different values b and b'] < negl(k), K-security parameter

Protocol design applications

Generally: A tool to enforce honest behavior in protocols without revealing any information. Idea: protocol players sends along with each next-msg, a ZK proof that next-msg= Protocol(history h, randomness r) on history h and c=commit(r) Possible since $L = \{\exists r$ s.t. next-msg = Protocol$(h.r)$ and $c = commit(r)\}$ in NP.

Arthur-Merlin Games [BaM85]

定理 7 (GoldwasserSipser86)**.** *AM (protocols with Public Coins) = IP*

AM Protocols enable "in practice" removal of interaction: the Fiat-Shamir Paradigm[FS87]. Fiat-Shamir Heuristic: If H is random-oracle, then completeness and soundness hold.

Warning: this does **NOT** mean every interactive ZK proof can transform to AM protocols and then use Fiat-Shamir heuristic, since IP =AM transformation requires extra super-polynomial powers from Merlin. And for Fiat-Shamir heuristic to work, Prover must be computationally bounded so not to be able to invert H. Yet, many specific protocols, can benefit from this heuristic.