NANJING UNIVERSITY

Websoft

第一次习题课

6. p质数 q合数 pq互质，$\sqrt{pq}$是有理数/无理数？并证明.

举例. $p=3$，$q=4$ $\sqrt{pq}=\sqrt{12}=2\sqrt{3}$ 无理数.

证明：假设$\sqrt{pq}$是有理数.

$\sqrt{pq}=\frac{m}{n}$，m,n互质.

有 $pq=\frac{m^2}{n^2}$.

若 $n\neq1$. $\frac{m^2}{n^2}$是分数. p、q均为整数，矛盾.

若 $n=1$. 有 $pq=m^2$.

则 m有质因子p. m^2有因子p^2.

则 q有因子p. 与p、q互质矛盾. 故$\sqrt{pq}$是无理数.

黄祥，陈剑豪，包予恒

一些说明

- 成绩构成
  - **作业30%，期中20%，期末50%**
  - 平时成绩以作业为主，各班成绩的均值会被对齐
    - 但是方差不会
- 作业发布
  - 作业在一般每次上课后发布，以周为单位处理
    - 第[i]周作业，[i+1]周批改后在习题课上讲解
  - 有违学术诚信的，当次作业成绩归零

关于学术诚信

- 几点注意事项
  - 抄袭他人或网络资料，属于严重违背学术诚信行为
  - 提供他人抄袭机会同样有违学术诚信
    - 可以进行不涉及最终解题的讨论
  - 自己确实不会，查阅资料后做出并在答案后注明参考源的不视为抄袭
    - 但未必不影响分数
  - 造假自然也有违学术诚信
    - 例如：上传损坏的文件谎称自己及时完成了提交
  - 妨碍他人（例如攻击平台）当然也是不行的
- 作业有违学术诚信原则的，分数归0

作业提交

- 第[i]周作业，[i+1]周之前提交（即周日24:00前）
  - **提前交：周六24:00前提交有少量奖励分（半道题的分数，不会溢出）**
  - 节假日可酌情延迟加分时间
  - 迟交：-20，不向下溢出
- 线上提交：
  - 在教学立方提交至每周发布的第一次作业即可
  - 写电子文档或写好拍照皆可，**按顺序排好序，单个文件**
- 必须写题号，不用抄题

习题课内容

- 上周作业中重点问题的讲解
  - 根据提交的作业情况选择重点难点讲解
  - 即使你的答案得分了，可能还是存在问题
- 上周知识的巩固拓展
  - 通常包括（可能超纲的）思考题，不要求能做出来
- 自主答疑
  - 自主提问

答疑

- 鼓励在群内进行不涉及具体解题的讨论
- 非习题课时间亦可在群内提问作业问题，但是
  - 提交截止前
    - 只回答确实存在的题面表述问题
  - 对应习题课前的提问
    - 有选择的汇总至习题课回答
  - 习题课后提问
    - 响应速度可能比较慢
- 已经有讲解的问题可能不会得到具体回答

逻辑不是什么？

一些符号

- $p \equiv q$：p和q等价
- $p \to q$：条件语句/蕴含（命题）
  - **整个陈述(statement，书上译为语句)为真**
  - 只讨论真值：$p \to (q \to p) \equiv \top$ $\neg p \to (p \to q) \equiv \top$
- $p \vdash q$：可以推出（推理过程）
  - 考虑公式之间的“后承”，**不关心公式的含义**
  - $p_1, p_2 \vdash q$是有效的，当且仅当$p_1, p_2 \vDash q$
- $p \vDash q$：语义蕴含
  - “任意赋值让p真就也能让q真”，
  - $p \vDash q$ iff $(p \to q)$ 永真
- $p \Rightarrow q$：不同人有不同用法，可能是上述含义中任意一个
  - 在不需要明确的逻辑含义时较为常用
- $p \supset q$：别用

自然演绎规则

- 假言推理 $p, p \to q \vdash q$
- 取拒式 $\neg q, p \to q \vdash \neg p$
- 假言三段论 $p \to q, q \to r \vdash p \to r$
- 析取三段论 $\neg p, p \vee q \vdash q$
- 附加律 $p \vdash p \vee q$
- 化简律 $p \wedge q \vdash p$
- 合取律 $p, q \vdash p \wedge q$
- 消解律 $p \vee q, \neg p \vee r \vdash q \vee r$

自然演绎规则是正确的，完备的

$\phi_1, \ldots, \phi_n \vdash \phi$ is valid *iff* $\phi_1, \ldots, \phi_n \vDash \phi$ holds

基于自然演绎规则的推导 基于真值表的语义蕴涵

逻辑命题“不是”推理证明的过程

- 一些书写规范，直接使用命题构成公式来描述推理
  - $\alpha, \alpha \to \beta \vdash \beta$，如果能写出$\alpha, \alpha \to \beta$这种结构，就证明了$\beta$
    - 例如 $A \to B, A \to B \to C \to \neg D \vdash C \to \neg D$
    - 这常常带来一种**误会：真的蕴涵命题是一种推理**
- 实质蕴涵怪论
  - 如p是真的，什么q都能推出p　如p是假的，什么q都能被p推出
    $p \to (q \to p) \equiv \top$　$\neg p \to (p \to q) \equiv \top$
  - 具体来说，我们能用已知真假命题去“推”任何命题
    - (“我不是地球生物”) → “我离散满分”
    - (“我不是地球生物”) → “我离散零分”
  - **这两个命题都是真的（前件为假，大概），但这不make sense**

逻辑语义不等于句子含义

- 当我们使用语言时，我们是要结合语境表达特定的信息，而不仅仅是表达一个逻辑命题
  - “我觉得最后一份课件是包予恒或者陈剑豪来做”
    - $a \wedge b$和$a \vee b$不冲突，那我是否认为最后一份课件可能是他们两个一起做？
- 想一想作业和考试题到底要表达什么目的
  - 例：用命题逻辑表达“如果A，那么B而且C而且D…”
    - 逻辑正确但是我不想给你分数的解
      - P：“A” Q：“B而且C而且D”
      - 结果：$P \rightarrow Q$

逻辑命题只提供对事实真假的判断

- 命题逻辑中，命题之间没有“顺序的推断关系”
  - 做题的时候，我们知道一些东西是真/假，然后判断另外一些东西是不是真的，这只是我们做题的“过程”
    - “不能玩游戏，除非做完作业”
      - 只是说“不存在没做完作业同时又玩游戏的事实”
      - 并没有说**先**做作业，**再**玩游戏
  - 命题的真假在所有原子的真假确定时就决定了
    - 想想真值表的内容，它会因为你有没有画完改变吗？

逻辑能怎么用?

判定问题与可满足问题（SAT）

- 判定问题（Decision problem）
  - 通俗的说：是否有方法能找到一种可行的输入，使得某个问题有可行解。
  - 类似地，是否存在赋值使许多逻辑命题都能被满足。
- 数独
  - P_{ijk} = T 表示i行j列填入k是真的
    - 一个显而易见的约束：$\neg(P_{121} \land P_{122})$
    - 所有的约束能不能同时被满足？
- 电路设计
  - 每个物理空间能放什么？
  - 放置的东西之间要满足什么关连？

	7		4		5			9
				2		4		
		5		6				
				5				
		7	3		1	6		
	9						8	
			2					
3								6
		1	7		4	3		

判定问题与可满足问题（SAT）

- 八皇后问题
  - 同一行，同一列，同一对角线只有一个皇后
  - Pij 表示i行j列填入皇后
    - 每行至少一个皇后
    - $Q_1 = \bigwedge_{i=1}^{n} \bigvee_{j=1}^{n} p(i,j)$
    - 每行至多一个皇后
    - $Q_2 = \bigwedge_{\mathrm{i}=1}^{n} \bigwedge_{j=1}^{n-1} \bigwedge_{k=j+1}^{n} \neg(p(i,j) \wedge p(i,k))$
    - 每列至多一个皇后
    - $Q_3 = \bigwedge_{j=1}^{n} \bigwedge_{\mathrm{i}=1}^{n-1} \bigwedge_{k=i+1}^{n} \neg(p(i,j) \wedge p(k,j))$
    - 对角线上至多一个皇后
    - $Q_4 = \bigwedge_{i=2}^{n} \bigwedge_{j=1}^{n-1} \bigwedge_{k=1}^{\min(i-1,n-j)} \neg(p(i,j) \wedge p(i-k,j+k))$
    - $Q_5 = \bigwedge_{i=1}^{n} \bigwedge_{j=1}^{n-1} \bigwedge_{k=1}^{\min(n-i,n-j)} \neg(p(i,j) \wedge p(i+k,j+k))$

思考题

- 探索：能否只用某一个二元逻辑运算符号，构建出所有的命题？有多少个这样的二元逻辑运算？（注：不保证答案大于0）
  - 例如：只使用∨，不使用∧和→等符号
  - 自定义一个二元逻辑运算：给出相应的真值表

- 定义逻辑运算符#：$a\#b=\neg(a\wedge b)$，判断#是否符合要求
  - 1. 验证$a\#a=\neg a$。
  - 2. 尝试仅用#表示$a\wedge b$、$a\vee b$、$a\rightarrow b$。
  - 3. 存在多少个不同的逻辑运算，满足题目条件？

定义逻辑运算符#：$a\#b = \neg(a \wedge b)$

1. 验证$a\#a = \neg a$。

解：$a\#a \ = \neg(a \wedge a)$

$= \neg a$ 幂等律

2. 用#表示a $\wedge b$

解： $a \wedge b = \neg\neg(a \wedge b)$　双重否定律

$= \neg(a\#b)$　定义

$= (a\#b)\#(a\#b)$

2. 用#表示a $\vee b$、 $a \to b$

解： $a \vee b = \neg(\neg a \wedge \neg b)$　德摩根律

$= \neg\big(\neg((\neg a)\#(\neg b))\big)$ 利用上一页的公式

$= (\neg a)\#(\neg b)$　双重否定律

$= (a\#a)\#(b\#b)$

解： $a \to b = \neg a \vee b$

$= (\neg\neg a)\#(\neg b)$　利用上方的公式

$= a\#(\neg b)$　双重否定律

$= a\#(b\#b)$

- 已验证仅使用逻辑运算符# (真值表如右图所示)，$\boldsymbol{a\#b} = \neg(\boldsymbol{a} \wedge \boldsymbol{b})$，可以表示¬，∧，∨，→，↔，因此可以构建出全部命题
- 我们称，{#}构成的逻辑系统是完备的。

- 探索：能否只使用一个逻辑运算符号（可以自定义二元运算）构建出全部的命题？（不限制使用次数）
- 3. 存在多少个不同的逻辑运算，满足题目条件？
- 尝试：能否逐个验证所有的二元逻辑运算？

a	b	$a \odot b$
0	0	?
0	1	?
1	0	?
1	1	?

每行有1或0两个选择，
一共有2^4=16种二元逻辑运算！

能否快速去掉一些错误答案？

提示：可以先考虑该运算符能否表示$\neg a$。

a	b	$a \odot b$
0	0	1
0	1	?
1	0	?
1	1	0

答案：只有两个逻辑运算符合要求：

$a \odot b = \neg(a \wedge b)$

a	b	$a \odot b$
0	0	1
0	1	1
1	0	1
1	1	0

$a \odot b = \neg(a \vee b)$

a	b	$a \odot b$
0	0	1
0	1	0
1	0	0
1	1	0

第二次习题课

黄祥，陈剑豪，包予恒

作业情况

- 讲解内容
  - HW1
    - Prob2
    - Prob3
    - Prob9
    - Prob10

HW1 Pro2

- 判断下列条件语句真假
  - a) 2 + 2 = 5 当且仅当 1 + 1 = 3。
  - b) 如果 1 + 1 = 2，则 2 + 2 = 5。
  - c) 如果 1 + 1 = 3，则 2 + 2 = 5。
  - d) 如果 0 > 1，则 2 > 1。
- 答案：
  - a) 假↔假=真
  - b) 真→假=假
  - c) 假→假=真
  - d) 假→真=真

HW1 Prob3

- 只有当你已经完成了专业要求(r)，没有欠大学的钱(m)，也没有图书馆的过期图书未还时(b)，你才能从大学毕业(g)
- 错解：$(r \wedge \neg m \wedge \neg b) \rightarrow g$

  可能的错误原因：把题目当成了因果判断，然后根据"如果我XXX，那么我就可以毕业"中出现的关键字写了个表达式？

  "→" (都)可以写成 "如果那么" ≠ "如果那么" **都**可以写成"→"
- 正解：$g \rightarrow (r \wedge \neg m \wedge \neg b)$

  你需要的只是看一看真值：可以毕业，可以不满足要求，唯一不可能的是不满足要求就毕业

  $\neg(g \wedge \neg(r \wedge \neg m \wedge \neg b))$ $\neg g \vee (r \wedge \neg m \wedge \neg b)$

HW1 Prob9

- 甲说：我会游泳。
- 乙说：甲不会游泳。
- 丙说：乙不会游泳。
- 丁说：我们有三个人会游泳。
- 以上只有一个人说假话，那么究竟谁说真话，谁说假话？谁会游泳，谁不会游泳？
- 请**分别**用自然语言表达的日常推理和命题逻辑表达的形式推理解决该问题。

HW1 Prob9

- 甲说：我会游泳。
- 乙说：甲不会游泳。
- 丙说：乙不会游泳。
- 丁说：我们有三个人会游泳。
- 以上只有一个人说假话，那么究竟谁说真话，谁说假话？谁会游泳，谁不会游泳？
- 请用自然语言表达的日常推理解决该问题。
  - 甲乙矛盾，必有一真一假
  - 因为只有一个人说假话，所以丙丁为真
  - 根据丙的真话，所以乙不会游泳
  - 根据丁的真话，所以甲丙丁会游泳，乙不会游泳

HW1 Prob9

- 甲说：我会游泳。
- 乙说：甲不会游泳。
- 丙说：乙不会游泳。
- 丁说：我们有三个人会游泳。
- 以上只有一个人说假话，那么究竟谁说真话，谁说假话？谁会游泳，谁不会游泳？
- 请用命题逻辑表达的形式推理解决该问题。
  - 令p 表示“甲会游泳”；q 表示“乙会游泳”；r 表示“丙会游泳”；s 表示“丁会游泳”；则：甲乙丙丁四人的论述分别为
  - (A): p,
  - (B): $\neg p$,
  - (C): $\neg q$,
  - (D): $(p \wedge q \wedge r \wedge \neg s) \vee (p \wedge q \wedge \neg r \wedge s) \vee (p \wedge \neg q \wedge r \wedge s) \vee (\neg p \wedge q \wedge r \wedge s)$
  - 只有一人说假话，故
  - (F): $(A \wedge B \wedge C \wedge \neg D) \vee (A \wedge B \wedge \neg C \wedge D) \vee (A \wedge \neg B \wedge C \wedge D) \vee (\neg A \wedge B \wedge C \wedge D)$
  - 根据$A \wedge B = F$, 所以$C \wedge D = T$
  - 所以$C=T$，所以$q = F$
  - 所以$D=T$，根据$q = F$化简D，只有第三项$p \wedge \neg q \wedge r \wedge s = T$
  - 于是甲、丙、丁都说真话，也都会游泳；只有乙说假话且不会游泳。

HW1 Prob10

- “析取范式”
  a) ¬、∧和∨构成一个逻辑运算符的功能完备集。
  b) ¬、∧构成一个逻辑运算符的功能完备集。
  c) ¬、∨构成一个逻辑运算符的功能完备集
- 不算错但是依赖了点必要前提的解：
  - XXXX能表达¬,∧,∨, →, ↔所以XXXX是完备的。
    - 完备性：通俗地说，就是什么都能表达。
    - **上述论证的原理是：**{¬,∧,∨, →, ↔}**是完备的，所以能表达它的，就能表达它所表达的，就也是什么都能表达的。**
      - 如果不要这个前提，我们可能应该讨论$2^4 - 2 = 14$个所有可能的真值表。
      - 思考题上我们认为这个完备集是已知的，但是作业讨论的要求是不是更具体？

一组逻辑运算符称为是**功能完备的**，如果每个复合命题都逻辑等价于一个只含这些逻辑运算符的

HW1 Prob10

- “析取范式”
  a) ¬、∧和∨构成一个逻辑运算符的功能完备集。
  b) ¬、∧构成一个逻辑运算符的功能完备集。
  c) ¬、∨构成一个逻辑运算符的功能完备集
- 解:
  a) 每个复合命题都有逻辑等价的析取范式，其中不含非¬、∧和∨的符号。
  b) …，不妨记其形式为$\alpha_1 \vee \cdots \vee \alpha_n$，其中$\alpha_i$是原子命题的合取式，由De Morgan律其与$\neg(\neg\alpha_1 \wedge \cdots \wedge \alpha_n)$逻辑等价，后者不含非¬、∧的符号。
  c) …，由De Morgan律其中每个α_i有逻辑等价的原子命题的析取式$\neg\beta_i$，对应的$\neg\beta_1 \vee \cdots \vee \neg\beta_n$不含非¬、∨的符号。

变量与常量，公式与命题

- 公式不一定是命题
  - $P(x)$，其中x是变量
    - x是可变的，我们不确定到底在陈述什么，也确定不了真假
    - 但是对当前的论域，我知道$P(x)$就是真的，真假能确定所以他可以是命题?
      - 你知道论域里所有的x，所以你知道的是$\forall x P(x)$，而不是$P(x)$
  - $P(c)$，其中c是常量
    - $P(c)$是命题，陈述了具体的c的性质P
- 没有自由变元的公式才能作为命题
  - 换句话说，能描述命题的自然语言陈述也应该约束了所有变元

思考题

- 请运用谓词逻辑表示下列已知和结论的陈述，并证明结论.
  - (1)“疫情期间，所有要进校的人均需要满足居家隔离14天或者集中隔离7天的条件。”
  - (2)“所有居家隔离14天的人均需要有固定的住所。”
  - (3)“张三没有固定的住所，且张三要在疫情期间进校。”
- 对论域D(全体人的集合)设置谓词
  - $A(x)$: x要在疫情期间进校，
  - $B(x)$: x需要居家隔离 14 天
  - $C(x)$: x需要集中隔离7天
  - $D(x)$: x有固定住所
- 各前提表示如下:
  - (1)$\forall x: A(x) \rightarrow B(x) \vee C(x)$;
  - (2)$\forall x: B(x) \rightarrow D(x)$
  - (3)令个体a表示张三，$\neg D(a)$^$A(a)$. 结论表示为: $C(a)$.

思考题

- 请运用谓词逻辑表示下列已知和结论的陈述，并证明结论.
  - (4) 结论:“张三需要被集中隔离7天”
- 推理过程
  - 1. $A(a) \rightarrow B(a) \vee C(a)$ 全称例示（由前提1）
  - 2. $A(a)$ 化简（由前提3）
  - 3. $B(a) \vee C(a)$ 假言推理（由1）
  - 4. $B(a) \rightarrow D(a)$ 全称例示（由前提2）
  - 5. $\neg D(a)$ 化简（由前提3）
  - 6. $\neg B(a)$ 取拒式（由4，5）

- 对论域D(全体人的集合)设置谓词
  - $A(x)$: x要在疫情期间进校，
  - $B(x)$: x需要居家隔离 14 天
  - $C(x)$: x需要集中隔离7天
  - $D(x)$: x有固定住所

思考题

- 试找出一个含命题变元p、q 和r 的复合命题，在p、q 和r 中恰有两个为假时该命题为真，否则为假。[提示：构造合取式的析取。将使命题为真的每一种真值组合构成一个合取式。每个合取式都应包含三个命题变元或它们的否定。]
- 解：

  $(p \land \neg q \land \neg r) \lor (\neg p \land q \land \neg r) \lor (\neg p \land \neg q \land r)$

思考题

- 令p、q、r 为如下命题:
  - p: 在这个地区发现过灰熊。
  - q: 在乡间小路上徒步旅行是安全的。
  - r: 乡间小路两旁的草莓成熟了。
- 试用p、q、r 和逻辑连接词(包括否定) 写出下列命题:
  - a)乡间小路两旁的草莓成熟了,但在这个地区没有发现过灰熊。
    - $r \wedge \neg p$
  - b) 在这个地区没有发现过灰熊,且在乡间小路上徒步旅行是安全的,但乡间小路两旁的草莓成熟了。
    - $\neg p \wedge q \wedge r$
  - c) 如果乡间小路两旁的草莓成熟了,徒步旅行是安全的当且仅当在这个地区没有发现过灰熊。
    - $r \rightarrow (q \leftrightarrow \neg p)$

思考题

- 令p、q、r 为如下命题:
  - p: 在这个地区发现过灰熊。
  - q: 在乡间小路上徒步旅行是安全的。
  - r: 乡间小路两旁的草莓成熟了。
- 试用p、q、r 和逻辑连接词(包括否定) 写出下列命题:
  - d) 在乡间小路上徒步旅行是不安全的，但在这个地区没有发现过灰熊且乡间小路两旁的草莓成熟了。
    - $\neg q \wedge \neg p \wedge r$
  - e) 为了使在乡间小路上旅行很安全，其必要但非充分条件是乡间小路两旁的草莓没有成熟且在这个地区没有发现过灰熊。
    - $q \rightarrow (\neg r \wedge \neg p)$
  - f) 无论何时在这个地区发现过灰熊且乡间小路两旁的草莓成熟了，在乡间小路上徒步旅行就不安全。
    - $(p \wedge r) \rightarrow \neg q$

第三次习题课

黄祥，陈剑豪，包予恒

作业情况

- 讲解内容
  - P1-P8
  - P11
- 平均分
  - 83.8

Problem 1

- 令$C(x)$ 为语句“x 有一只猫作为宠物”，$D(x)$ 为语句“x 有一只狗作为宠物”，$F(x)$ 为语句“x 有一只雪貂作为宠物”。用$C(x)$、$D(x)$、$F(x)$、量词和逻辑联结词表达下列语句。令论域为你班上的所有学生。
  - c) 班上的一些学生有一只猫和一只雪貂，但没有狗。
    - $\exists x(C(x) \land F(x) \land \neg D(x))$
  - e) 对猫、狗和雪貂这三种动物的任意一种，班上都有学生将其作为宠物。
    - $(\exists x C(x)) \land (\exists x D(x)) \land (\exists x F(x))$
    - 也可写成$(\exists x C(x)) \land (\exists y D(y)) \land (\exists z F(z))$

Problem 2

- 如果每个变量的论域都为实数集合，判断下列各语句的真值。
- a) $\exists x(x^2 = 2)$
  - True
- b) $\exists x(x^2 = -1)$
  - False
- c) $\forall x(x^2 + 2 \geq 1)$
  - True
- d) $\forall x(x^2 \neq x)$
  - False

Problem 3

- 证明下列逻辑等价式, 其中x 在A 中不作为自由变元出现。假设论域非空。
- a) $(\forall x P(x)) \lor A \equiv \forall x(P(x) \lor A)$
  - 分两种情况:
    - 如果A 为真, 那么$(\forall x P(x)) \lor A$ 为真, 且$(P(x) \lor A)$ 为真, 则$\forall x(P(x) \lor A)$ 为真, 等式成立。
    - 如果A 为假。如果$\forall x P(x)$ 为真, 那么左边为真, 而右边也为真。如果存在x使得$P(x)$ 为假, 那么两边都为假。
  - 综上, 两边等式成立。

Problem 3

- 证明下列逻辑等价式, 其中x 在A 中不作为自由变元出现。假设论域非空。
- b) $\left(\exists x P(x)\right) \vee A \equiv \exists x(P(x) \vee A)$
  - 分两种情况:
    - 如果A 为真, 那么$(\exists x P(x)) \vee A$ 为真, 且存在x 使得$P(x) \vee A$为真, 则$\exists x(P(x) \vee A)$为真, 等式成立。
    - 如果A 为假。如果存在至少一个x 使得$P(x)$ 为真, 那么左边为真, 而右边也为真。如果所有x 使得$P(x)$ 为假, 那么两边都为假。
  - 综上, 两边等式成立。

Problem 4

- 下列语句的真值是什么?
- a) $\exists ! x P(x) \rightarrow \exists x P(x)$
  - true
- b) $\forall x P(x) \rightarrow \exists ! x P(x)$
  - false (除非论域只包含一个元素)
- c) $\exists ! x \neg P(x) \rightarrow \neg \forall x P(x)$
  - true

Problem 5

- 离散数学班上
  - 有 1 个数学专业的新生,
  - 12 个数学专业的二年级学生,
  - 15 个计算机科学专业的二年级学生,
  - 2 个数学专业的三年级学生,
  - 2 个计算机科学专业的三年级学生,
  - 和 1 个计算机科学专业的四年级学生。
- 用量词表达下 列语句, **再给出其真值。**
  - 令 P(s, c, m) 表示语句"学生 s 为 m 专业的 c 年级学生"。
    - s 的论域为离散数学班上的全部学生,
    - c 的论域为四个年级,
    - m 的论域为所有专业。
  - d) 班上每个学生要么是二年级学生, 要么是计算机科学专业的。
    - $\forall s(\exists c P(s, c, \text{计算机科学}) \lor \exists m P(s, \text{二}, m))$, 为假。

Problem 5

- 离散数学班上
  - 有 1 个数学专业的新生,
  - 12 个数学专业的二年级学生,
  - 15 个计算机科学专业的二年级学生,
  - 2 个数学专业的三年级学生,
  - 2 个计算机科学专业的三年级学生,
  - 和 1 个计算机科学专业的四年级学生。
- 用量词表达下 列语句, 再给出其真值。
  - 令 P(s, c, m) 表示语句“学生 s 为 m 专业的 c 年级学生”。
    - s 的论域为离散数学班上的全部学生,
    - c 的论域为四个年级,
    - m 的论域为所有专业。
  - e) 存在这样一个专业使得该班级有这个专业每一个年级的学生。
    - e) $\exists m \forall c \exists s P(s, c, m)$, 为假。

Problem 6

- 使用谓语、量词、逻辑联结词和数学运算符表达语句“有一个正整数不是三个整数的平方和”。
  - $\exists x \forall a \forall b \forall c((x > 0) \wedge x \neq a^2 + b^2 + c^2)$, 其中域由所有整数组成。

Problem 7

- 假定命题函数$P(x,y)$ 的论域由x 和y 的序偶组成, 其中x 是1、2或3, y 是1、2 或3。用析取式和合取式写出下列命题
- a) $\forall\, x \forall\, y\, P(x,y)$
  - $P(1,1) \land P(1,2) \land P(1,3) \land P(2,1) \land P(2,2) \land P(2,3) \land P(3,1) \land P(3,2) \land P(3,3)$
- b) $\forall\, y \exists\, x\, P(x,y)$
  - $(P(1,1) \lor P(2,1) \lor P(3,1)) \land (P(1,2) \lor P(2,2) \lor P(3,2)) \land (P(1,3) \lor P(2,3) \lor P(3,3))$

Problem 8

- 将下列逻辑式转化为前束范式。
  - a) $\exists x P(x) \lor \exists x Q(x) \lor A$, 其中 A 是不涉及任何变量的命题
    - $\exists x \exists y$ （$P(x) \lor Q(y) \lor A$ ）
  - b) $\neg(\forall x P(x) \lor \forall x Q(x))$
    - $\exists x \exists y \neg(P(x) \lor Q(y))$
  - c) $\exists x P(x) \rightarrow \exists x Q(x)$
    - $\forall x \exists y (P(x) \rightarrow Q(y))$

Problem 11

- 用推理规则证明:
- 如果下列为真
  - $\exists x \neg P(x)$
  - $\forall x(P(x) \vee Q(x))$
  - $\forall x(\neg Q(x) \vee S(x))$,
  - $\forall x(R(x) \rightarrow \neg S(x))$
- 则 $\exists x \neg R(x)$ 为真

步骤		推理
1	$\exists x \neg P(x)$	前提
2	$\neg P(c)$	存在示例 (1)
3	$\forall x(P(x) \vee Q(x))$	前提
4	$P(c) \vee Q(c)$	全称示例 (3)
5	$Q(c)$	(4)
6	$\forall x(\neg Q(x) \vee S(x))$	前提
7	$\neg Q(c) \vee S(c)$	全称示例 (6)
8	$S(c)$	(5)(7)
9	$\forall x(R(x) \rightarrow \neg S(x))$	前提
10	$R(c) \rightarrow \neg S(c)$	全称示例 (9)
11	$\neg R(c)$	拒取式 (8)(10)
12	$\exists x \neg R(x)$	存在引入 (11)

思考题

- 用归谬法证明不存在有理数 r 使得 $r^3 + r + 1 = 0$

思考题

- 用归谬法证明不存在有理数 r 使得 $r^3 + r + 1 = 0$
  - 假设存在一个有理数$\mathrm{r} = \frac{a}{b}$是方程的一个根，其中 a, b 为互质的整数。
  - 代入原方程即$a^3 + ab^2 + b^3 = 0$。
  - 对 a, b 奇偶性的 3 种可能情形进行讨论
    - a, b 互质，a 和 b 不可能同为偶数
  - 容易验证 $a^3 + ab^2 + b^3$为奇，不等于0。由归谬法可以证明不存在这样的有理数根。

补充内容-主析取/合取范式的转换

- 小项
  - n个命题变元的合取式，称为布尔合取或小项，其中每个变元与它的否定不能同时存在，但是二者必须出现且仅出现一次例如
    - $P \wedge Q,\ P \wedge \neg Q,\ \neg P \wedge Q, \neg P \wedge \neg Q$
  - n个命题变元共有2^n个小项，每个小项可以用n位二进制予以编码
  - 若$n = 2$，
    - $m_{11} = P \wedge Q$
    - $m_{10} = P \wedge \neg Q$
    - $m_{01} = \neg\ P \wedge Q$
    - $m_{00} = \neg\ P \wedge \neg Q$
- 对于给定的命题公式，如果有一个等价公式，它仅由小项的析取式组成，则该等价式称作原式的主析取范式
- 在真值表中，一个公式的真值为T的指派所对应的小项的析取，即为该公式的主析取范式

补充内容-主析取/合取范式的转换

- 大项
  - n个命题变元的析取式，称为布尔析取或大项，其中每个变元与它的否定不能同时存在，但是二者必须出现且仅出现一次例如
    - $P \vee Q,\ P \vee \neg Q,\ \neg P \vee Q, \neg P \vee \neg Q$
  - 每个大项可以用n位二进制予以编码
  - 若$n = 2$，
    - $M_{00} = P \vee Q$
    - $M_{01} = P \vee \neg Q$
    - $M_{10} = \neg\, P \vee Q$
    - $M_{10} = \neg\, P \vee \neg Q$
- 对于给定的命题公式，如果有一个等价公式，它仅由大项的合取式组成，则该等价式称作原式的主合取范式
- 在真值表中，一个公式的真值为F的指派所对应的大项的合取，即为该公式的主合取范式

例题

- 利用真值表，求$(P \wedge Q) \vee (P \wedge \neg R)$的主合取范式和主析取范式

P	Q	R	$(P \wedge Q) \vee (P \wedge \neg Q)$
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

- 主析取范式
  - 在真值表中，一个公式的真值为T的指派所对应的小项的析取，即为该公式的主析取范式
  - $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$
- 主合取范式
  - 在真值表中，一个公式的真值为F的指派所对应的大项的合取，即为该公式的主合取范式
  - $(P \vee \neg Q \vee R) \wedge (P \vee \neg Q \vee \neg R) \wedge (\neg P \vee Q \vee \neg R) \wedge (\neg P \vee \neg Q \vee \neg R)$ ×
  - $(\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$ √

例题

- 利用真值表，求$(P \wedge Q) \vee (P \wedge \neg R)$的主合取范式和主析取范式

- 主析取范式
  - 在真值表中，一个公式的真值为T的指派所对应的小项的合取，即为该公式的主析取范式
  - $(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$
  - $m_{111} \vee m_{110} \vee m_{011} \vee m_{001}$
  - 说明m_{101}，m_{100}，m_{010}，m_{000} 在真值表中的为F
  - 对应到大项为$(\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$ (主合取)
  - $M_{101} \wedge M_{100} \wedge M_{010} \wedge M_{000}$

- 主合取范式
  - 在真值表中，一个公式的真值为F的指派所对应的大项的合取，即为该公式的主合取范式
  - $(\neg P \vee Q \vee \neg R) \wedge (\neg P \vee Q \vee R) \wedge (P \vee \neg Q \vee R) \wedge (P \vee Q \vee R)$
  - $M_{101} \wedge M_{100} \wedge M_{010} \wedge M_{000}$
  - 说明$M_{111} \vee M_{110} \vee M_{011} \vee M_{001}$ 在真值表中的为T
  - 对应到小项为$(P \wedge Q \wedge R) \vee (P \wedge Q \wedge \neg R) \vee (\neg P \wedge Q \wedge R) \vee (\neg P \wedge \neg Q \wedge R)$ (主析取)
  - $m_{111} \vee m_{110} \vee m_{011} \vee m_{001}$

证明方法 习题课

黄祥 陈剑豪 包予恒

作业情况概括

- 讲解内容
  - P1
  - P2
  - P12
  - 思考题
- 平均分
  - 98

Problem 1

- 试符号化以下各命题，并根据前提推证结论是否有效。
- 前提：
  - (1) 有的病人喜欢所有的医生
  - (2) 没有一个病人喜欢庸医
- 结论：
  - 没有医生是庸医

Problem 1

参考答案：定义 $P(x)$ 表示 x 是病人，$D(x)$ 表示 x 是医生，$Q(x)$ 表示 x 是庸医，$L(x,y)$ 表示 x 喜欢 y。

前提：(1) $\exists x(P(x) \land \forall y(D(y) \to L(x,y)))$

(2) $\forall x(P(x) \to \forall y(Q(y) \to \neg L(x,y)))$

结论：$\forall x(D(x) \to \neg Q(x))$

证明：

(a)	$P(c) \land \forall y(D(y) \to L(c,y))$	(1) 的存在例示
(b)	$P(c) \to \forall y(Q(y) \to \neg L(c,y))$	(2) 的全称例示
(c)	$P(c)$，$\forall y(D(y) \to L(c,y))$	(a) 化简
(d)	$D(y) \to L(c,y)$	(b) 全称例示
(e)	$\forall y(Q(y) \to \neg L(c,y))$	(b) (c) 假言推理
(f)	$Q(y) \to \neg L(c,y)$	(e) 的全称例示
(g)	$L(c,y) \to \neg Q(y)$	(f) 的等价命题
(h)	$D(y) \to \neg Q(y)$	(d) (g) 假言三段论
(i)	$\forall x(D(x) \to \neg Q(x))$	(h) 的全称生成

- 前提：
  - (1) 有的病人喜欢所有的医生
  - (2) 没有一个病人喜欢庸医
- 结论：
  - 没有医生是庸医。

Problem 2

- 请运用命题逻辑进行表示，并证明下列推理。
  - （1）“今天海面不平稳并且紫外线不强”
  - （2）“若今天海面不平稳或紫外线很强，则探险队不出海”，
  - （3）“若探险队不出海，则探险队将修理船只”，
  - （4）“若探险队修理船只，则探险队在晚上发布行程记录”
- 证明结论
  - “探险队在晚上发布行程记录”

Problem 2

p：今天海面平稳，q：今天紫外线不强，r：探险队出海，s：探险队修理船只，t：探险队在晚上发布行程记录

表示：$\neg p \wedge q$，$\neg p \vee \neg q \to \neg r$ ，$\neg r \to s$，$s \to t$，证明 t

1. $\neg p \wedge q$
2. $\neg p$
3. $\neg p \vee \neg q$
4. $\neg r$ （$\neg p \vee \neg q \to \neg r$）
5. s （$\neg r \to s$）
6. t （$s \to t$）

- 前提
  - （1）“今天海面不平稳并且紫外线不强”
  - （2）“若今天海面不平稳或紫外线很强，则探险队不出海”，
  - （3）“若探险队不出海，则探险队将修理船只”，
  - （4）“若探险队修理船只，则探险队在晚上发布行程记录”
- 证明结论
  - “探险队在晚上发布行程记录”

Problem 7

- 有一个$n * n$的方格表，先允许从中任意选择$n - 1$个方格涂为黑色，然后再逐步地将那些至少与两个已涂黑的方格相邻的方格也涂为黑色。证明，不论怎样选择最初的$n - 1$个格，都不能按这样的法则涂黑所有的方格。
  - 假设能够涂黑所有的方格，那么作为黑色区域来说，方格纸的边界就是区域的边界，如果将每个小方格的边长记作1, 那么黑色区域的边界总长就应达到$4n$。
  - 但是，在一开始时，黑色区域仅包括$n - 1$个小方格, 即使它们都互不相邻，那么区域的边界长度也仅为$4(n - 1)$
  - 而在以后的逐步扩大黑色区域的面积的过程中，由于只能涂黑那些至少已与黑色区域有两条公共边的方格，因此面积的扩大并不带来边界总长度的增加，从而边界总长度将始终不会超过$4(n - 1)$
  - 上述两桩事实是相互矛盾的

Problem 12

- a) **证明或驳斥**: 如果a 和b 是有理数，那么a^b一定也是有理数。
  - 不成立， $a = 2, b = \frac{1}{2}$
- b) 是否存在a 和b 是无理数，使得a^b是有理数。
  - 考虑$\sqrt{2}^{\sqrt{2}}$是否为有理数
  - 若是，则成立
  - 若不是，则令$x = \sqrt{2}^{\sqrt{2}}, y = \sqrt{2}$ ，x^y 为有理数，亦成立

思考题

证明：$4k+1$ 型的素数有无穷多个.

证明：$4k+3$ 型的素数有无穷多个.

证明：$4k+1$型的素数等于两个正整数的平方和.

思考题

证明：4k+1 型的素数有无穷多个.

- 方法1：证明$4\,n^2+1$的素因子p都是$4k+1$型的
  - 否则，$4\,n^2+1$ 有一个素因子$p = 4k+3$.
  - 考虑一个等式：$(2n)^{(p-1)} = (2n)^{4k+2} = (4\,n^2)^{2k+1}$
  - 已知 $p\,|(4\,n^2+1)$ （第一行的假设），从而 $4\,n^2 \equiv -1\,(mod\;p)$.
  - 因此，$(4\,n^2)^{2k+1} \equiv -1\,(mod\;p)$.（$2k+1$ 个$mod\;p = -1$的数的积还是-1），$(4\,n^2)^{2k+1} = (2\,n)^{2(2k+1)} = (2n)^{p-1} \equiv -1\,(mod\;p)$.
  - 但是，根据欧拉定理，$(2n)^{p-1} \equiv 1\,(mod\;p)$, 矛盾
    - 欧拉定理：若正整数a和n互素，则$a^{\varphi(n)} \equiv 1\,(mod\;n)$
    - 欧拉函数：$\varphi(n)$不大于n且与n互素的数的个数(n为素数时$\varphi(n) = n-1$)
    - 这里$2n$和p 互素，否则 $p\,|\,4n^2$

- 方法2：假设只有有限个$4k+1$型的素数，不妨设为$p_1,\ldots,p_n$,
  - 考虑 $m=(2p_1\ldots p_n)^2+1$， m的素因子都是$4k+1$型的(m是$4n^2+1$型，上一种方法的结论)
  - 但是，这些 p_i都不是 m的因子。矛盾。(否则$p_i|m$，即$p_i|(2p_1\ldots p_n)^2+1$)

思考题

证明：$4k+3$ 型的素数有无穷多个.

- 反证法，假设只有有限个$4k+3$型的素数，不妨设为$p_1,\ldots,p_n$,
- 考虑 $m=4(p_1\ldots p_n)-1=q_1\ldots q_l$， q_j是素数。
- 显然$q_j\neq p_i$ （否则$p_i|m$，即$p_i|q_1\ldots q_l$ 即 $p_i|4(p_1\ldots p_n)-1$）
- 因此， q_j都是$4k+1$型的（都是奇数，不可能是4k+2和4k型）
- 从而， $q_1\ldots q_l\equiv 1 \pmod 4$， 即 $m\equiv 1 \pmod 4$.（模4余1相乘还是余1）
- 但是， $4(p_1\ldots p_n)-1\equiv -1 \pmod 4$， 即 $m\equiv -1 \pmod 4$. 矛盾。

思考题

证明：4k+1型的素数等于两个正整数的平方和.

- 设素数$p=4k+1$，那么$p-i\equiv -i\ (mod\ p)$，$i=1,\dots,2k.$
- 有 $4k\ (4k-1)\dots(2k+1)\ \equiv\ (-1)\ (-2)\dots(-2k)\ (mod\ p)$
- $(4k)!\equiv \left((2k)!\right)^2\ (mod\ p)$ （两边同乘$2k!$，右边2k项的负号消掉）
- 由威尔逊定理，$(4k)!\equiv -1\ (mod\ p)$
  - 威尔逊定理：设p为大于1的正整数，则p为素数当且仅当$(p-1)!\ \equiv -1\ (mod\ p)$
- 令$e=(2k)!$ 我们有： $e^2\equiv -1\ (mod\ p)$.
- 考虑所有型如$ex+y$的数,其中x, y为非负整数,$x,y\ <\ sqrt\ p$. 则这样的数有$([sqrt\ p\ ]+1)^2$ 个 (0,1,⋯, $[sqrt\ p\ ]$)
- 由于$([sqrt\ p]+1)^2>p$, 所以必定有两个这样的数模p同余（这样的数的数量超过了p的数量）
- 即存在非负整数$a,b,c,d<sqrt\ p$,使$ea+b\equiv ec+d\ (mod\ p), ea+b\neq ec+d$.
- 从而$e(a-c)\equiv d-b\ (mod\ p)$
- 于是$-(a-c)^2\equiv (d-b)^2(mod\ p)$ （两边同时平方， $e^2\equiv -1\ (mod\ p).$）
- $(a-c)^2+(d-b)^2\ \equiv\ 0\ (mod\ p)$, 显然$0<(a-c)^2+(d-b)^2\ <2p\ (a,b,c,d\ <sqrt\ p)$
- 所以$(a-c)^2+(d-b)^2=p$. 于是p可以表示为两个正整数的平方和

集合与函数 习题课

黄祥 陈剑豪 包予恒

作业情况概括

- 讲解内容
  - 1
  - 2
  - 4
  - 5
  - 8
  - 11
  - 12
  - 13
  - 14
  - 15
  - 16
  - 18
  - 20
- 平均分：94

Prob1

- 判断下列等式中哪个等式为真。
  - f) $\{\emptyset\} \in \{\emptyset, \{\emptyset\}\}$ 真
  - g) $\{\{\emptyset\}\} \in \{\{\emptyset\}, \{\emptyset\}\}$ 假

Prob2

- 判断下列各集合是否为某集合的幂集。

a) $\emptyset$

b) $\{\emptyset, \{a\}\}$

c) $\{\emptyset, \{a\}, \{\emptyset, a\}\}$

d) $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

- 错解
  - a）认为是空集的幂集
    - {Ø}
  - c）认为是{Ø, a}的幂集
    - {Ø, {Ø}, {a}, {Ø,a}}

Prob4

令 $A_i = \{\dots, -2, -1, 0, 1, \dots, i\}$，求

a) $\bigcup_{i=1}^{n} A_i$

b) $\bigcap_{i=1}^{n} A_i$

答案:

a) $\{\dots, -2, -1, 0, 1, \dots, n\}$

b) $\{\dots, -2, -1, 0, 1\}$

- $A_1 = \{\dots, -2, -1, 0, 1\}$
- $A_2 = \{\dots, -2, -1, 0, 2\}$
- $A_n = \{\dots, -2, -1, 0, n\}$

Prob 5

令 f 为从 $\mathbf{R}$ 到 $\mathbf{R}$ 的函数 $f(x) = x^2 + 2x$。求

a) $f^{-1}(\{1\})$

b) $f^{-1}(\{x|0 < x < 1\})$

c) $f^{-1}(\{x|x > 3\})$

答案:

a) $\{-1 - \sqrt{2} - 1, -1 + \sqrt{2}\}$

b) $\{x| -1 - \sqrt{2} < x < -2 \vee 0 < x < -1 + \sqrt{2}\}$

c) $\{x|x < -3 \vee x > 1\}$

Prob 8

- 假定f 是从X 到Y 的函数，g 是从Y 到X 的函数。证明$f \circ g = I_Y$，$g \circ f = I_X$ 与$f^{-1} = g$，$g^{-1} = f$**等价**。其中I_X和I_Y 分别是X 和Y 上的恒等函数。
  - 1. 证明若$f \circ g = I_Y$，$g \circ f = I_X$, 则$f^{-1} = g$，$g^{-1} = f$:
    - I_X为双射，则$g \circ f$为双射，f 为单射，g 为满射。
    - 同理可知g 为单射f 为满射。于是f 和g 都为双射，
    - 存在反函数。所以$f^{-1} = g$，$g^{-1} = f$。
  - 2. 证明若$f^{-1} = g$，$g^{-1} = f$, 则$f \circ g = I_Y$，$g \circ f = I_X$:
    - 对任意$x \in X$，$f(x) = g^{-1}(x) = y \in Y$，有$f(x) = y$, $g(y) = x$。
    - 对任意$x \in X$，$g \circ f(x) = g[f(x)] = g(y) = x = I_X(x)$。$g \circ f = I_X$。
    - 反之同理。

Prob 11

计算下列集合的基数.

(1) $A=\{x,y,z\}$

(2) $B=\{x|x=n^2\wedge n\in N\}$

(3) $C=\{(x,y)|x,y\in N\}$

(4) 平面上所有的圆心在 x 轴上的单位圆的集合

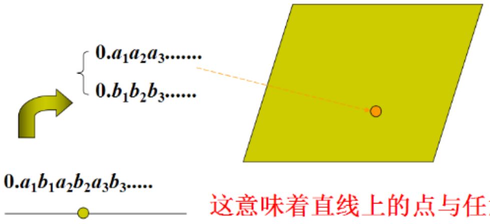
(5) 复数集合

- 若A与自然数n等势，则 $|A|=n$
- 若A与自然数集合N等势，则 $|A|=\aleph_0$
- 若A与实数集合R等势，则 $|A|=\aleph$

- (0,1)与整个实数集等势
  - 双射：$f:(0,1)\to R: f(x)=\mathrm{tg}(\pi x-\frac{\pi}{2})$
- 对任意不相等的实数a, b ($a<b$), $[0,1]$与$[a, b]$等势
  - 双射：$f:[0,1]\to[a,b]: f(x)=(b-a)x+a$

  (这实际上意味着：任意长的线段与任意短的线段等势)

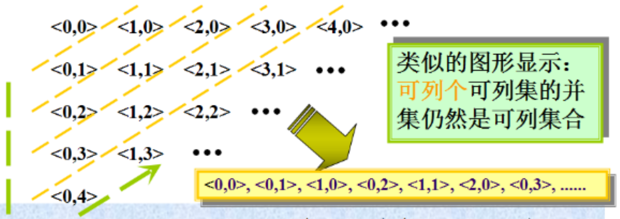
直线上的点集与平面上的点集等势



这意味着直线上的点与任意有限维空间的点“一样多”！

自然数集的笛卡儿积是可列集

- 所有的自然数对构成的集合与自然数集等势



$$I(m,n)=\sum_{i=1}^{m+n} i+m=\frac{(m+n)(m+n+1)}{2}+m$$

答案：

(1) 3 (2) $\aleph_0$ (3) $\aleph_0$ (4) $\aleph$ (5) $\aleph$

Pro 12

- 设*A*,*B* 为可数集，证明:
  - (1) $A \cup B$ 是可数集;

(1) 若两个集合都是有穷集，那么 $card(A \cup B) = n + m \le \aleph_0$. 若其一为有穷集，另一为无穷可数集，不妨设 A 为其中的有穷集且 $card(A) = n$，则可以构造如下双射 $h : A \cup B \to N$. 当 $x \in A$ 时，若 $x = a_i$，则 $h(x) = i$；当 $x \in B$ 时，若 $x = b_j$，则 $h(x) = j + n$. 如果 $card(A) = card(B) = \aleph_0$，那么存在双射 $f : A \to N$ 和 $g : B \to N$. 如下构造函数 $h : A \cup B \to N$，

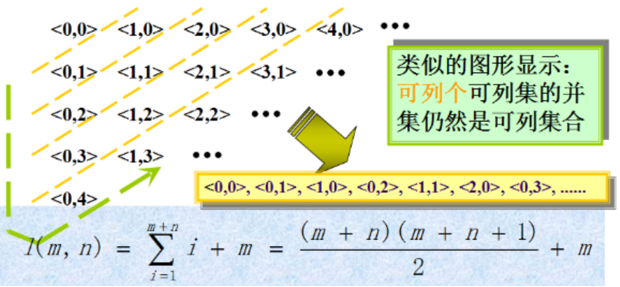
$$h(x) = \begin{cases} 2i, & \text{若} x \in A \text{且} x = a_i \\ 2j + 1, & \text{若} x \in B \text{且} x = b_j \end{cases}$$

显然 h 为双射. 这就证明了 $card(A \cup B) = \aleph_0$.

Pro 12

- 设A,B 为可数集，证明：
  - (2) $A \times B$ 是可数集.

- 所有的自然数对构成的集合与自然数集等势



(2) 若两个集合都是有穷集，那么 $card(A \times B) = n \cdot m \leq \aleph_0$. 若其一为有穷集，另一为无穷可数集，不妨设 A 为其中的有穷集，可以构造双射 $h : A \times B \to N$。$h(< ai, bi >) = i + jn$. 如果 $card\,A = card\,B = \aleph_0$，那么存在双射 $f : A \to N$ 和 $g : B \to N$. 构造函数 $h : A \times B \to N$，

$$h(< x, y >) = \frac{(i+j+1)(i+j)}{2} + i,\ \text{其中}\ f(x) = i, g(y) = j$$

显然 h 是双射的. 从而得到 $card(A \times B) = \aleph_0$.

Pro 14

- 设$A = \{a,b,c\}$，$B = \{0,1\}^A$，由定义证明$P(A) \approx \{0,1\}^A$.

答案： $\mathcal{P}(A) = \{,\{a\},\{b\},\{c\},\{a,b\},\{a,c\},\{b,c\},\{a,b,c\}\}$，$\{0,1\}^A = \{f_0,f_1,f_2,f_3,f_4,f_5,f_6,f_7\}$，构造双射函数 f.

$f() = f_0$，$f(\{a\}) = f_1$，$f(\{b\}) = f_2$，$f(\{c\}) = f_3$，

$f(\{a,b\}) = f_4$，$f(\{a,c\}) = f_5$，$f(\{b,c\}) = f_6$，$f(\{a,b,c\}) = f_7$，

根据等势的定义有 $\mathcal{P}(A) \approx \{0,1\}^A$. 请注意题意要求等势定义证明.

2^S的记法 [编辑]

在集合论中，X^Y是由所有从Y到X的函数构成的集合。因为2可以定义为$\{0,1\}$（见自然数），2^S这集合包含了所有从S到$\{0,1\}$的函数。把2^S内的函数对应于由这函数给出的1的原像，可看出在2^S和$\mathcal{P}(S)$之间存在双射，其中每个函数是$\mathcal{P}(S)$中这函数所对应的子集的特征函数。所以就集合论来说2^S和$\mathcal{P}(S)$是相同的。

Pro 15

令 $\{1,2,3\}^\omega$ 为所有仅由数字 1, 2 或 3 构成的无限长的序列的集合。证明该集合不可数。

答案： *方案 1:* 假设 $\{1,2,3\}^\omega$ 可数，则我们将其中所有元素按照某种顺序列出:

$$L_1 = a_{11}a_{12}a_{13}\dots$$
$$L_2 = a_{21}a_{22}a_{23}\dots$$
$$L_3 = a_{31}a_{32}a_{33}\dots$$
$$\dots\dots$$

使用下列规则构造一个新的串 L

$$\mathrm{L} = a_1a_2a_3\dots$$

其中

$$a_i = \begin{cases} 2 & \text{若 } a_{ii} = 1 \\ 1 & \text{若 } a_{ii} \neq 1 \text{ 或 } L_i \text{ 长度小于 } 1 \end{cases}$$

则 L 显然与所有列出的 $\{1,2,3\}^\omega$ 中的元素都不同，与 $\{1,2,3\}^\omega$ 中所有元素均可列出矛盾。因此 $\{1,2,3\}^\omega$ 不可列，所以不可数。

实数集不是可列集

- **(0,1)不是可数集 //注意：(0,1)与实数集合等势**
  - **"对角线证明法"**

假设(0,1)中的所有元素可以按照某种顺序列出：

$$0.b_{11}b_{12}b_{13}b_{14}\dots$$
$$0.b_{21}b_{22}b_{23}b_{24}\dots$$
$$0.b_{31}b_{32}b_{33}b_{34}\dots$$
$$0.b_{41}b_{42}b_{43}b_{44}\dots$$
$$\vdots$$

则$0.b_1b_2b_3\dots(b_i\neq 9,\ b_i\neq b_{ii})$不在上述序列中。

Pro 16

计算：

a) $23300 \bmod 11$ b) $2^{3300} \bmod 31$ c) $3^{516} \bmod 7$

答案：

a) 2。$23300 = 233 * 10 * 10 = (21 * 11 + 2) * 10 * 10 \equiv 2 * (-1) * (-1) \equiv 2(mod 11)$

b) 1。$2^{23300} \equiv 2^{5*4660} \equiv 32^{4660} \equiv 1^{4660} \equiv 1(mod 31)$

c) 1。$3^6 \equiv 1(mod 7), 3^{516} \equiv 3^{6*86} \equiv 1(mod 7)$

Pro 18

- 借助于费马小定理证明如果n 是一个正整数，则42 能整除n^7-n。
  - 只需证明7 能整除n^7-n且6 能整除n^7-n
  - 先证7 能整除n^7-n：根据费马小定理，若a 不是p 的倍数，则$a^{p-1}\equiv 1\ (mod\ p)$，取$a=n$，$p=7$，
    - 若n 是7 的倍数7 能整除n^7-n显然成立
    - 若n 不是7 的倍数，则$a^6\equiv 1\ (mod\ 7)$，即$7|(\mathrm{n}^6-1)$,7 能整除n^7-n也同样成立。
  - 再证明6 能整除n^7-n：$n^7-n=n(n-1)(n2+n+1)(n+1)(n2-n+1)$，$(n-1)n(n+1)$ 必然被2 和3 整除，所以6 能整除n^7-n。
  - 综上，42 能整除n^7-n。

Pro 20

证明：若 m 和 n 互质，则 $m^{\phi(n)} + n^{\phi(m)} \equiv 1(\mathrm{mod}\ mn)$.

答案： 由欧拉定理，$m^{\phi(n)} \equiv 1(mod\ \ n)$，即 $n|m^{\phi(n)} - 1$. 同理 $m|n^{\phi(m)} - 1$。

从而，$mn|(m^{\phi(n)} - 1)(n^{\phi(m)} - 1)$，即 $mn|m^{\phi(n)}n^{\phi(m)} - (m^{\phi(n)} + n\phi(m) - 1)$. 而 $mn|m^{\phi(n)}n^{\phi(m)}$ ，故有 $mn|m^{\phi(n)} + n^{\phi(m)} - 1$

得证 $m^{\phi(n)} + n^{\phi(m)} \equiv 1(mod\ \ mn)$。

归纳与递归 习题课

黄祥 陈剑豪 包予恒

作业情况概括

- 本次内容
  - 5, 9-16
- 均分
  - 91.4

Pro 5

正整数 n 的拆分是把 n 写成正整数之和的方式. 例如, $7=3+2+1+1$ 是 7 的拆分. 设 P_m 等于 m 的不同分拆的数目, 其中和式里项的顺序无关紧要, 并设 $P_{m,n}$ 是用不超过 n 的正整数之和来表示 m 的不同方式数.

a) 证明: $P_{m,n}=P_m$.

b) 证明: 下面的 $P_{m,n}$ 的递归定义是正确的.

$$P_{m,n}=\begin{cases} 1 & m=1 \\ 1 & n=1 \\ P_{m,m} & m<n \\ 1+P_{m,m-1} & m=n>1 \\ P_{m,n-1}+P_{m-n,n} & m>n>1 \end{cases}$$

a) m 无法用于大于 m 的数参与分拆，因此 $P_{m,m}=P_m$.

b) 证明: 对定义逐条证明: $m=1$ 时，只有一种拆分方法，即 1 本身，因此 $P_{1,n}=1$. n $=1$ 时，只有一种拆分方法，即拆成 m 个 1 的和，因此 $P_{m,1}=1$. $m<n$ 时，由 (a) 中证明可知，此时 n 的大小不影响结果，因此等于 $P_{m,m}$. $m=n>1$ 时，存在 $m=m$ 这种拆分方式，以及其他 $P_{m,m-1}$ 种拆分方式，因此等于 $1+P_{m,m-1}$. $m>n>1$ 时，存在不含 n 的拆分 ($P_{m,n-1}$) 和包含 n 的拆分 ($P_{m-n,n}$) 两种情况, 因此等于 $P_{m,n-1}+P_{m-n,n}$.

Pro 5

正整数 n 的拆分是把 n 写成正整数之和的方式. 例如, $7=3+2+1+1$ 是 7 的拆分. 设 P_m 等于 m 的不同分拆的数目, 其中和式里项的顺序无关紧要, 并设 $P_{m,n}$ 是用不超过 n 的正整数之和来表示 m 的不同方式数.

a) 证明: $P_{m,n}=P_m$.

b) 证明: 下面的 $P_{m,n}$ 的递归定义是正确的.

$$P_{m,n}=\begin{cases}1 & m=1\\ 1 & n=1\\ P_{m,m} & m<n\\ 1+P_{m,m-1} & m=n>1\\ P_{m,n-1}+P_{m-n,n} & m>n>1\end{cases}$$

c) 用这个递归定义求出 5 和 6 的拆分数.

c) $P_5=7, P_6=11.$

Pro 9

- 某班有学生60 人，其中有38 人学习PASCAL 语言，有16 人学习C语言，有21 人学习COBOL 语言；有3 个人这三种语言都学习，有2 个人这三种语言都不学习，问仅学习两门语言的学生数是多少?

答案： 设 A、B、C 分别表示学习 PASCAL、C、COBOL 的学生的集合。因 $|A\cup B\cup C| = |U| - |\overline{A}\cap\overline{B}\cap\overline{C}| = 58$。由容斥原理，有 $|A\cup B\cup C| = |A| + |B| + |C| - |A\cap B| - |A\cap C| - |B\cap C| + |A\cap B\cap C|$，则 $|A\cap B| + |A\cap C| + |B\cap C| = |A| + |B| + |C| + |A\cap B\cap C| - |A\cup B\cup C| = 20$。又因 $|A\cap B\cap\overline{C}| = |A\cap B| - |A\cap B\cap C|$，从而有：$|A\cap B\cap\overline{C}| + |A\cap\overline{B}\cap C| + |\overline{A}\cap BC\cap C| = |A\cap B| + |B\cap C| + |A\cap C| - 3|A\cap B\cap C| = 11$。即仅学习两门外语的学生数是 11 人。

Pro 10

- 长度为$n(n > 5)$ 且以123 开始或以321 结尾的三进制串有多少个?
  - $3^{n-3} + 3^{n-3} - 3^{n-6} = 53 * 3^{n-6}$

隔板法

- **隔板法**就是在n个元素间的（n-1）个空插入k-1个板子，把n个元素分成k组的方法。
- 非空隔板法
  - 将n个相同的求放到m个不同的盒子里的个数为：$C(m-1，n-1)$
- 可为空的隔板法
  - 等于把$n+m$个求放进m个盒子里，不允许空盒子
  - $C(\mathrm{n}+m-1, m-1)$

Pro 11

- 长度为12 且不包含“11” 子串的二进制串有多少个?
  - 最多6个1
  - 假设有k个1的时候满足条件的二进制串集合为A_k， 每个1之间的k-1个距离为$a_1, \ldots a_{k-1}$(正整数)，第一个1之前，最后一个1之后的0的个数为x_1, x_k(非负整数)
  - $|A_k|$相当于$x_0 + a_1 + \cdots + a_{k-1} + x_k = 12 - k$
  - 令$x_i = a_i - 1, i = 1,2, \ldots, k - 1$
  - 转化为$a_0 + a_1 + \cdots + a_{k-1} + a_k = 13 - 2k$ 的非负整数解个数（13-2k个球放到k+1个盒子里，非空）
  - $|A_k| = C(13 - k, 13 - 2k)$
  - $|A_k| = C(13,13) + C(12,11) + +C(11,9)+ C(10,7) + C(9,5) + +C(8,3) + C(7,1)$
  - 共377

Pro 13

- 设x_1、x_2、x_3、x_4、x_5 和x_6 是正整数, 方程$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 < 32$ 有多少个解?
  - 非空隔板法，考虑$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 = 32$,6个隔板31个位置
  - $6 \le y \le 31, \sum \ C(y-1,5)$
    - $C(5,5) + C(6,5) + \cdots + C(30,5)$
    - $C(6,6) + C(6,5) + \cdots + C(30,5)$
    - $C(7,6) + C(7,5) + \cdots + C(30,5)$
    - ...
    - $C(31,6)$
    - 736281

Pro 12

- 从1000 到9999 之间, 包含多少个正整数
- a) 被9 整除?
  - 1000
- b) 被5 或7 整除?
  - 被5 整除的有1800 个， 被7 整除的有1286 个， 被35 整除的有257 个， 答案为1800 + 1286 – 257 = 2829。
- c) 是偶数?
  - 4500
- d) 不被5 也不被7 整除?
  - 9000 – 2829 = 6171

Pro 12

- 从1000 到9999 之间, 包含多少个正整数
- e) 有不同的十进制数字?
  - $9 \times 9 \times 8 \times 7 = 4536$。
- f) 被5 整除但不被7 整除?
  - 即被5 整除且不被35 整除的正整数个数，答案为1800 – 257 = 1543。
- g) 不被3 整除?
  - 6000
- h) 被5 和7 整除?
  - 即被35 整除的正整数个数，答案为257

Pro 14

- 由一个正n 边形的顶点构成的三角形有多少个？如果正n 边形的边不能是构成三角形的边，这样的三角形又有多少个

答案： 从 n 边中选三点的情况有 $\mathcal{C}(n,3)=\frac{n(n-1)(n-2)}{6}$ 种.

如果三角形的边是正 n 边形的边有两种情况，第一种是有一条边是正 n 边形的边，这种情况有 $(n-4)\times n$ 种，第二种是有两条边是正 n 边形的边，这种情况有 n 种，

则三角形的边不是正 n 边形的边的情况有 $\mathcal{C}(n,3)-(n-4)n-n=\frac{n(n-4)(n-5)}{6}$ 种。

Pro 15

给出关于 $\sum_{k=1}^{n} k * C(n,k) = n * 2^{n-1}$ 的组合证明。

答案：从 n 个人中，选择一个委员会（委员会大小为 1 n 任意），并选择一个委员会的领导。总的方式数有两种计算方法。可以首先选择领导，再选择委员会。从 n 个人中选取一个领导，共有 n 种选择，并从剩下 n-1 个人中选择委员会的其他成员，有 $2^n - 1$ 种选择，总共有 $n * 2^n - 1$ 种选择。也可以首先选取一个委员会，再选择领导。当委员会大小为 k 时，从 n 个人中选大小为 k 的委员会有 $C(n,k)$ 种选择，从大小为 k 的委员会选择领导共有 k 种选择，因此总的选择方式共有 $\sum_{k=1}^{n} k * C(n,k)$ 种。

Pro 16

考虑一个 $N \times N$ 网格，其中的每一个单元格可以取值 $+1$ 或 -1。我们称这种网格为二进制网格 *(Binary grid)*。任何行的行乘积 *(row product)* 都被定义为该单行中所有元素的乘积。同样，一列的列乘积 *(column product)* 被定义为该单个列中所有元素的乘积。如果 N 行的行乘积中，有且只有一个结果为 -1，而 N 列的列乘积中，有且只有一个结果为 -1，则该 $N \times N$ 的二元网格称为魔术网格。换句话说，魔术网格要求其他 $N-1$ 个行乘积全部为 $+1$，其他 $N-1$ 个列乘积应也全部为 $+1$。试计算所有 $N \times N$ 的网格中，魔术网格的数量。

答案： 1) 确定要使其行列乘积为 -1 的行和列. 可以有 n 种方式选择行，对于选定的每一行，可以有 n 种方式选择列：总共 n^2 种方式。

2) 现在，随机填充剩余的 $(n-1)^2$ 个单元格 (都不属于先前选择的行或列)。这可以有 $2^{(n-1)^2}$ 种方式。

3) 我们填充所选行和列的单元格. 请注意，在第 2 步之后，我们得到一个 $N \times N$ 的网格，所有行和列乘积都已知。此时，填充第一步选中的行和列。显然，对于该行和列中的元素，是可以唯一地确定要插入的数字的符号。换句话说，只有一种填充方式. 注意所选行和列相交的单元格可以用来使该行该列乘积同时为-1，这是因为其为所有行乘积乘以所有列乘积为偶数（每个数算两次）。

第七次习题课

陈剑豪，黄祥，包予恒

作业：排列组合&离散概率

- 讲解内容
  - 1，3，9，13，15，16

Prob1

由m 个A 和n 个B 构成序列, 其中m, n 为正整数, $m \le n$. 如果要求每个A 后面至少紧跟一个B, 问：有多少个不同的序列.

答案： 方法一：先放n 个B , 只有一种放法. 然后在每个B 之间的n 个空档选择m 个放A, 每个空格至多放一个A，共C(n,m) 种放法.

C（n-m, m+1）

方法二：先放m 个AB, 只有一种放法. 把AB 看成隔板, m 个隔板共构成m+ 1 个空格, 在空格中放入n −m 个B, 这时每个空格可放多个B. 因此适用不定方程求解模型：求$x_1 + x_2 + \cdots + x_{m+1} = n - m$ 的非负整数解个数.

答案是C(n − m + m + 1 − 1, n − m) = C(n, n − m) = C(n,m).

相同物体分配到不同盒子

- n个相同物体分配到k个不同的盒子中，有多少种分配方案?

$x_1+\ldots+x_k=n$ 的非负整数解

$\boldsymbol{x}_1$个0 | … | $\boldsymbol{x}_k$个0

含n个0和(k-1)个1的0-1串，C (n+k-1, n)

Problem 3

- 用3 个1, 2 个2, 5 个3, 这十个数字能构成多少个能被2 整除的四位数?
- **答案：**
- • 十位为2: $2 \times 2 = 4$ 种
- • 百位为2: $2 \times 2 = 4$ 种
- • 千位为2: $2 \times 2 = 4$ 种
- • 没有2: $2 \times 2 \times 2 = 8$ 种.
- 总共20 种.

Problem 9

设 p 和 q 是素数且 n = pq。随机选择小于 n 的正整数，该正整数不被 p 或 q 整除的概率是多少？

答案： 易知， p, 2p, 3p, . . . ,(q – 1)p 都可以被 p 整除。这里有 q – 1 个数被 p 整除，同理可知，有 p – 1 个数可以被 q 整除。由于 p 和 q 都是素数，他们的最小公倍数是 n，所以不存在一个能同时被 p 和 q 整除的小于 n 的正整数。所 以，随机选择的正整数不被 p 或 q 整除的概率是 1-[(p +q – 2)/(pq-1)]。

Problem 13

当一个均匀的骰子被掷10 次时，出现偶数点的次数的方差是多少?

答案：设随机变量*X* 是骰子抛掷十次的结果, 根据独立性

$V(x) = n(p - p^2) = 10 \times (\frac{1}{2} - (\frac{1}{2})^2) = 2.5.$

比安内梅公式的应用

- 例：求扔两个骰子点数之和的方差
  - 第一个骰子点数与第二个骰子点数两个随机变量相互独立；故可使用Bienaymé公式

$$\mathrm{Var}[X_1 + X_2] = \mathrm{Var}[X_1] + \mathrm{Var}[X_2]$$
$$= \frac{35}{12} + \frac{35}{12} = \frac{35}{6}$$

Problem 15

某人爱说谎, 三句只能信两句. 他扔了一个骰子, 报告说是“四点”. 问这个骰子真是四点的概率是多少?

答案:

$$P = \frac{P(\text{骰子真是四点})}{P(\text{某人说是四点})}$$

$$= \frac{(P(\text{扔到四点}) \times P(\text{没有说谎}))}{(P(\text{不是四点}) \times P(\text{说谎是四点}) + P(\text{扔到四点}) \times P(\text{没有说谎}))}$$

$$= (2/3 \times 1/6)/(5/6 \times 1/3 \times 1/5 + 2/3 \times 1/6) = 2/3$$

Problem 16

假设现在有100 个座位, 从1 号到100 号, 从其中随机选择25 个座位, 所选的连续座位对的期望是多少?(譬如{1, 2}就是一个连续座位对).

答案： 一共有 99 个连续座位对: {1, 2}, {2, 3}, ..., {99, 100}, 每个连续座位对被选择的概率是$\frac{25}{100}\times\frac{24}{99}$。总座位对的期望是 $99\times\frac{25}{100}\times\frac{24}{99}=6$.

例：Expected Value in the Hatcheck Problem

- 负责寄存帽子的服务生把帽子搞乱了，只能随机发还。问他可以期望还对几个？
  - 令$X_i = 1$ 若第 i 个客人拿到他的帽子；否则 $= 0$。

$$X = X_1 + X_2 + \cdots + X_n$$

$$\mathrm{Ex}[X_i] = 1 \cdot \Pr[X_i = 1] + 0 \cdot \Pr[X_i = 0] = \frac{1}{n}$$

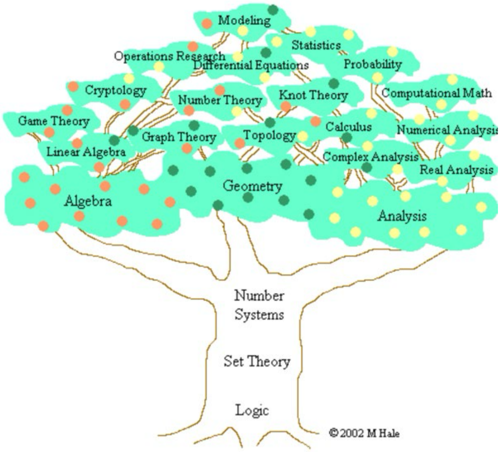
$$\mathrm{Ex}[X] = \mathrm{Ex}[X_1] + \mathrm{Ex}[X_2] + \cdots + \mathrm{Ex}[X_n] = n \cdot \frac{1}{\mathrm{n}} = 1$$

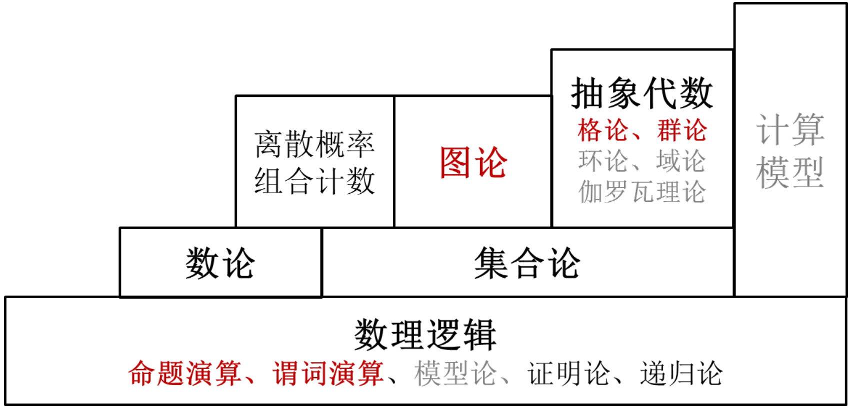
小结

- 条件概率与贝叶斯定理
- 随机变量及其期望、方差（特别注意线性特性）

Outline

- 数理逻辑
  - 命题逻辑
  - 谓词逻辑
  - 集合论
- 数论
- 组合
  - 组合计数
  - 离散概率
- 代数
  - 二元关系
  - 格论





数理逻辑

- 命题逻辑
  - 真值表
  - 常用的逻辑等价定律
  - 合取范式/析取范式
  - 命题推理规则
- 谓词逻辑
  - 前束范式
  - 谓词推理规则
- 证明方法
  - 归谬
  - 数学归纳法
- 集合论
  - 基数
  - 等势关系
  - 可数集

- 怎么写命题逻辑和谓词逻辑的推理?
- 命题逻辑和谓词逻辑最大的区别?
  - 谓词逻辑必须有谓词、变量、量词!
- 怎么叙述一个归纳过程?
- 怎么讨论集合的势（基数）?

自然演绎规则

怎么写命题逻辑的推理？

- 假言推理　　$p, p \to q \vdash q$
- 取拒式　　$\neg q, p \to q \vdash \neg p$
- 假言三段论　　$p \to q, q \to r \vdash p \to r$
- 析取三段论　　$\neg p, p \vee q \vdash q$
- 附加律　　$p \vdash p \vee q$
- 化简律　　$p \wedge q \vdash p$
- 合取律　　$p, q \vdash p \wedge q$
- 消解律　　$p \vee q, \neg p \vee r \vdash q \vee r$

怎么写谓词逻辑的推理？

基于规则的推理（举例）

$$\exists x(C(x) \land \neg B(x)),\ \forall x(C(x) \to P(x)) \Rightarrow \exists x(P(x) \land \neg B(x))$$

因为 $\exists x(C(x)\land\neg B(x))$　　//这是前提

根据存在例示，有某个a，$C(a)\land\neg B(a)$成立。

根据化简，得到$C(a)$ 成立，$\neg B(a)$成立。

因为$\forall x(C(x)\to P(x))$　　//这是前提

根据全称例示，得到 $C(a)\to P(a)$

根据假言推理，得到 $P(a)$

根据合取律，得到 $P(a)\land\neg B(a)$

根据存在生成，得到 $\exists x(P(x)\land\neg B(x))$

怎么叙述一个归纳过程？

- 归纳法：$P(0)$成立，如果$\forall m \le n. P(m)$成立，**要是能证明$\boldsymbol{P(n+1)}$成立……**
  - $P(0), \forall n. \left(\forall m \le n. P(m)\right) \to P(n+1) \vdash \forall P(n)$
  - 要处理的是还不知道是不是成立的$P(n+1)$，不是$P(n)$
  - 如$P(n+1) = \forall x. Q(n+1, x) \to R(x)$，要处理所有$x \in \{x | Q(n+1, x)\}$

怎么讨论集合的势（基数）？

- 不要做任意的基数算术
  - $|S| + |T| \stackrel{\text{def}}{=} |S \cup T|$
- 利用已知的基数
  - $0,1,2,\dots,\aleph_0,\aleph_1$
- 可用的比较方式
  - a到b**存在双射**， a和b的基数相同， $|a| = |b|$
  - a到b**存在单射**，a的基数小于等于b的，$|a| \leq |b|$
  - $|a| < |b| \stackrel{\text{def}}{=} (|a| \leq |b|) \wedge \neg(|a| = |b|)$
- 证明存在不要写“可以对应”，把相应的映射写出来
  - 特殊的A到$\aleph_0$有单射的写法：记A中的元素为$a_1, a_2, a_3 \dots$

证明方法中各种常见问题

- 考虑好逆否命题和充分条件、必要条件，不要写半个证明
  - 一般来说，直接写出一个逆否命题不叫证明叫抄题

数论, 代数

- 数论
  - 高斯同余、算术中国剩余定理、费马小定理、欧拉定理…
- 二元关系
  - 关系的性质，自反、对称、传递…
  - 关系的闭包(Warshall算法)
  - 等价关系（集合的划分）
- 格论（偏序集与格）
  - 偏序与全序
  - 哈斯图
  - 极大（小）元，最大（小）元
  - 上（下）确界
  - 链和反链
  - 格的定义

- 怎么判定一个性质?

怎么判定一个性质？

- 按照定义把所有条件列出来，不要省略
  - E.g.,

    对于任意素数p，定义集合$S = \{1,2,\cdots,p-1\}$上的关系

    $$R = \{(a,b) \mid a = b \vee ab \equiv 1 \pmod p), a \in S, b \in S\}$$

    试问R是否为等价关系？若是，请给出证明；若否，请给出反例.
  - $\forall a. (a,a) \in R$?
  - $\forall a. \forall b. (a,b) \in R \to (b,a) \in R$?
  - $\forall a. \forall b. \forall c. \big((a,b) \in R \wedge (b,c) \in R\big) \to (a,c) \in R$?

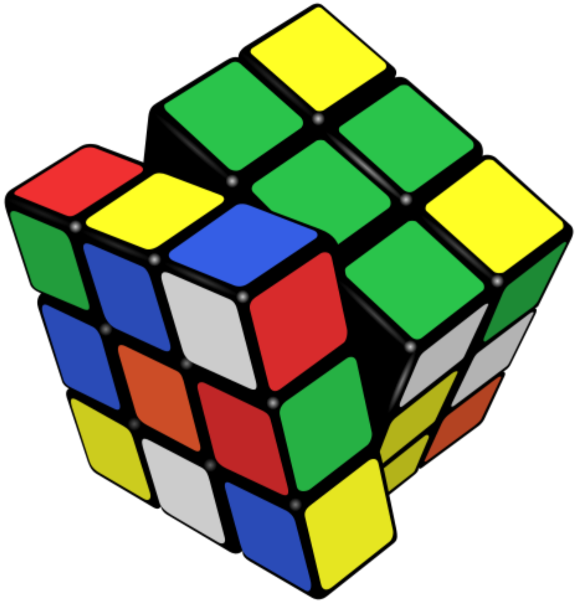
第八周习题课

离散数学

南京大学计算机科学与技术系

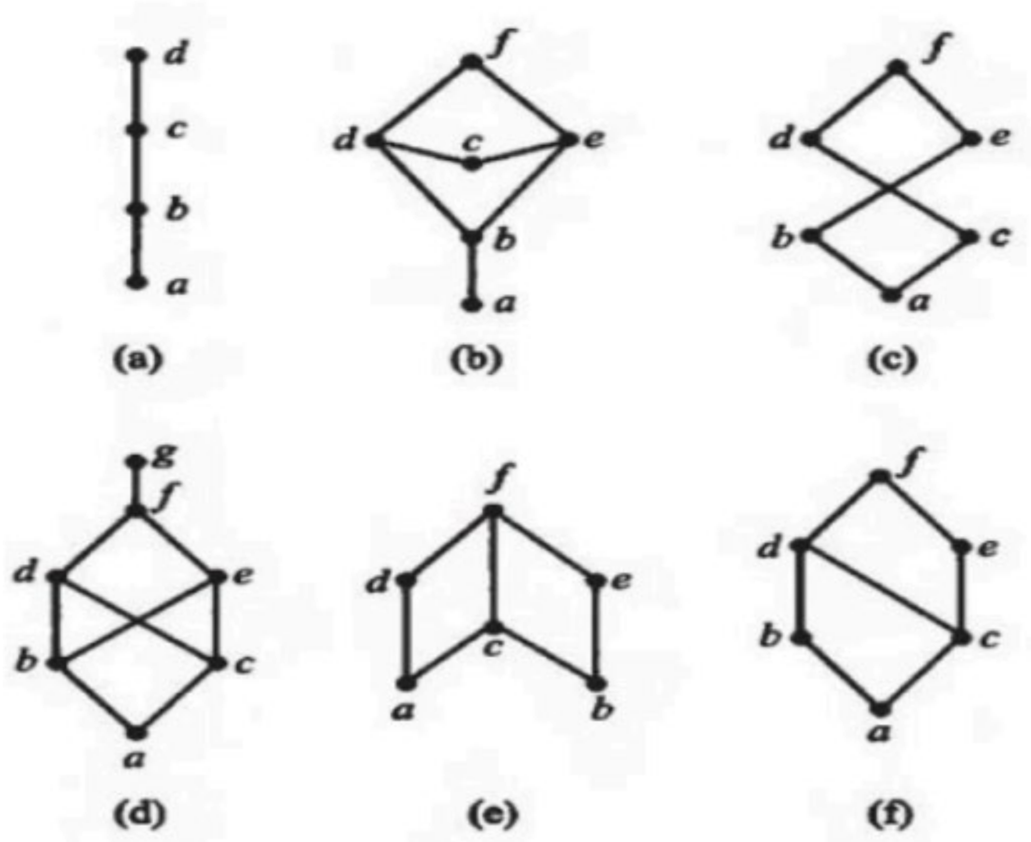
内容提要

- 偏序集与格
- 期中考试试题



Problem 6

下图给出了 6 个偏序集的哈斯图. 判断其中哪些是格. 如果不是格, 请说明理由.

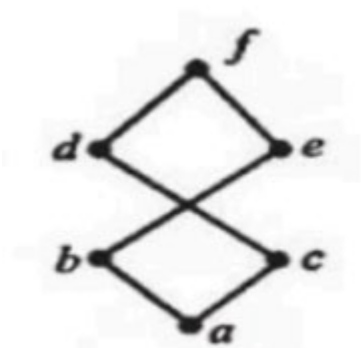


答案: (a),(c),(f) 是格. (b),(d),(e) 不是格. 在 (b) 中 {d, e} 没有最大下界. 在 (d) 中 {d, e} 没有最大下界. 在 (e) 中 {a, b} 没有最大下界.

Problem 7

格 Problem 6 (c) 的哪些元素有补元? 对于有补元的元素, 写出其补元.

补元的定义: 设<A, ∧, ∨, 0, 1> 是有界格, a∈A, 若存在 b ∈A, 使得 a ∨ b=1, 且 a ∧ b =0, 称b是a的补元。

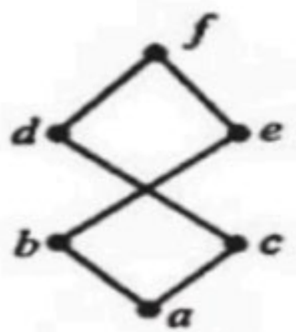


(c)

答案：所有元素都有补元. a 与 f 互为补元, b 的补元是 c 和 d, c 的补元是 b 和 e, d 的补元是 b 和 e, e 的补元是 c 和 d.

Problem 8

说明格 Problem 6 (c) 是否为分配格, 有补格或布尔格.



(c)

定义 11.5 设 $<L, \wedge, \vee>$ 是格，若 $\forall a, b, c \in L$，有

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

成立，则称 L 为分配格.

定义 11.9 设 $<L, \wedge, \vee, 0, 1>$ 是有界格，若 $\forall a \in L$，在 L 中都有 a 的补元存在，则称 L 是有补格.

例如图 11.7 中的 L_2, L_3 和 L_4 是有补格，L_1 不是有补格，图 11.8 中的 L_2 和 L_3 是有补格，L_1 不是有补格，因为 b, c, d, e 都不存在补元.

定义 11.10 如果一个格是有补分配格，则称它为布尔格或布尔代数.

根据定理 11.6，在分配格中，如果一个元素存在补元，则是惟一的. 因此，在布尔代数中，每个元素都存在着惟一的补元，可以把求补元的运算看做是布尔代数中的一元运算. 从而可以把一个布尔代数标记为 $<B, \wedge, \vee, ', 0, 1>$，其中 $\wedge, \vee, 0, 1$ 和有界格一样，$'$ 为求补运算，$\forall a \in B$，a' 是 a 的补元.

答案：不是分配格, 因为含有 5 元子格与五角格同构. 是有补格, 每个元素都有补元. 不是布尔格, 因为不是分配格.

定义 11.4 设 $<L, \wedge, \vee>$ 是格，S 是 L 的非空子集，若 S 关于 L 中的运算 $\wedge$ 和 $\vee$ 仍构成格，则称 S 是 L 的子格.

Problem 9

设 $(L, \leq)$ 为一有界分配格，L_1 是 L 中所具有补元的元素组成的集合，试证明：$(L_1, \leq_1)$ 是 $(L, \leq)$ 的子格

答案：设 $(L, \leq)$ 诱导的代数格为 $(L, \vee, \wedge)$, 由于 0,1 互为补元，所以 $0, 1 \in L_1$，故 L_1 非空. 对于任意的 $a, b \in L_1$，存在 $a', b' \in L$，使 a', b' 分别为 a, b 的补元.

注意到 $(L, \leq)$ 为有界分配格，有

$(a \vee b) \wedge (a' \wedge b') = (a' \wedge b' \wedge a) \vee (a' \wedge b' \wedge b) = 0 \vee 0 = 0$

$(a \wedge b) \vee (a' \vee b') = (a' \vee b' \vee a) \wedge (a' \vee b' \vee b) = 1 \wedge 1 = 1$

同理可证：$(a \vee b) \vee (a' \wedge b') = 1$, $(a \wedge b) \wedge (a' \vee b') = 0$

因此 $a \vee b$ 和 $a \wedge b$ 均有补元, 从而 $a \vee b, a \wedge b \in L_1$, 证得 $(L_1, \leq_1)$ 是 $(L, \leq)$ 的子格

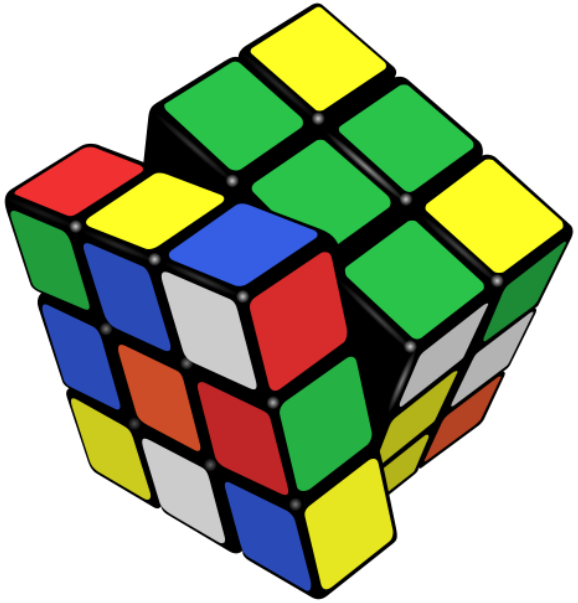
Problem 10

设格 $(L, \leq)$, 试证明对于任意的 a, b, c $\in L$, 有 $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ 成立等价于 $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$ 成立

证明：
假设对于任意的 a, b, c $\in L$, 有
$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$
则 $(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c)$
$= ((a \wedge a) \vee (b \wedge a)) \vee ((a \wedge c) \vee (b \wedge c))$
$= (a \vee (a \wedge b) \vee (a \wedge c)) \vee (b \wedge c)$
$= a \vee (b \wedge c)$

反之，类似可证.
$a \wedge (a \vee c) = (a \wedge (a \vee b)) \wedge (b \vee c)$
$= a \wedge (a \vee b) \wedge (b \vee c)$
$= a \wedge (b \vee (a \wedge c))$
$= (a \vee (a \wedge c) \wedge (b \vee (a \wedge c)$
$= (a \wedge b) \vee (a \wedge c)$

- 偏序集与格
- ***期中考试试题***



一、（本题满分12分）

自定义谓词，用**谓词逻辑**语句表示下列各前提和结论的陈述，并证明结论成立.

前提：

1) 2024年春，所有大一计算机系的同学均参加了春游：玄武湖骑行。
2) 所有参加玄武湖骑行的同学要么自备了骑行车辆，要么租用了园区骑行车辆。
3) 所有租用园区骑行车辆的同学均需要交纳租用押金或者签署租用协议书。
4) 王小花同学是大一计算机系同学，并且王小花同学没有自备骑行车辆。
5) 王小花同学没有交纳租用押金。

结论：

王小花同学签署了租用协议书。

【参考解答与评分标准】

（定义各谓词：4分）$A(x)$：x为大一计算机系同学；$B(x)$：x参加玄武湖骑行；$C(x)$：x自备骑行车辆；$D(x)$：x租用园区骑行车辆；$E(x)$：x交纳了租用押金；$F(x)$：x签署了租用协议书；选择个体k：王小花

各语句翻译如下：（翻译：4分）

前提：1）$\forall x(A(x) \to B(x))$；2）$\forall x(B(x) \to C(x) \vee D(x))$；3）$\forall x(D(x) \to E(x) \vee F(x))$；4）$A(k) \wedge \neg C(k)$；5）$\neg E(k)$；结论：$F(k)$

推理过程如下（推理过程：4分，可以不写后面的说明）

① $A(k) \to B(k)$	全称例示 from 1)
② $B(k) \to C(k) \vee D(k)$	全称例示 from 2)
③ $A(k) \to C(k) \vee D(k)$	假言三段论 from ①、②
④ $A(k)$	化简 from 4）
⑤ $C(k) \vee D(k)$	假言推理 from ③、④
⑥ $\neg C(k)$	化简 from 4）
⑦ $D(k)$	取拒式 from ⑤、⑥
⑧ $D(k) \to E(k) \vee F(k)$	全称例示 from 3）
⑨ $E(k) \vee F(k)$	假言推理 from ⑦、⑧
⑩ $\neg E(k)$	Premise 5)
⑪ $F(k)$	取拒式 from ⑨、⑩

仅用命题逻辑证明本题最多给4分。

二、（本题满分10分）

请将下列命题翻译成谓词逻辑语句，并证明命题成立：

对于任意大于2的正整数n，均存在连续的n个正整数，它们均为合数。

【参考解答与评分标准】

表达：谓词$C(x)$表示x是合数，可翻译为：$\forall n(n > 2 \wedge n \in \mathbb{Z}^{+}) \rightarrow \left(\exists k \forall i(i > 0 \wedge i \leq k) \rightarrow i + k \in \mathbb{Z}^{+} \wedge C(i+k)\right)$其它相似的表达也可以，比如：$\forall n\left((n \in \mathbb{N} \wedge n > 2) \rightarrow \exists k\left((k \in \mathbb{N} \wedge k > 1) \wedge \forall i\left((i \in \mathbb{N} \wedge i < n) \rightarrow C(i+k)\right)\right)\right)$（6分）

2）构造性证明，$(n+1)!+2$，$(n+1)!+3$，…，$(n+1)!+(n+1)$，该序列满足要求，每个都是合数。（4分）

三、（本题满分12分）

令 ϕ 为 2 次整系数多项式函数的集合，即 $\phi = \{f: \mathbb{R} \to \mathbb{R} \mid f(x) = ax^2 + bx + c,\ a, b, c \in \mathbb{Z}, a \neq 0\}$.

(1) 试分析ϕ是否为可数集合；

(2) 试分析$\{x \in \mathbb{R} \mid \exists f \in \phi, f(x) = 0\}$是否为可数集合；

(3) 对于任意给定的$f \in \phi$，令$S_f = \{x \in \mathbb{R} \mid x = f(x)\}$，$T_f = \{x \in \mathbb{R} \mid x = f(f(x))\}$，试证明：$S_f \subseteq T_f$.

【参考解答与评分标准】

1. 函数集合Φ属于可数集合；具体证明参考可数集合笛卡尔积示例；（4分）
2. 解集属于可数集合；具体证明参考可数集合笛卡尔积示例；（4分）
3. 有定义可得，$\forall x_0 \in S_f \leftrightarrow x_0 = f(x_0)$；两边运用函数的复合运算，可得 $f(x_0) = f(f(x_0)) = x_0$；所以可得$\forall x_0 \in S_f \to x_0 \in T_f$，所以可得$S_f \subseteq T_f$（4分）

四、（本题满分10分）

令$\mathbb{Z}^+$为正整数集,令$A=\mathbb{Z}^+\times\mathbb{Z}^+$，定义$A$上的二元关系$R$如下：

$$\big((a,b),(c,d)\big)\in R \Leftrightarrow \frac{a}{b}=\frac{c}{d}\ ,$$

证明：R为等价关系，并给出商集A/R.

【参考解答与评分标准】

1. 等价关系证明略，只需要证明自反、对称、传递即可。（6分）
2. 商集答案略（4分）

五、（本题满分10分）

某厂流水线采用基于AI大模型的检测系统实现自动化缺陷样品检测. 已知该厂样品的缺陷率为0.1%. 在自动化检测过程中，如果某样品有缺陷，则该样品被成功检测为缺陷样品的概率为99%；如果样品无缺陷，则该样品被检测为无缺陷样品（正常样品）的概率为95%. 现在某个样品被AI系统检测为缺陷样品，请问该样品确实为缺陷样品的概率是多少？

【参考解答与评分标准】

定义事件A: 表示被检测样品有缺陷，B: 表示被检测样品被检测为缺陷样品；要求的是条件概率$p(A|B)$

$$p(A|B)=\frac{p(AB)}{p(B)}=\frac{p(B|A)p(A)}{p(B)}=\frac{0.1\%\times 99\%}{0.1\%\times 99\%+5\%\times 99.9\%}=\frac{11}{566}\approx 0.0194$$

（给出事件定义即可给4分，过程6分）

六、（本题满分10分）

若p为素数，q为合数，且p与q互素（最大公约数为1），请判断$\sqrt{pq}$是有理数还是无理数，并给出结论的证明。

【参考解答与评分标准】

说明：本题解法较多，给出结论和运用反证法均可得分，证明过程为6分。

结论：$\sqrt{pq}$为无理数（2分）

假设$\sqrt{pq}$为有理数，则$\sqrt{pq}=\frac{m}{n}$，且$(m,n)=1$。（2分）

解法一：由$m^2=n^2pq$，可得$p|m^2$；

由于p为质数，所以$p|m$；

$$p|m \to p^2|m^2 \to p^2|n^2pq \to p|n^2q$$

由于p,q互素，所以$p|n^2$。

$$p|n^2 \to p|n$$

所以$(m,n)=p$，与$(m,n)=1$矛盾。（6分）

解法二：由$m^2=n^2pq$，可得$n^2|m^2 \to n|m$；

由于$(m,n)=1$，所以$n=1 \to pq=m^2 \to p|m^2$；

由于p为质数，所以$p|m$；

$$p|m \to p^2|m^2 \to p^2|pq \to p|q$$

与p,q互素矛盾。（6分）

解法三：

由$m^2=n^2pq$，可得$n^2|m^2 \to n|m$；

由于$(m,n)=1$，所以$n=1 \to pq=m^2$；

将m^2写作质数乘积的形式：

$$m^2=a_1^{m_1}a_2^{m_2}a_3^{m_3}\ldots$$

注意其指数均为偶数。

将q写作质数乘积的形式：

$$q=a_1^{q_1}a_2^{q_2}a_3^{q_3}\ldots$$

由于p,q互素，所以q不存在于p的分解中，即

$$pq=pa_1^{q_1}a_2^{q_2}a_3^{q_3}\ldots$$

p所对应的指数为奇数，与m^2的指数均为偶数矛盾。（6分）

七、（本题满分12分）

给定两个正整数n,k满足$k\le n$。给定一个n元有限集合A，令$P(A)$表示A的幂集.

(1) 令B为A的一个大小为k的子集（$0\le k\le n$），证明$P(A)$恰好有$2^{2^{n-k}}-1$个非空子集S满足$B\subseteq\bigcap_{D\in S}D$；

(2) 证明$P(A)$恰好有$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(2^{2^{n-i}}-1)$ 个非空子集S满足$\bigcap_{D\in S}D=\emptyset$.

【参考解答与评分标准】

1） 若$B\subseteq\bigcap_{D\in S}D$，则任何集合$D\in S$均满足$B\subseteq D$ （1分）

因此每个S的构造可以看成先选$P(A-B)$的一个非空子集S'，然后令每个集合$D'\in S'$都并上B。（3分）

由于S'不能为空集，我们可以计算得到满足要求的S有$2^{|P(A-B)|}-1=2^{2^{n-k}}-1$个。（2分）

(2) 证明$P(A)$恰好有$\sum_{i=0}^{n}(-1)^i\binom{n}{i}(2^{2^{n-i}}-1)$个非空子集$S$满足$\bigcap_{D\in S}D=\emptyset$.

2） 对A的任意元素a，构造集合T_a为$P(A)$的所有满足$\{a\}\subseteq\bigcap_{D\in S}D$的非空子集$S$。我们需要计算$2^{2^n}-1-|\bigcup_a T_a|$。（2分）

根 据 容 斥 原 理 ， $|\bigcup_a T_a|=L_1-L_2+\cdots+(-1)^{n-1}L_n$ 。 其 中 $L_k=\sum_{1\le i_1<i_2<\cdots<i_k\le n}|T_{i_1}\cap\cdots\cap T_{i_k}|$。（2分）

由于$T_{i_1}\cap\cdots\cap T_{i_k}$为$P(A)$的所有满足$\{i_1,\dots,i_k\}\subseteq\bigcap_{D\in S}D$的非空子集$S$，根据第一问，我们有$\left|T_{i_1}\cap\cdots\cap T_{i_k}\right|=2^{2^{n-k}}-1$。代入得证。（2分）

八、（本题满分12分）

假设有30个小球，小球的颜色一共有14种（每个小球只有一种颜色）．将这些小球平均放入6个箱子里，每个箱子刚好放入5个小球。令$A_1, A_2, A_3, A_4, A_5, A_6$分别为6个箱子里面小球的颜色的集合。证明以下两个条件不可能同时满足：

(1) 任意箱子内部的小球颜色两两不同，即 $|A_i| = 5\ (i = 1,2,\cdots,6)$；

(2) 对任意两个不同的箱子，最多只有一种相同颜色的小球被同时放置到这两个箱子里，即

$$\left|A_i \cap A_j\right| \le 1\ \ (1 \le i < j \le 6)。$$

【参考解答与评分标准】

根据反证法假设存在一种小球放置方案使得两个条件(1)(2)均满足（1分）

根据鸽笼原理，必然存在一种颜色有至少3个小球a_1, a_2, a_3，不妨假设它们的颜色为红色（3分，证明中提及鸽笼原理即得3分）

根据条件(1)，这3个小球a_1, a_2, a_3必然被放置到3个不同的箱子，不妨假设这3个箱子编号为1,2,3。（2分）

根据条件(1)(2)，这3个箱子内部剩余的12个小球颜色必然两两不同，并且不为红色。因此，$|A_1 \cup A_2 \cup A_3| = 13$。（2分）

考虑4号箱子，根据条件(2)，$|A_4 \cap (A_1 \cup A_2 \cup A_3)| = |(A_4 \cap A_1) \cup (A_4 \cap A_2) \cup (A_4 \cap A_3)| \leq |(A_4 \cap A_1)| + |(A_4 \cap A_2)| + |(A_4 \cap A_3)| \leq 3$。因此，4号箱子最多用了前三号箱子的三种颜色。（2分）

结合条件(1)，4号箱子至少出现了2种颜色的小球，并且这2种颜色和前三号箱子的13种颜色均不相同。因此，小球颜色一共有至少15种，矛盾。（2分）

九、（本题满分12分）

已知k为大于等于2的正整数，并且给定集合$A_1, A_2, A_3, \dots, A_k$.

(1) 若$A_1, A_2, A_3, \dots, A_k$均为有限集合，试给出使

$$P\left(\bigcup_{i=1}^{k} A_i\right) \approx P(A_1) \times P(A_2) \times \cdots \times P(A_k)$$

成立的充分必要条件，并证明结论；

（注：$P(A)$表示集合A的幂集，$A \approx B$表示集合A与B等势.）

(2) 若$A_1, A_2, A_3, \dots, A_k$均为可数集合，且其中至少存在一个无限集合，请证明：

$$P\left(\bigcup_{i=1}^{k} A_i\right) \approx P(A_1) \times P(A_2) \times \cdots \times P(A_k).$$

【参考解答与评分标准】

1. 充分必要条件为：$\forall i, j, i \neq j, A_i \cap A_j = \emptyset$；给出充分必要条件（2分），证明可使用数学归纳法（4分）；
2. 不妨假设A_1为无限可数集合。

由条件得$\bigcup_{i=1}^{k} A_i$为可数集合。由于k是有限的正整数，$\bigcup_{i=1}^{k} A_i$为无限可数集合，与自然数集等势（2分）

因此，$P(A_1)$与$P(\bigcup_{i=1}^{k} A_i)$均与实数集等势。$P(A_2), \dots, P(A_k)$的基数小于等于实数集的基数（3分）

由于k是有限的正整数，$P(A_1) \times P(A_2) \times \cdots \times P(A_k)$也与实数集等势，命题得证（1分）

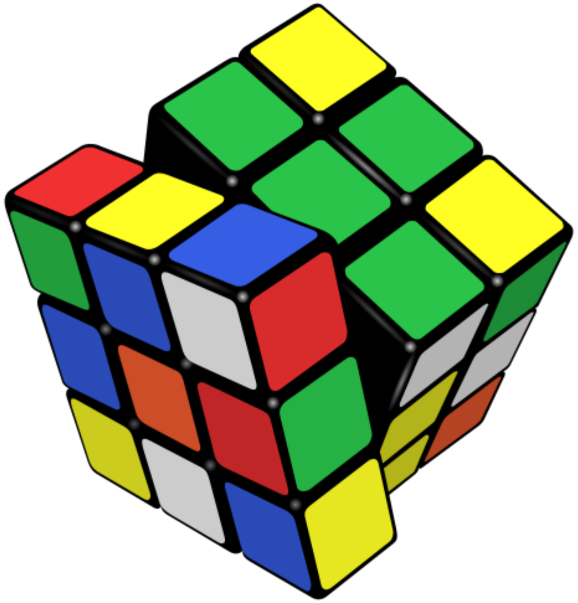
第十一周习题课

离散数学

南京大学计算机科学与技术系

内容提要

- 代数系统引论
- 群论导引



Problem 1

设 S 为 n 元集, 问

(1) 集合 S 上可以定义多少个不同的二元运算?

(2) 其中有多少个二元运算是可交换的?

(3) 其中有多少个二元运算是幂等的?

(4) 其中有多少个二元运算是既不可交换又不幂等的?

(1) n^{n^2} 个;

(2) $n^{\frac{n(n+1)}{2}}$ 个;

(3) n^{n^2-n} 个;

(4) $n^{n^2} - n^{\frac{n(n+1)}{2}} - n^{n^2-n} + n^{\frac{n(n-1)}{2}}$ 个.

Problem 2

设A = {0, 1}, S = A^A,

(1) 试列出S中的所有元素;

(2) 给出S上函数复合运算的运算表, 并指出单位元、零元和每一个可逆元素的逆元.

(1) $f_1 = \{\langle 0,0\rangle, \langle 1,0\rangle\}$

$f_2 = \{\langle 0,0\rangle, \langle 1,1\rangle\}$

$f_3 = \{\langle 0,1\rangle, \langle 1,0\rangle\}$

$f_4 = \{\langle 0,1\rangle, \langle 1,1\rangle\}$

(2)

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_1	f_4	f_4
f_2	f_1	f_2	f_3	f_4
f_3	f_1	f_3	f_2	f_4
f_4	f_1	f_4	f_1	f_4

单位元为 f_2, 没有零元 (但有右零元), f_2 和 f_3 有逆元, 都是自己.

Problem 3

设 A = {a, b, c}, a, b, c $\in$ R, 能否确定 a, b, c 的值使得

(1) A 对普通加法封闭?

(2) A 对普通乘法封闭?

(1) 不能. 假设存在满足题意的集合 A, 那么 A 中必然存在绝对值最大的非零元素, 不妨假设是 a, 那么 $|a + a| = 2|a| > |a|$ 比 A 中绝对值最大的元素还大, 因此不属于 A, 矛盾. 故不存在满足题意的集合.

(2) 能, A = {-1, 0, 1}.

Problem 4

判断下列集合对所给的二元运算是否封闭，并说明理由.

(1) 非零整数集合 Z^* 和普通的除法运算.

(2) 全体 $n \times n$ 实可逆矩阵集合关于矩阵加法和乘法运算，其中 $n \geqslant 2$.

(3) 正实数集合 R^+和 $\circ$ 运算，其中 $\circ$ 运算定义为：

$$\forall a, b \in R^+, \ a \circ b = ab - a - b$$

(4) $S = \{x \mid x = \ln n, n \in Z^+\}$ 关于普通的加法和乘法运算.

(1) 不封闭.
(2) 加法不封闭，乘法封闭.
(3) 不封闭.
(4) 加法封闭，乘法不封闭.

Problem 5

R 为实数集，定义以下4 个函数f_1，f_2，f_3，f_4. ∀x，y ∈ R 有
$f_1((x, y)) = x \cdot y$，$f_2((x, y)) = x - y$，
$f_3((x, y)) = \max(x, y)$，$f_4((x, y)) = |x - y|$.
(1) 判断上述二元运算是否为可交换，可结合，幂等的.
(2) 求上述二元运算的单位元，零元以及每一个可逆元素的逆元.
(3) 设A = {a, b}，试给出A 上一个不可交换，也不可结合的二元运算.

(1)

	可交换	可结合	幂等
f_1	√	√	×
f_2	×	×	×
f_3	√	√	√
f_4	√	×	×

(2)

	单位元	零元	逆元
f_1	1	0	$1/x(x \neq 0)$
f_2	×	×	×
f_3	×	×	×
f_4	×	×	×

(3)

$\circ$	a	b
a	b	b
b	a	a

Problem 6

设$S = \{1, 2, ..., 10\}$，问下面定义的运算能否与S 构成代数系统$\langle S, *\rangle$? 如果能，则说明$*$ 运算是否满足交换律、结合律，并给出单位元和零元.

(1) $x * y = \gcd(x, y)$，$\gcd(x, y)$ 是x 与y 的最大公约数.

(2) $x * y = \mathrm{lcm}(x, y)$，$\mathrm{lcm}(x, y)$ 是x 与y 的最小公倍数.

(3) $x * y = \max(x, y)$.

(4) $x * y =$ 质数p 的个数，其中$x \leqslant p \leqslant y$.

	代数系统	交换律	结合律	单位元	零元
(1)	√	√	√	×	1
(2)	×				
(3)	√	√	√	1	10
(4)	×				

Problem 7

判断集合 $A = \{x \mid x \in N \land x$ 与 5 互素 $\}$ 能否构成代数系统 $V = \langle N, +\rangle$ 的子代数，并说明理由.

不能. $2 + 3 = 5$.

Problem 8

设集合 $A = \{a, b, c, d\}$ 上的一个二元运算 $\circ$ 如下表所示：

∘	a	b	c	d
a	a	b	c	d
b	b	a	d	d
c	c	d	a	d
d	d	d	d	d

(1) 说明运算是否可结合？为什么？

(2) 求单位元与零元.

(1) 因为 $(b \circ b) \circ c = a \circ c = c, b \circ (b \circ c) = b \circ d = d$，不满足结合律.

(2) 单位元 a，零元 d.

Problem 9

设集合A = {a, b, c}，∘ 是 A 上的二元运算，在 V = ⟨A, ∘⟩ 的运算表中，除了a ∘ b = a 以外，其余运算结果都等于b.

试给出V = ⟨A, ∘⟩ 的两个非恒等映射的自同态.

（自同态：如果映射 f 是 V 到 V 的，则称 f 为自同态.）

设 f 为同态，于是由 $f(b)f(b)=f(bb)=f(b)$，知道 $f(b)$ 是幂等元. 而该运算表中只有 b 是幂等元，于是得到 $f(b)=b$. 假设 $f(c)=a$，那么就有

$$b=f(b)=f(cb)=f(c)f(b)=ab=a$$

矛盾，于是 $f(c)\neq a$. 假设 $f(a)=c$，那么就有

$$c=f(a)=f(ab)=f(a)f(b)=cb=b$$

也产生矛盾. 综合上述结果知道同态映射 f 满足 $f(b)=b, f(c)\neq a, f(a)\neq c$. 因此，可能的赋值是：

$$f(a)=a,b;\quad f(b)=b;\quad f(c)=b,c$$

从而得到 4 个函数：

$$f_1=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,b\rangle\},\qquad f_2=\{\langle a,a\rangle,\langle b,b\rangle,\langle c,c\rangle\}$$
$$f_3=\{\langle a,b\rangle,\langle b,b\rangle,\langle c,b\rangle\},\qquad f_4=\{\langle a,b\rangle,\langle b,b\rangle,\langle c,c\rangle\}$$

但是，由于

$$f_1(ac)=f_1(b)=b,\quad f_1(a)f_1(c)=ab=a$$

并且 f_2 是恒等映射，于是只有 f_3 和 f_4 满足要求.

Problem 10

判断下列集合关于指定的运算是否构成半群, 独异点和群:

(1) a 是正实数, $G = \{a^n | n \in \mathbb{Z}\}$, 运算是普通乘法.

(2) $\mathbb{Q}^+$ 为正有理数, 运算是普通乘法.

(3) $\mathbb{Q}^+$ 为正有理数, 运算是普通加法.

(4) 一元实系数多项式的集合关于多项式的加法.

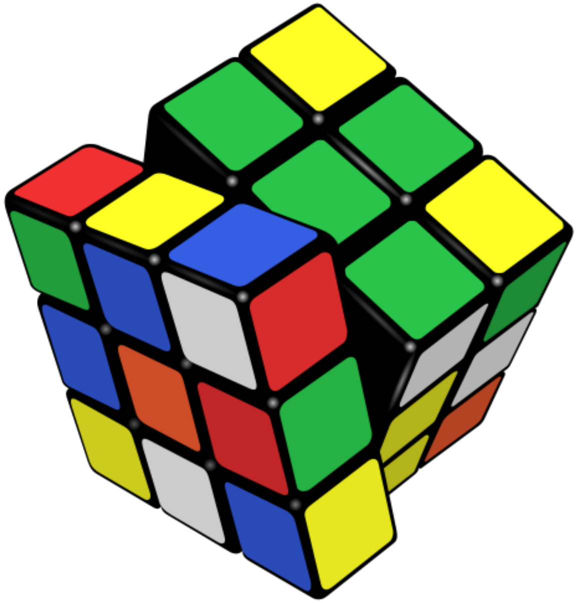
(5) 一元实系数多项式的集合关于多项式的乘法.

(6) $U_n = \{x | x \in \mathbb{C} \land x^n = 1\}$, n 为某个给定正整数, $\mathbb{C}$ 为复数集合, 运算是复数乘法.

	半群	独异点	群
(1)	√	√	√
(2)	√	√	√
(3)	√	×	×
(4)	√	√	√
(5)	√	√	×
(6)	√	√	√

注: (4) (5) 两小题中, 形如 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 只有 x 一个变元, 系数均为实数的多项式, 叫做一元实系数多项式.

- 偏序集与格
- *群论导引*



Problem 11

$S = \{a, b, c\}$，$*$ 是S 上的二元运算，且$\forall x, y \in S$，$x * y = x$.

（1）证明S 关于$*$ 运算构成半群.

（2）试判断S 成为独异点的条件.

（1）运算显然是封闭的．因为$\forall x, y, z \in S$，$(x * y) * z = x * y = x$ 且 $x * (y * z) = x * y = x$．所以结合律成立．综上，S关于$*$运算构成半群.

（2）若存在$e \in S$，使得 e 为 S 中的单位元，必有 $a * e = e * a = a$，而$\forall x, y \in S$，$x * y = x$，那么$e * a = e$，于是得到 $e = a$．因此如果存在单位元，这个单位元必然与每个元素相同．因此 S 成为独异点当且仅当$a = b = c$.

Problem 12

证明：有单位元且满足消去律的有限半群一定是群。

答案: 设 G 是一个有单位元且适合消去律的有限半群，要整 G 是群，只需证明 $\forall a \in G$，a 可逆。考虑 $a, a^2, \cdots, a^k, \cdots$，因为只有有有限个元素，故存在 $k > l$ 使得 $a^l = a^k$。令 $m = k - l$，有 $a^l e = a^l a^m$，其中 e 是单位元。利用消去律得到 $a^m = e$。于是 $m = 1$ 时 $a = e$ 可逆；$m > 1$ 时 $aa^{m-1} = a^{m-1}a = e$，即 a 有逆元 a^{m-1}。总之，a 是可逆的。因此 G 一定是群。

Problem 13

设 G 是一个群，并且 |G| 为偶数，证明 G 中必定存在一个元素 g 满足 $g \neq e$ 且 $g = g^{-1}$

答案： 归谬法，假定不存在这样的 g. 则每个非单位元元素都与其逆不同. 由条件知 G 有限，则可以使用选择公理和群论公理，每次从中取出一个非单位元元素和它的逆，最终会只剩单位元（因为逆元唯一，不会剩余一个单位元和一个非单位元）. 那么 G 中有奇数个元素，与条件矛盾.

Problem 14

证明：设 a 是群 ⟨G, ∘⟩ 的幂等元，则 a 一定是单位元.

答案： 由条件有 $a \circ a = a$, 因为 G 是群, 任何一个元素都有逆元. 等式两边同乘 a 的逆元, 有

$$a^{-1} \circ (a \circ a) = a^{-1} \circ a.$$

由于运算可结合, 得到

$$a = e \circ a = (a^{-1} \circ a) \circ a = a^{-1} \circ (a \circ a) = a^{-1} \circ a = e.$$

即 a 一定是单位元.

Problem 15

(结合律) 假定集合 S 上定义的二元操作 $\circ$ 满足结合律. 我们知道二元操作只定义在两个元素上, 当参与运算的元素超过两个时, 会有很多种不同的顺序, 比如, 假定 $a, b, c, d \in S$, 那么可能会有的情况有

$$(a \circ b) \circ (c \circ d), (a \circ (b \circ c)) \circ d, a \circ ((b \circ c) \circ d)$$

等等, 注意到**每一步只进行一次运算**. 证明: 无论我们怎么放置括号, 这种嵌套运算的最终结果是不变的. 即证明对 $s_1 s_2 ... s_n \in S$, 任意括号嵌套顺序下的结果都等同于 $((...((s_1 \circ s_2) \circ s_3)...) \circ s_n)$.

(提示: 使用数学归纳法, 基础情况是 $n = 2$, 手动尝试一下从 $n = 4$ 到 $n = 5$ 的情况).

答案: 对 n 进行归纳, $n = 2$ 时, 只有一种情况, 得证.

归纳假设在 $n = k$ 时, 结论成立. 尝试证明 $n = k + 1$ 的情况.

由于每一步只进行一次运算, 考虑最先进行的运算, 设为 $(s_i \circ s_{i+1})$, 其中 $1 \leq i \leq k$. 设 $(s_i \circ s_{i+1}) = s_j \in S$.

应用归纳假设,

$$\begin{aligned}
\text{原式} &= (...((...((s_1 \circ s_2) \circ s_3)... \circ s_j) \circ s_{i+2})...s_{k+1}) \\
&= (...((...((s_1 \circ s_2) \circ s_3)... \circ (s_i \circ s_{i+1})) \circ s_{i+2})...s_{k+1}) \\
&= (...((...((s_1 \circ s_2) \circ s_3)... \circ s_i) \circ s_{i+1})...s_{k+1})
\end{aligned}$$

得证

Problem 16

设 G 为群，a, b ∈ G 且是有限阶元。记 $|a| = r$，证明：

(1) $a^k = e$ $(k \in Z)$ 当且仅当 $r|k$

(2) $|b^{-1}ab| = |a|$

(3) $|ab| = |ba|$

(1) 充分性：

由于 $r|k$，必存在整数 m 使得 $k = mr$，所以有 $a^k = a^{mr} = (a^r)^m = e^m = e$。

必要性：

根据带余除法，$\exists m, i \in \mathbb{Z}$ 使得 $k = mr + i$，$0 \leq i \leq r-1$，从而有 $e = a^k = a^{mr+i} = (a^r)^m a^i = ea^i = a^i$。

而 $|a| = r > i \geq 0$，因此必有 $i = 0$，即可得 $r|k$。

(2) $|b^{-1}ab| = |a|$
(3) $|ab| = |ba|$

(2) 记 $|b^{-1}ab| = t$，则一方面，

$$(b^{-1}ab)^r = \underbrace{(b^{-1}ab)(b^{-1}ab)\cdots(b^{-1}ab)}_{r个}$$

$$= b^{-1}a^r b == b^{-1}eb = e$$

由 (1) 得 $t|r$。

另一方面，

$$a = b(b^{-1}ab)b^{-1} = (b^{-1})^{-1}(b^{-1}ab)b^{-1}$$

即 $(b^{-1})^{-1}(b^{-1}ab)b^{-1}$ 的阶是 $b^{-1}ab$ 的阶的因子，即 $r|t$ ，从而 $|b^{-1}ab| = |a|$

(3) 记 $|b^{-1}ab| = t$，则

$$(ab)^{t+1} = \underbrace{(ab)(ab)\cdots(ab)}_{t+1个} = a\,\underbrace{(ba(ba)\cdots(ba))}_{t个}\,b$$

$$= a(ba)^t b = aeb = ab$$

由消去律得 $(ab)^t = e$，即 $r|t$。同理可证 $t|r$。因此 $|ab| = |ba|$。

Problem 17

(数论) 我们知道, 在整数集合 Z 上的同余关系是一个等价关系. 我们用记号 $[a]_n$ 表示 a 的模 n 同余类. 即

$$b \in [a]_n \Leftrightarrow a \equiv b \pmod{n}.$$

模 n 同余类构成的集合是一个重要的概念, 有许多记法, 例如 $\mathbb{Z}_n, \mathbb{Z}/n\mathbb{Z}$ 等. 例如 $\mathbb{Z}/2\mathbb{Z} = \{[0]_2, [1]_2\}$. 对于正整数 n, 我们记扩展的加法为

$$[a]_n + [b]_n := [a+b]_n.$$

易证 $\mathbb{Z}_n$ 在扩展加法下构成一个群. 类似地, 扩展乘法为

$$[a]_n \times [b]_n := [a \times b]_n.$$

现在令 $\mathbb{Z}_n^* := \{[m]_n \in \mathbb{Z}_n | \gcd(m,n) = 1\}$. 证明: $\mathbb{Z}_n^*$ 在扩展乘法下构成一个群.

答案: 首先, 我们有 $m \equiv m' \pmod{n} \wedge l \equiv l' \pmod{n} \Rightarrow ml \equiv m'l' \pmod{n}$, 故扩展乘法为良定义的操作. 对任意 $[m]_n, [l]_n \in \mathbb{Z}_n^*$, 我们有 $\gcd(m,n) = 1, \gcd(l,n) = 1$, 所以 $\gcd(lm,n) = 1$. 因此扩展乘法在 $\mathbb{Z}_n^*$ 上封闭. 由乘法结合性可以直接得到扩展乘法的结合性. 单位元为 $[1]_n$ 对任意 $[m]_n \in \mathbb{Z}_n^*$, 由贝祖定理, 因为 $\gcd(m,n) = 1$, 故存在 k, r 使得 $km + rn = 1$, 即 $[k]_n \times [m]_n = [km]_n = [1]_n$, 存在逆元.

最大公约数（续）

- gcd(a, b)一定是a和b的线性组合，即：

  $$\exists s, t\in Z，\ gcd(a, b)=sa+tb$$

  //欧几里德算法得出结论
- 裴蜀定理 (Bézout's identity)

  $ax + by = c$有整数解当且仅当 $\gcd(a, b) \mid c$.
- 非零整数a和b是互素的 *iff* $\exists s, t\in Z.\ sa+tb=1$
  - 必要性显然。以下证明充分性。假设$\exists s, t\in Z.\ sa+tb=1$.
  - 假设gcd(a, b)=d， $\exists a_1, b_1\in Z.\ a=a_1d, b=b_1d$.
  - 我们有$sa_1d+tb_1d=1$. 即 $(sa_1+tb_1)d=1$.
  - 因此d=1. 即gcd(a, b)=1。

Problem 18

对没有单位元的半群 M，是否一定能在其中加入一个新元素 e 使得 M ∪ {e} 是含有单位元 e 的半群?

是。验证添加 e 之后的半群仍满足结合律即可。

Problem 19

设 M 是有单位元 e 的半群，a，b是 M 中的可逆元，试证 ab 也是 M 的可逆元。

$$(ab)(b^{-1}a^{-1}) = ((ab)b^{-1})a^{-1} = (a(bb^{-1}))a^{-1} = e$$

第十四周习题课

离散数学

南京大学计算机科学与技术系

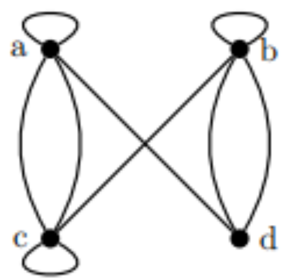
内容提要

- ***图的表示与图同构***
- 图的连通性

Problem 1

Problem 1

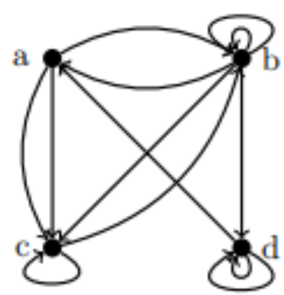
用邻接矩阵表示左侧的图；并画出右侧邻接矩阵表示的有向图。



$$\begin{bmatrix} 0 & 1 & 2 & 0 \\ 1 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 2 \end{bmatrix}$$

答案：

$$\begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 1 & 2 & 0 & 0 \end{bmatrix}$$



注意不对称的邻接矩阵对应有向图

Problem 2

Problem 2

具有 4 个顶点的非同构简单图中，有多少个

1) 包含 C_3?

2) 无孤立点?

3) 是二部图?

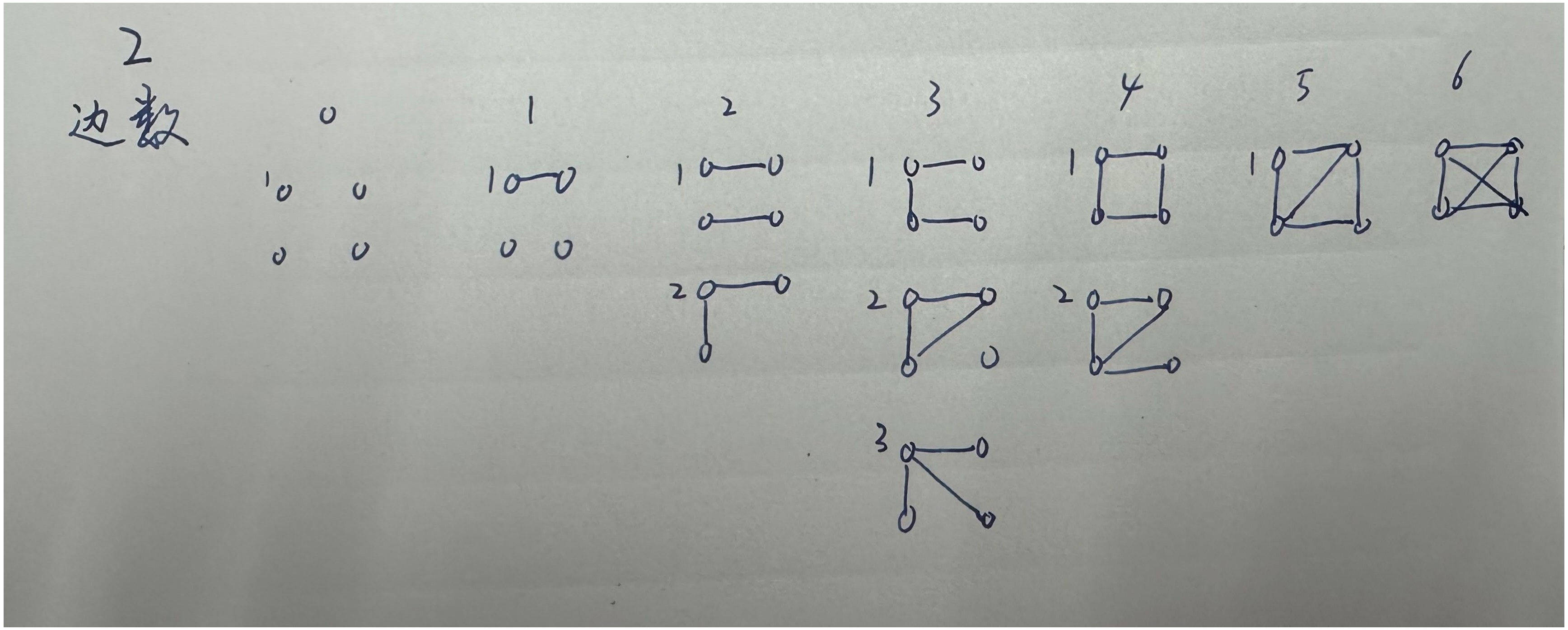
答案:

1) 4

2) 7

3) 7

Problem 2(cont.)



Problem 3

Problem 3

若简单图 G 和 H 是同构的，证明 $\bar{G}$ 和 $\bar{H}$ 也是同构的。

答案：

设存在一个同构映射 $f: V_G \to V_H$。因为 G 和 H 同构，因此 $\forall a, b \in V_G$, $a - b \in E_G$ 当且仅当 $f(a) - f(b) \in E_H$。因此 $a - b \notin E_G$ 当且仅当 $f(a) - f(b) \notin E_H$，即 $a - b \in E_{\bar{G}}$ 当且仅当 $f(a) - f(b) \in E_{\bar{H}}$，因此 f 也是 $\bar{G}$ 到 $\bar{H}$ 的同构映射，即 $\bar{G}$ 和 $\bar{H}$ 同构。

简单地说，补图中两个顶点有边，当且仅当原图中这两个顶点之间无边。利用G、H同构，给出其补图的同构映射即可。

Problem 4

Problem 4

若简单图 G 与 $\bar{G}$ 是同构的，则 G 称为**自补图**

试证明：若图 G 是自补图，则图 G 的顶点数 $\mathcal{V}$ 满足 $\mathcal{V} \equiv 0, 1\,(mod 4)$。

答案：

因为 G 是自补图，所以 G 和 $\bar{G}$ 的边数相等，$\mathcal{E}_G + \mathcal{E}_{\bar{G}} = \frac{\mathcal{V}(\mathcal{V}-1)}{2}$，则 $\mathcal{E}_G = \frac{\mathcal{V}(\mathcal{V}-1)}{4}$，

因为边数只能是整数，所以要么 $\mathcal{V} \equiv 0\,(mod 4)$ 要么 $(\mathcal{V}-1) \equiv 0\,(mod 4)$。

v=2(mod4) 或 v=3(mod4)时，边数不是整数

综上得证。

对边数的简单分析即可

Problem 5

Problem 5

具有 n 个顶点的非同构的简单图有多少个? 其中 n 是:

a) 2　　b) 3　　c) 4

答案:

a) 2

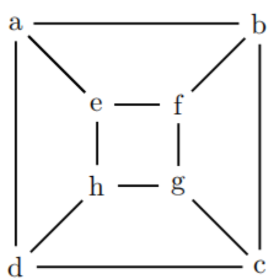
b) 4

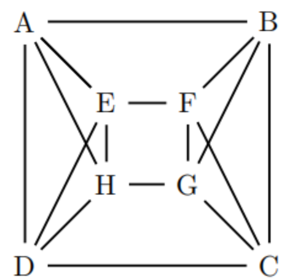
c) 11

Problem 6

Problem 6

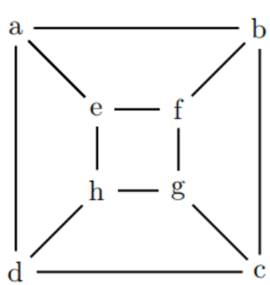
证明 [下左图] 和 [下右图的补图] 同构。



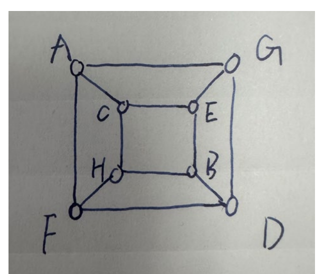


答案:

对应关系如图所示



画出右图的补图如下



Problem 7

Problem 7

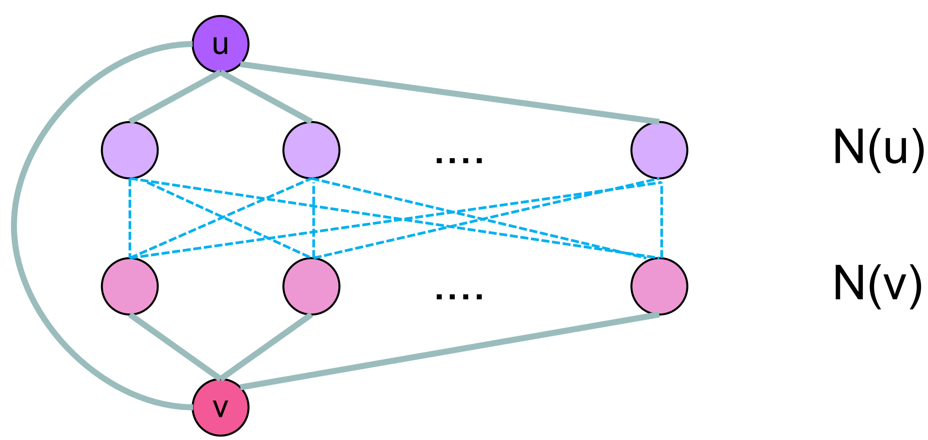
G 的围长是指 G 中最短回路的长；若 G 没有回路，则定义 G 的围长为无穷大。
证明：围长为 4 的 k 正则图至少有 $2k$ 个顶点，且恰有 $2k$ 个顶点的这样的图（在同构意义下）只有一个。

答案:

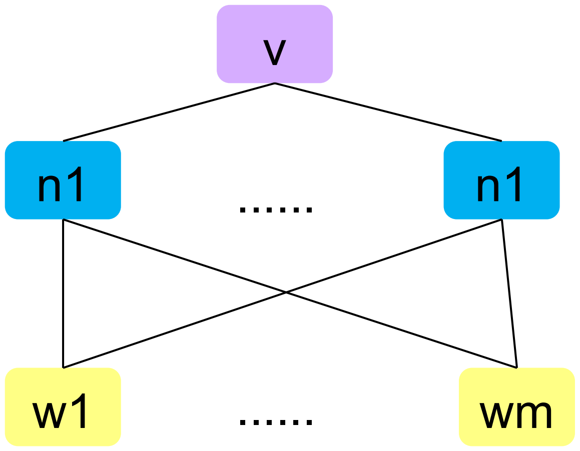
设 u, v 是 G 中相邻顶点，$N(u)$ 和 $N(v)$ 分别代表 u 和 v 的邻居构成的集合，则 $N(u)$ 和 $N(v)$ 不相交，否则 G 的围长为 3，产生矛盾。因此，G 至少有 $2(k-1)+2$ 个顶点。

因为是 k 正则图，每个顶点应该连接 k 个顶点，易知 $N(u)$ 和 $N(v)$ 内部不能相连，否则围长为 3, 因此将 $N(u)\setminus\{v\}$ 中的 k-1 个顶点分别和 $N(v)\setminus\{u\}$ 中的 k-1 个顶点相连，这样每个顶点的度数都为 k，即可得到 $2k$ 个顶点的围长为 4 的图，此时 G-u,v 是一个完全二部图，这样的图（在同构意义下）只有一个，加上 u,v 后在同构意义下依然唯一。

如无特意说明，以后各题只考虑有限个点的图。



Problem 7(cont.)



一些想到的其他证法
1、点数下界的其他证法：Mantel定理
不含K3的简单图，设顶点数v，有边数上界(v^2)/4

double counting: 边数 = kv/2 <= v^2/4
得到：v >= 2k

2、反证法:
设点数v < 2k
考虑某顶点u与其邻居n1, ..., nk,
以及除它们外v - (k+1) < k-1个顶点 w1, ..., wm
显然，ni(i = 1~k)之间不能相邻，且每个ni除与u相连之外，仍需要连k-1条边
这些边只能连到w1,...,wm
而w1,..., wm的数量小于k-1，矛盾

同时，若v = 2k，
那么有且仅有ni与wj之间两两相连能满足条件
实质上给出了同构意义下唯一的图的构造

Problem 8

Problem 8

证明：简单图 G 是二部图，当且仅当 G 没有包含奇数条边的简单回路。

答案： 证明：

必要性：设 G 是偶图，设两个不相交的非空顶点集合为 A 和 B。若 G 存在回路 c，设 c 的起点属于 A，则从 A 出发时通路在奇数步后停在 B，在偶数步后停在 A。所以回路 c 的长度必为偶数。

充分性：若所有的回路长度都为偶数，要证图 G 是偶图。假设 G 是连通图，若不连通，则每次仅考虑一个连通分支。设 v 是图的一个顶点，设 A 是有从 v 出发奇数长度通路的所有顶点的集合，设 B 是有从 v 出发偶数长度通路的所有顶点的集合。由于这个分支是连通的，所以每个顶点都属于 A 或 B。没有顶点同时属于 A 和 B，若假设存在一个顶点 v' 同时属于 A 和 B，则从 v 到 v' 的奇长度通路，加上 v' 到 v 的偶长度通路，就得到一个奇回路，与前提矛盾。因此，顶点集合划分成两个部分。要证每条边的端点都在不同的部分中，假设 (x, y) 是一条边，$x \in A$，则从 v 到 x 的奇长度通路加上 (x, y) 就产生从 v 到 y 的偶长度通路，所以 $y \in B$。同理可证 $x \in B$ 的情况。

综上所述可得 G 是二部图。

->：二部图的情况下，不可能存在奇回路（否则顶点归属的类发生矛盾）

<-：证明没有奇回路情况下，能够将图的顶点划分成A和B两部分

内容提要

- 图的表示与图同构
- ***图的连通性***

Problem 9

Problem 9

证明：$\kappa(G)=1$ 的 r-正则图 G，若 $r>1$，总满足 $\lambda(G)\leq\frac{r}{2}$。（$\lambda(G)$ 表示 G 的边连通度）

答案： 考虑 G 的割点 v，$G-v$ 至少有 2 个连通分量 C_1,C_2，其中至少一个与 v 相连的边数量不超过 $\frac{r}{2}$，这些边构成 G 的一个割边集，于是 $\lambda(G)\leq\frac{r}{2}$。

如果图存在割点、割边，一个自然的想法是去考虑图在该位置的局部性质

Problem 10

Problem 10

若无向图 G 中恰有两个奇数度的结点，则这两结点间必有一条路。

答案： 标准答案用词“迹”(Trace)指没有重复边的通路，也就是简单通路的同义词

证明：设图 G 的两个奇数度结点为 v_1 和 v_2，从 v_1 开始构建一条迹，即从 v_1 出发经过关联于 v_1 的边 e_1 到达结点 u_1，若 $deg(u_1)$ 为偶数，则必有不同于 e_1 的边 e_2 与 u_1 关联，经过 e_2 到达结点 u_2，如此继续下去，每次取一边，直到另一个奇数结点停止，因为 G 中只有两个奇度数的结点，故此结点只能是 v_1 和 v_2 中的一个，若该结点是 v_2，则得到 v_1 到 v_2 的一条迹；若该结点仍然是 v_1，则此路是闭迹，由于每条闭迹都关联偶数条边，而 $deg(v_1)$ 是奇数，所以至少有一条关联于 v_1 的边不在此闭迹上，继续从 v_1 出发，依次进行下去，这样有限次后必可到达结点 v_2，此即为一条从 v_1 到 v_2 的路。

另一种方法：目标是证明这两个奇度顶点在一个连通分支内

反证：如果这两个节点之间无路，那么它们不在一个连通分支内
那么可以将G分为多个连通分支，且两个奇度节点不在一个连通分支内，不妨设它们分别在G1和G2内
那么G1与G2都只有一个度数为奇数的顶点，此时G1（与G2）中顶点度数和为奇数，矛盾

Problem 11

Problem 11

给定一个顶点个数有限的简单图 G，假定我们只可以通过如下方式逐步删除 G 中的顶点：每一步可以删除度数小于 2 的顶点。试证明：如果 G 中的所有顶点能被删除当且仅当 G 中没有回路。

答案： 必要性：反设 G 中有回路，则显然 G 中此回路上的顶点不会被删除，得证。

充分性：由于 G 是由 1 个或多个连通分支并起来的图，我们考虑 G 中任意一个连通分支 G_1：取 G_1 中最长的一条通路 P，不妨按顺序命名 P 上顶点为 v_1，v_2，...，v_{n-1}，v_n，其中 v_1，v_n 为通路 P 的两端。下面证明 v_1，v_n 的顶点度数为 1。

已知 v_1，v_n 分别与 v_2，v_{n-1} 相连，以 v_1 为例，若 v_1 还与除了 v_2 之外的顶点 w 相连，分两种情况讨论：w 是 P 上的点，则 G 中存在回路，与题目条件矛盾；w 不是 P 上的点，那么 wv_1+P 形成了新的更长的通路，与我们自己假设的 P 是最长通路矛盾。所以不存在除了 v_2 之外的顶点 w 与 v_1 相连。因此 $D(v_1)=1$，$D(v_n)=1$。

那么按照题目中的步骤，我们每次选取 G_1 中的最长通路，显然最长的一条通路总是存在（若相等则任取一条），将两端的顶点（度数为 1）删除，这个操作只要 G_1 中还有顶点就可以永远进行下去直到 G_1 中所有点都被删除。扩展到整个图 G 上也同样适用。因此充分性得证。

也可用归纳法
基础：顶点个数为3的无回路图，所有顶点可被删除
归纳：n=k时成立
n=k+1时：考虑任意大小k的子图G’，先删G’外那一点或先删G’都可以

Problem 12

证明：G 是 2-边连通图当且仅当 G 中任意两个顶点之间至少有两条不含公共边的通路。
（提示：证明过程中可使用 Whitney 定理，但需注意和本题的差异）

答案：证明：

- 若 G 中任意两顶点都至少有两条边不重道路连接，显然对任意 $e \in E(G)$，$G-e$ 是连通的，故 G 为 2-边连通的。
- 若 G 是 2-边连通的，则 G 无割边。把 G 分解成块，块与块之间以 G 中的割点互相连接。设 u, v 是 G 中任意两顶点。分两种情况：
  - 若 u, v 同属于 G 的某一块，则由 Whitney 定理知，结论成立。
  - 若 u, v 属于 G 的不同块，设 $B_1, B_2, ..., B_n$ 是 G 的块，其中块 B_i 与块 B_{i+1} 以割点 V_i 相互连接且 $|v(B_i)| \geq 3$。不妨设 $u \in B_1$，$v \in B_n$。由之前的证明可知，在 B_1 中存在两条由 u 到 v_1 的不相交的路 P_{11}, P_{12}；同理在 B_i 中存在两条由 v_{i-1} 到 v_i 的不相交的路 P_{i1}, P_{i2}；在 B_n 中存在两条由 v_{n-1} 由 v 的不相交的路 P_{n1}, P_{n2}。于是我们找到两条 u 到 v 的边不相交的路：$P_{11} \cup P_{21} \cup ... \cup P_{n1}$ 和 $P_{12} \cup P_{22} \cup ... \cup P_{n2}$。

G分成若干块，在各块内用Whitney定理得到两段无公共边的路径，然后再把各段拼接起来

Problem 12(cont.)

仿照Whitney，写一个无公共边版的归纳证明也是可以的（考虑：无公共点包含无公共边）

Whitney定理的证明

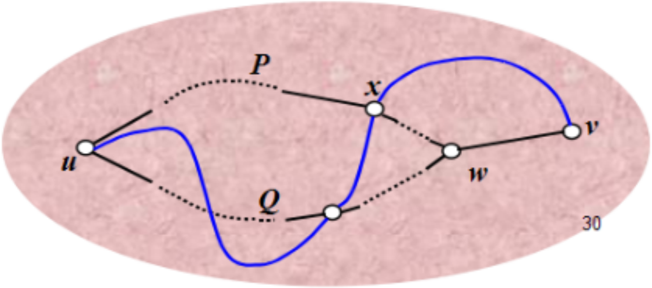
- ⇒ 设u,v是图G中的任意两点。下面对距离$d(u,v)$进行归纳证明。

  当$d(u,v)=1$, $uv\in E_G$, 因为G是2-连通图，G-uv仍连通，则G中除边uv外，必有另一条不含uv的路径。

  假设当$d(u,v)<k$时，至少存在两条中间点不相交的通路。

  若$d(u,v)=k$, 设u,v间的一条最短路径是$u\ldots wv$。则$d(u,w)<k$, 由归纳假设u,w之间存在两条中间点不相交的路径，设为P, Q。因为G是2-连通图，G-w中仍有(不含w的)uv-路径P'，且它与P, Q有公共点(u就是一个)。

  假设这样的公共点中距离v最近的是x(不妨假设它在P上)，则$Q+wv$边以及P上的ux-段+P'上的xv-段是u,v之间两条中间点不相交的通路。



- ⇐ 充分性显然

Problem 13

假设 P 是连通图 G 中的一条最长的初级通路（点不重复），且 P 不是回路。试证明 P 的端点不是图 G 的割点。

答案: 对于 P 的任意端点 u: 对任意不属于 P 的点 v，v 到 u 的任意通路 Q 中间一定有 P 上的其他点，否则取 Q 上包含 u 的边 e，P+e 是更长的初级通路，矛盾。即 v 一定能通过某个不含 u 的通路与 P 上的其他点连通。

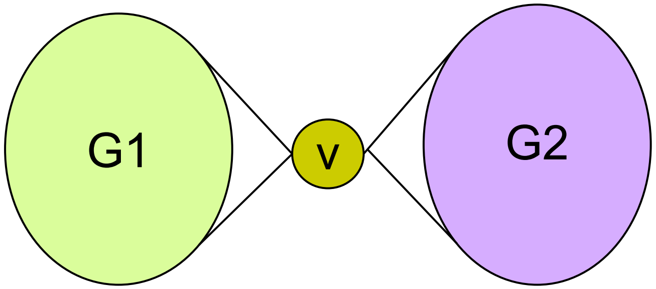
考虑 G−u 上任意的 v_1，v_2，分情况讨论:

v_1，v_2 都在 P 上，取 P 上 v_1，v_2 段，两者仍然是连通的;

v_1，v_2 只有一个在 P 上，不妨记为 v_1，开头已证 v_2 一定能通过某个不含 u 的通路与 P 上的 v_1 连通;

v_1，v_2 都不在 P 上，继续利用开头的论证，v_1，v_2 与 u 的通路中间移动有 P 上的其他点，记为 v_3，v_4，u 的删除不影响 v_3，v_4 仍然连通，因此 v_1，v_2 也连通。

于是 G−u 是连通图，P 的端点不是 G 的割点。



另一种方法：
反证：如果P端点是G割点，不妨设为v

图G被v分为两部分，且P中除v外顶点都在某一部分，不妨设为G1中，
但是，显然可以在G2内找一段路径接到P上去，使P变得更长
此时，与P是最长的路径矛盾

Problem 14

Problem 14

证明：设 G 是一个简单图，k 是一个自然数，若 $\delta(G) \geq \frac{v+k-2}{2}$，则 G 是 k-连通的。

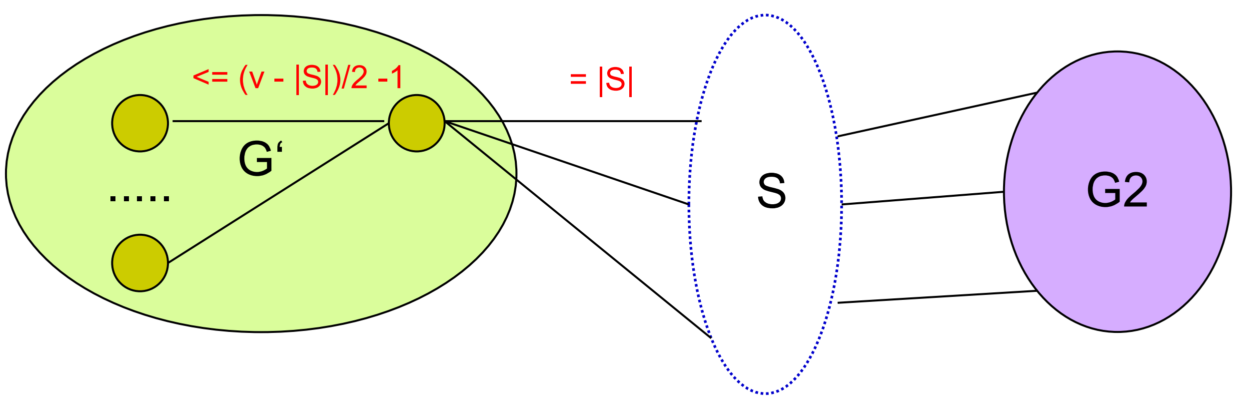
答案:

证明：用反证法. 假如 G 不是 k-连通的, 则 G 的连通 $\kappa < k$, 即存在 G 的点割集 S, 使得 |S|<k, 且 G-S 不连通。

因 G-S 有 v-|S| 个顶点, 且至少有两个连通分支, 故必有 G-S 的某个连通分支 G' 含有不超过 $\frac{v-|S|}{2}$ 个顶点。

注意到 G' 中任一个顶点只可能与 G' 内的点及 S 中的点相邻, 因而其在 G 中的顶点度 $\frac{v-|S|}{2}-1+|S| = \frac{v+|S|-2}{2}$。结合 |S|<k, 这意味着 $\delta(G) \leq \frac{v+|S|-2}{2} < \frac{v+k-2}{2}$, 与定理条件矛盾。

证毕.



若最小度如题所述，那么假设存在大小<k的点割集S，将G-S分为G’与G2，此时考察G-S中较小的连通分支（不妨设为G’）中点的度数，产生矛盾

Problem 15

Problem 15

设 n 阶图 G 的边数为 m，试证明：若 $m > C_{n-1}^2$，则 G 为连通图。

答案：

证明：假设 G 不连通，有 2 个或以上连通分支。(2 分)

设其中一个连通分支中顶点数为 $n_1 \geq 1$，其余顶点数为 $n_2 \geq 1$，$n_1 + n_2 = n$，$m \leq C_{n_1}^2 + C_{n_2}^2$ （4 分）

可以验证：$C_{n_1}^2 + C_{n_2}^2 \leq C_{n-1}^2$，即 $n_1(n_1-1) + n_2(n_2-1) \leq (n-1)(n-2)$ （4 分）

验证中用到关键等式：$0 \leq (n1-1)(n2-1)$

因此 $m \leq C_{n-1}^2$，矛盾。所以 G 为连通图。

简单来说，只要分成两个连通分支或以上，那么边数就小于等于C(n-1, 2)

第十七周习题课

离散数学

南京大学计算机科学与技术系

内容提要

- 生成树和树的应用

Prim算法（求最小生成树）

1: E={*e*}, *e*是权最小的边

2: 从E以外选择与E里顶点关联，又不会与E中的边构成回路的权最小的边加入E

3: 重复第2步，直到E中包含*n*-1条边

算法结束

Kruskal算法（求最小生成树）

1: E={ }

2: 从E以外选择不会与E中的边构成回路的权最小的边加入E

3: 重复第2步，直到E中包含*n*-1条边

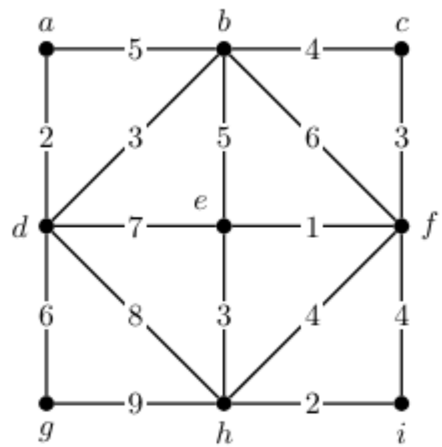
算法结束

Problem 1

Problem 1

分别用普林（Prim）算法和克鲁斯卡尔（Kruskal）

总的权值即可）



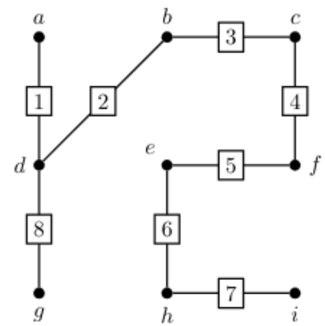


Figure 1: *

Prim

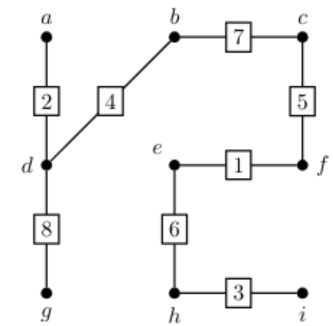


Figure 2: *

Kruskal

答案： 最小生成树权值应为 24。

Prim 选边序列：$(a, d), (d, b), (b, c), (c, f), (f, e), (e, h), (h, i), (d, g)$

Kruskal 选边序列：$(e, f), (a, d), (h, i), (b, d), (c, f), (e, h), (b, c), (d, g)$

Problem 2

Problem 2

试求以下无向带权图的最小生成树 T（请直接将图中所求最小生成树的边加粗），并求此最小生成树的权值 $W(T)$.

答案:

$W(MST)$=1+2+2+3+3+4+5=20

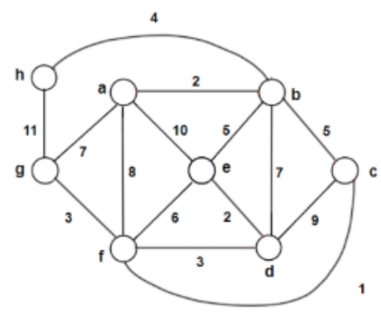
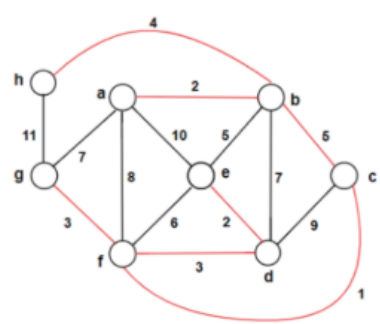


Figure 3: 第七题图



Problem 3

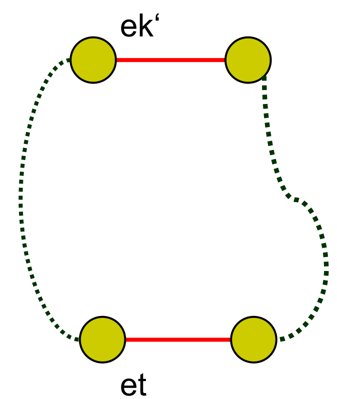
证明或反驳：每条边权重均不相同的带权图

1）有唯一的最小生成树。

2）有唯一的“次小生成树”满足，存在一最小生成树的权值小于等于该树，且其他生成树的权值均大于等于该树。

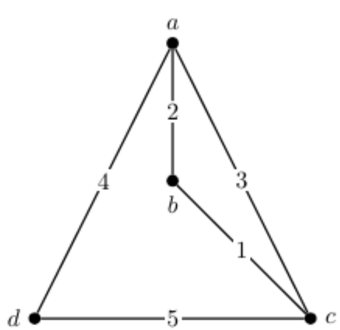
答案：

1）反证，记不同的最小生成树 T,T' 边集按权重从小到大排序为 $T=\{e_1,e_2,\dots,e_{n-1}\},T'=\{e'_1,e'_2,...,e'_{n-1}\}$。因为 $T\neq T'$，必存在最小的 $k<n$ 使得 $e_k\neq e'_k$，不妨令 $w(e'_k)<w(e_k)$，将 e'_k 加入 T，得到的 $T+e'_k$ 中有一个包含 e'_k 的圈 C，因为 $\{e_1,e_2,\dots,e_{k-1},e'_k\}=\{e'_1,e'_2,\dots,e'_k\}\subseteq T'$ 无环，所以存在 $t>k.e_t\in C$，删去 e_t 得到 G 的另一个生成树 $T+e'_k-e_t$，$w(T+e'_k-e_t)=w(T)+w(e'_k)-w(e_t)<w(T)+w(e'_k)-w(e_k)<w(T)$，与 T 是 G 上的最小生成树矛盾。



2）反驳，如下图

最小生成树 $\{(a,b),(b,c),(a,d)\}$，次小生成树 $\{(b,c),(a,c),(a,d)\}$ 和 $\{(a,b),(b,c),(c,d)\}$



对于ek’与ek的选择方法使得，在T中加入ek’后构成的环中，ek’一定是环中权值最小的边。此时保留ek’而删掉另一条边，能够得到一个更小的生成树。

Problem 4

Problem 4

令 G 为一无向带权连通图，假设图中存在一个回路. 试证明：在此回路上若存在一条边 e 其权值严格大于此回路上的其它各边，则 e 不在 G 的任何最小生成树中。

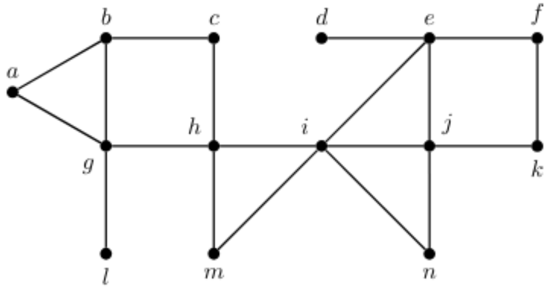
答案： 不妨假设该回路 C 是顶点不重复的简单回路，设 $e = uv$。以下使用反证法来证明 e 不在任何最小生成树中，假设 T 是包含 e 的最小生成树。$T - \{e\}$ 必含两个连通分支，设为 $T1, T2$。$C - \{e\}$ 是图 G 中的 uv-通路，其中必有一边满足其两个端点 x,y 分别在 $T1, T2$ 中，设其为 e'。$T' = T - \{e\}\ \{e'\}$，显然 T' 是生成树。因 e 的权重大于 e' 的权重，T' 的权重比 T 更小，矛盾。所以，e 不在任何最小生成树中。

与上一题类似，如果这条环的最大边在某个最小生成树中，删除它，并以环中另一条边代替之，那么得到了一个更小的生成树，矛盾

Problem 5

Problem 5

用深度优先搜索和广度优先搜索来构造下图的生成树。选择 a 作为这个生成树的根，并假定顶点都以字母顺序来排序。



答案： DFS：$\to a, a\to b, b\to c, c\to h, h\to g, g\to l, h\to i, i\to e, e\to d, e\to f, f\to k, k\to j, j\to n, i\to m$

BFS：$\to a, a\to b, a\to g, b\to c, g\to h, g\to l, h\to m, h\to i, i\to e, i\to j, i\to n, e\to d, e\to f, j\to k$

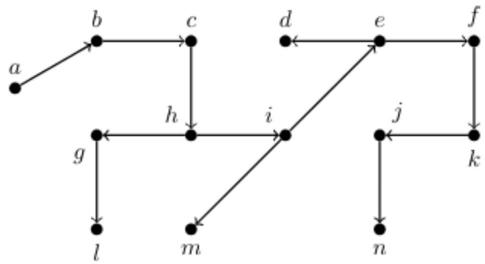


Figure 4: *

DFS

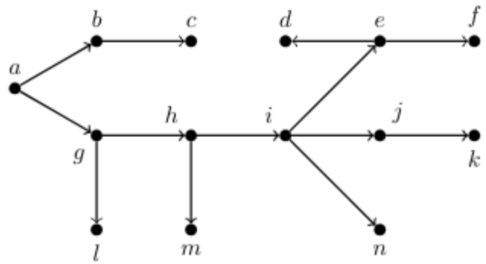


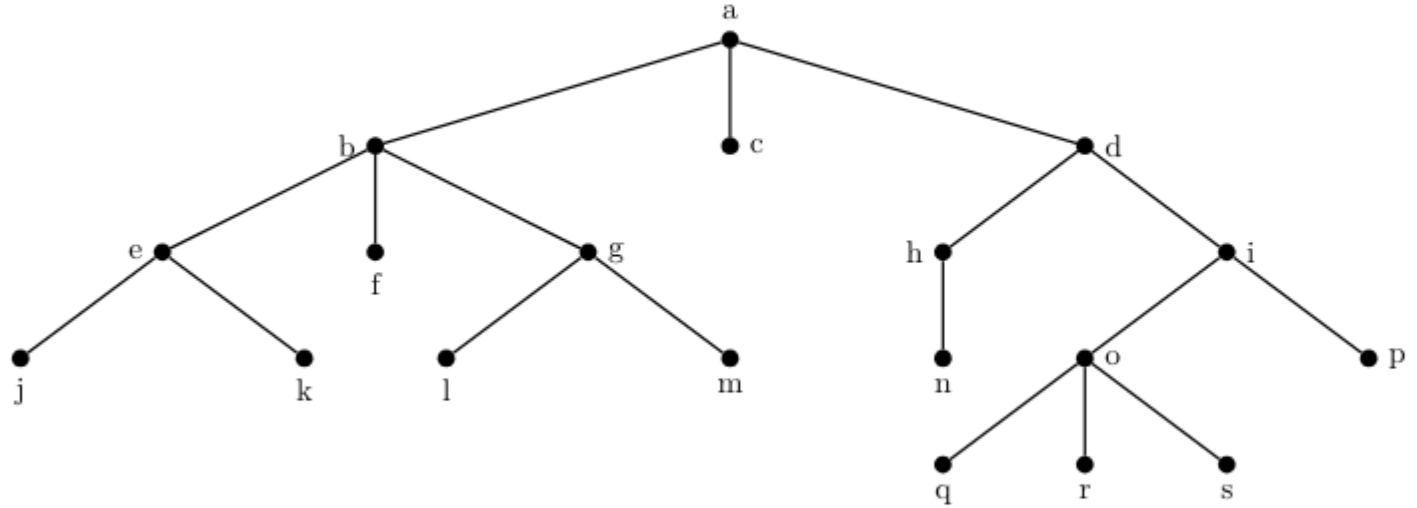
Figure 5: *

BFS

Problem 6

Problem 6

确定前序遍历、中序遍历和后续遍历下所给的有序根树的顶点的顺序。



答案： 前序：$a, b, e, j, k, f, g, l, m, c, d, h, n, i, o, q, r, s, p$；

中序：$j, e, k, b, f, l, g, m, a, c, n, h, d, q, o, r, s, i, p$；

后序：$j, k, e, f, l, m, g, b, c, n, h, q, r, s, o, p, i, d, a$。

前序遍历：先访问当前节点，再从左到右访问各子节点
中序遍历：先访问左子节点，再访问当前节点，再从左到右访问其他子节点
后序遍历：先从左到右访问各子节点，再访问当前节点

Problem 7

Problem 7

求下列前缀/后缀表达式的值（$a \uparrow b = a^b$）

a) $- \quad \times \quad 6 \quad / \quad 4 \quad 2 \quad 3$

b) $\times \quad + \quad 3 \quad + \quad 3 \quad \uparrow \quad 3 \quad - \quad 3 \quad 3 \quad 3$

c) $5 \quad 2 \quad 0 \quad - \quad - \quad 1 \quad 3 \quad 4 \quad + \quad + \quad \times$

d) $4 \quad 2 \quad \times \quad 2 \quad \uparrow \quad 6 \quad 2 \quad - \quad 6 \quad 3 \quad / \quad \times \quad -$

e) $\uparrow \quad - \quad \times \quad 4 \quad 4 \quad \times \quad 7 \quad 2 \quad + \quad 3 \quad 8$

f) $\times \quad / \quad 9 \quad 3 \quad + \quad \times \quad 2 \quad 3 \quad - \quad 9 \quad 4$

答案：

a) $-(\times(6, /(4,2)), 3) = -(\times(6,2), 3) = -(12,3) = \mathbf{9}$

b) $\times(+(3, +(3, \uparrow(3, -(3,3)))), 3) = \times(+(3, +(3, \uparrow(3,0))), 3) = \times(+(3, +(3,1)), 3) = \times(7,3) = \mathbf{21}$

c) $((5,(2,0)-)-, (1,(3,4)+)+)\times = ((5,2)-, (1,7)+)* = (3,8)\times = \mathbf{24}$

d) $(((4,2)\times, 2)\uparrow, ((6,2)-, (6,3)/)\times)- = ((8,2)\uparrow, (4,2)\times)- = (64,8)- = \mathbf{56}$

e) $\uparrow(-(\times(4,4), \times(7,2)), +(3,8)) = \uparrow(-(16,14), 11) = \uparrow(2,11) = \mathbf{2048}$

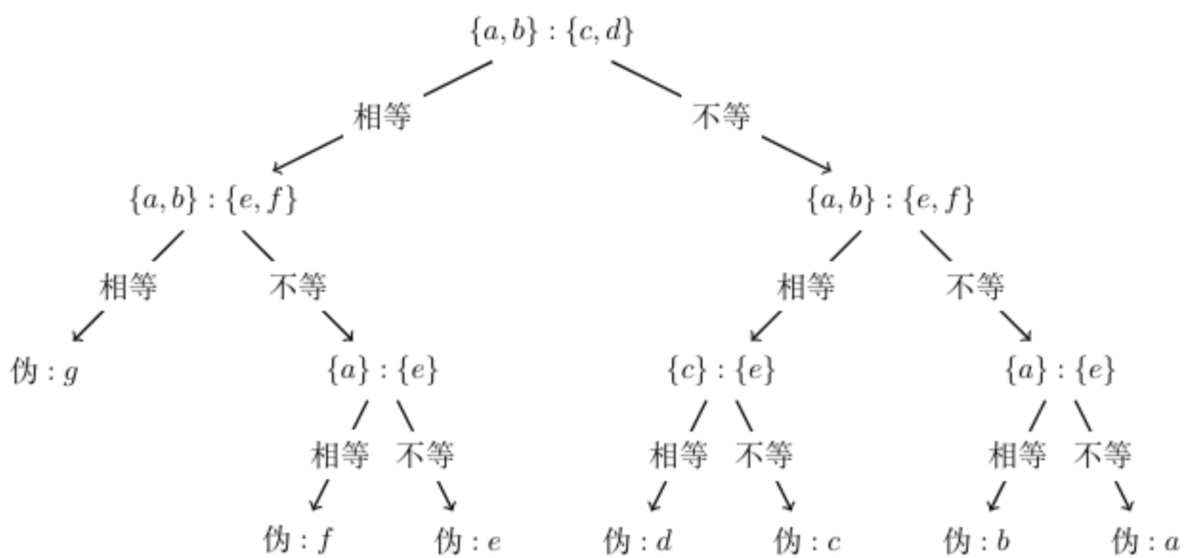
f) $\times(/(9,3), +(\times(2,3), -(9,4))) = \times(3, +(6,5)) = \times(3,11) = \mathbf{33}$

Problem 8

Problem 8

若一枚伪币与其他硬币质量不等，那么为了在 7 枚硬币中找出这枚伪币，用天平称量找出伪币的方案在最坏情况下最少要多少次？并给出相应方案（画出决策树）。

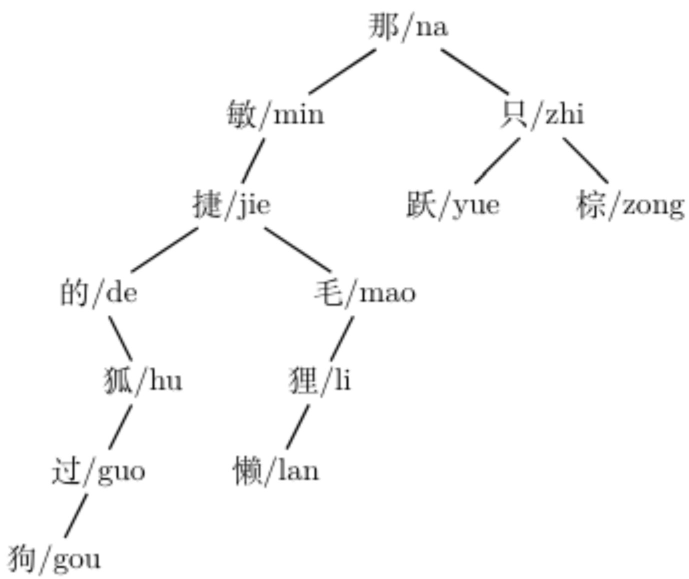
答案： 每次称量有 {相等, 不等} 两种情况，因此决策树是二元树，最终情况（叶节点数）有 7 种。将硬币编号为 $a, b, \ldots, g$，有方法如下图：最坏情况下决策树的高度为 3，即 3 次。



Problem 9

Problem 9

用字典序构造下面句子里的拼音字的二叉搜索树：“na zhi min jie de zong mao hu li yue guo na zhi lan gou”
(那只敏捷的棕毛狐狸跃过那只懒狗。)



Problem 10

Huffman Coding (1952)

- 输入：正实数序列$w_1,w_2,\ldots,w_t$。
- 输出：具有t个树叶，其权序列为$w_1,w_2,\ldots,w_t$的最优二叉树。
- 过程：
  - T棵根树（森林），其根的权分别是$w_1,w_2,\ldots,w_t$。
  - 选择根权最小的两棵树，以它们为左、右子树（合并）生成新的二叉树，其根权等于两棵子树的根权之和。
  - 重复第2步，直至形成一棵树。

注意：结果可能不唯一(如果“当前”权最小顶点对不唯一)。

Problem 10

a) 用赫夫曼编码来编码具有这些频率的符号：$a:0.36$, $b:0.18$, $c:0.18$, $d:0.10$, $e:0.08$, $f:0.06$, $g:0.04$，在算法中用以下两种不同的方式打玻平局。

I. 在算法的每个阶段从权最小的树中选择顶点数最多的两个树来组合。

II. 在每个阶段从权最小的树中选择顶点数最少的两个树来组合。

b) 计算用每种编码来编码一个符号所需要的平均位数并且对每种编码计算这个位数的方差。对于编码一个符号所需要的位数的方差，哪种打破平局的过程所产生的会小一些?

答案： 一种方案如图所示

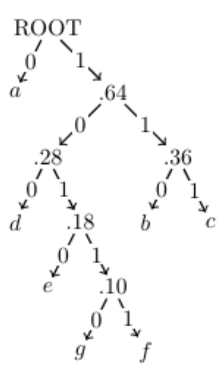


Figure 6: *

I

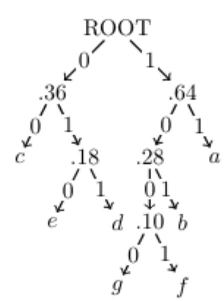
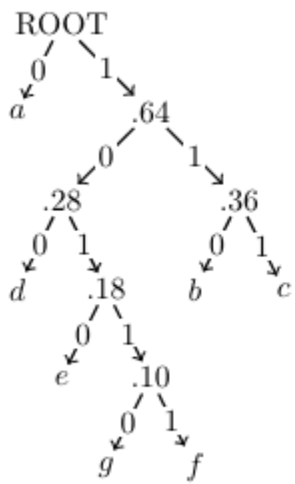


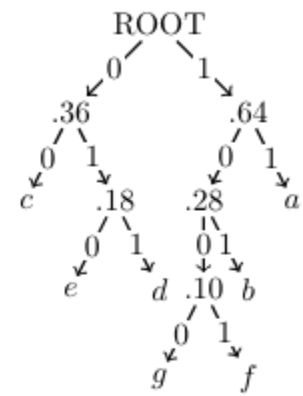
Figure 7: *

II

Problem 10

答案： 一种方案如图所示





平均值:

$$\mathrm{avg(I)} = 0.36 \times 1 + 0.18 \times 3 + 0.18 \times 3 + 0.10 \times 3 + 0.08 \times 4 + 0.06 \times 5 + 0.04 \times 5 = 2.56$$

$$\mathrm{avg(II)} = 0.36 \times 2 + 0.18 \times 3 + 0.18 \times 2 + 0.1 \times 3 + 0.08 \times 3 + 0.06 \times 4 + 0.04 \times 4 = 2.56$$

方差:

$$\mathrm{var(I)} = 0.36 \times 1^2 + 0.18 \times 3^2 + 0.18 \times 3^2 + 0.10 \times 3^2 + 0.08 \times 4^2 + 0.06 \times 5^2 + 0.04 \times 5^2 - 2.56^2 = 1.7264$$

$$\mathrm{var(II)} = 0.36 \times 2^2 + 0.18 \times 3^2 + 0.18 \times 2^2 + 0.10 \times 3^2 + 0.08 \times 3^2 + 0.06 \times 4^2 + 0.04 \times 4^2 - 2.56^2 = 0.4464$$

(II) 的方差更小

Q&A

欢迎提问