

命题逻辑

命题的定义

能判断真假的陈述句叫做命题。

- 命题是陈述句。其他的语句，如疑问句、祈使句、感叹句均不是命题。
- 这个陈述句对事物的判断是否符合客观事实是可以给出结论的：不是真 (符合客观事实)就是假 (不符合客观事实)不能不真也不假，也不能既真又假，所以又称二值逻辑。
- 悖论不是命题。

命题的真值

真值只取两个值：真 (判断与事实相符)或假 (判断与事实不符)。通常用 1 (或字母 T)表示真，用 0 (或字母 F)表示假。

命题的分类

简单命题

也称原子命题，指不能再分解为更简单的陈述句的命题。

复杂命题

由若干简单命题用联结词联结成的命题。

联结词

- 否定联结词 \neg 。否定联结词是一元联结词。相当于日常用语中的“非”、“不”、“无”、“没有”等。
- 合取联结词 \wedge 。合取词是二元联结词。相当于自然语言中的“与”、“并且”、“而且”、“也”等。
- 析取联结词 \vee 。析取词是二元联结词。相当于自然语言中的“或”、“要么...要么”等。

- 蕴含联结词 \rightarrow 。蕴含词是二元联结词。相当于自然语言中的“若... 则”、“如果... 就”、“只有... 才”。
- 等价联结词 \leftrightarrow 。等价联结词是二元联结词。相当于自然语言中的“等价”、“当且仅当”、“充要条件”等。

同时联结词的运算顺序优先级按照上方的由上到下递减。

命题公式

1. 单个命题常项或命题变项 $p, q, r, \dots, p_i, q_j, r_i, \dots$ 是命题公式。
2. 如果 A 是命题公式, 则 $\neg A$ 也是命题公式。
3. 如果 A 和 B 是命题公式, 则 $A \wedge B, A \vee B, A \rightarrow B, A \leftrightarrow B$ 均是命题公式;
4. 只有有限次地利用 (1)(3)形成的符号串才是命题公式。

公式层数

1. 若 A 是单个命题常项或命题变项, 则称 A 是 0 层公式;
2. 称 A 是 $n + 1 (n \geq 0)$ 层公式是指 A 符合下列情况之一:
 - (a) $A = \neg B$, B 是 n 层公式。
 - (b) $A = B \wedge C$, 其中 B, C 分别为 i 层和 j 层公式, 且 $n = \max(i, j)$ 。
 - (c) $A = B \vee C$, 其中 B, C 分别为 i 层和 j 层公式, 且 $n = \max(i, j)$ 。
 - (d) $A = B \rightarrow C$, 其中 B, C 分别为 i 层和 j 层公式, 且 $n = \max(i, j)$ 。
 - (e) $A = B \leftrightarrow C$, 其中 B, C 分别为 i 层和 j 层公式, 且 $n = \max(i, j)$ 。

赋值

可以使用真值表来计算命题公式的值。

- 重言式/永真式: 若命题公式 A 在所有赋值下都是真的, 则称 A 为重言式或永真式。
- 矛盾式/永假式: A 在所有赋值下都是假的, 则称 A 为称为矛盾式或永假式。

- 可满足式：若 A 至少存在一组成真赋值。

设 A 、 B 是两个命题公式, 若等价式 $A \leftrightarrow B$ 是重言式, 则称公式 A 与 B 是等价的, 记作 $A \Leftrightarrow B$ 。

公式之间的等价关系的特点:

- 自反的: $A \Leftrightarrow A$ 。
- 对称的: 若 $A \Leftrightarrow B$, 则 $B \Leftrightarrow A$ 。
- 传递的: 若 $A \Leftrightarrow B$, $B \Leftrightarrow C$, 则 $A \Leftrightarrow C$ 。

等价公式

常用等价公式:

$\neg(\neg A) \Leftrightarrow A$	双重否定律
$A \vee A \Leftrightarrow A, A \wedge A \Leftrightarrow A$	等幂律
$A \vee B \Leftrightarrow B \vee A, A \wedge B \Leftrightarrow B \wedge A$	交换律
$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$	结合律
$(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$	
$A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$	分配律
$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$	
$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$	德·摩根律
$\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$	
$A \vee (A \wedge B) \Leftrightarrow A$	吸收律
$A \wedge (A \vee B) \Leftrightarrow A$	
$A \vee 1 \Leftrightarrow 1, A \wedge 0 \Leftrightarrow 0$	零律
$A \vee 0 \Leftrightarrow A, A \wedge 1 \Leftrightarrow A$	同一律
$A \vee \neg A \Leftrightarrow 1$	排中律
$A \wedge \neg A \Leftrightarrow 0$	矛盾律
$A \rightarrow B \Leftrightarrow \neg A \vee B$	蕴含等值式
$A \leftrightarrow B \Leftrightarrow (A \rightarrow B) \wedge (B \rightarrow A)$	等价(双条件)等值式
$A \leftrightarrow B \Leftrightarrow (A \wedge B) \vee (\neg A \wedge \neg B)$	
$A \rightarrow B \Leftrightarrow \neg B \rightarrow \neg A$	假言易位
$A \leftrightarrow B \Leftrightarrow \neg A \leftrightarrow \neg B$	等价否定等值式
$(A \rightarrow B) \wedge (A \rightarrow \neg B) \Leftrightarrow \neg A$	归谬论

等价的书写规范?

置换定理

设 $\Phi(A)$ 是含命题公式 A 的命题公式， $\Phi(B)$ 是用命题公式 B 置换了 $\Phi(A)$ 中的 A 之后的得到的命题公式，如果 $A \Leftrightarrow B$ ，则 $\Phi(A) \Leftrightarrow \Phi(B)$ 。

析取范式与合取范式

仅由有限个简单合取式构成的析取式称为析取范式。

仅由有限个简单析取式构成的合取式称为合取范式。

范式存在定理

任一命题公式都存在与之等价的析取范式和合取范式。

主合取范式与主析取范式

极小项与极大项

真值表法

相互转换

真值函数

称定义域为 $\{00\dots 0, 00\dots 1, \dots, 11\dots 1\}$ ，值域为 $\{0, 1\}$ 的函数是 n 元真值函数 (其中 $n \geq 1$)。

常用 $F: \{0, 1\}^n \rightarrow \{0, 1\}$ 表示 F 是 n 元真值函数。

共有 2^{2^n} 个 n 元真值函数。

冗余与全功能集

冗余的联结词

在一个联结词的集合中, 如果一个联结词可由集合中的其他联结词定义, 则称此联结词为冗余的联结词, 否则称为独立的联结词。

全功能集

设 S 是一个联结词集合，如果任何真值函数都可以由仅含 S 中的联结词构成的公式表示，则称 S 是联结词全功能集。

若 S 是全功能集，则任何命题公式都可用 S 中的联结词表示。

若 S_1, S_2 是两个联结词集合，且 $S_1 \subseteq S_2$ ，若 S_1 是全功能集，则 S_2 也是全功能集。

若一个联结词的全功能集中不含冗余的联结词，则称它是极小全功能集。

推理

前提：已知的命题公式。

结论：从前提出发应用推理规则推出的命题公式。

推理：从前提推出结论的思维过程。

若 $(A_1 \wedge A_2 \wedge \dots \wedge A_n) \rightarrow B$ 为重言式，则称 A_1, A_2, \dots, A_n 推出结论 B 的推理正确， B 是 A_1, A_2, \dots, A_n 的逻辑结论或有效结论。称 $(A_1 \wedge A_2 \wedge \dots \wedge A_n) \rightarrow B$ 为由前提 A_1, A_2, \dots, A_n 推出结论 B 的推理的形式结构。

用“ $A \Rightarrow B$ ”表示 $A \rightarrow B$ 是重言式，因而若有前提 A_1, A_2, \dots, A_n 推出结论 B 的推理正确，也记作 $(A_1 \wedge A_2 \wedge \dots \wedge A_n) \Rightarrow B$ 或：

前提： A_1, A_2, \dots, A_n

结论： B

推理定律

$A \Rightarrow (A \vee B)$	附加律
$(A \wedge B) \Rightarrow A$	化简律
$(A \rightarrow B) \wedge A \Rightarrow B$	假言推理
$(A \rightarrow B) \wedge \neg B \Rightarrow \neg A$	拒取式
$(A \vee B) \wedge \neg B \Rightarrow A$	析取三段论
$(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow (A \rightarrow C)$	假言三段论
$(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$	等价三段论
$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (A \vee C) \Rightarrow (B \vee D)$	构造性二难
$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (\neg B \vee \neg D) \Rightarrow (\neg A \vee \neg C)$	破坏性二难

推理规则

1. 前提引入规则：在推理过程中，可以随时引入已知的前提。
2. 结论引入规则：在推理过程中，前面已推出的有效结论 (本演绎的中间结论)都可作为后续推理的前提引用。
3. 置换规则：在推理过程中，命题公式中的子公式都可以用与之等价的命题公式置换，得到证明的公式序列的另一公式。

两种特殊证明法

附加前提证明法

欲证明：

前提： A_1, A_2, \dots, A_k

结论： $C \rightarrow B$

等价地证明：

前提： A_1, A_2, \dots, A_k, C

结论： B

反证法

欲证明：

前提： A_1, A_2, \dots, A_k

结论： B

将 $\neg B$ 加入前提, 若推出矛盾, 则得证推理正确。

谓词逻辑

个体词与谓词

个体词

个体词指可以独立存在的客体，它可以是一个具体的事物，也可以是一个抽象的概念。

谓词

用来刻画个体词的性质或个体词之间关系的词是谓词。

个体常项与个体变项

表示具体的或特定的个体的词称为个体常项，一般用小写英文字母 abc 来表示，表示抽象的或泛指的个体的词称为个体变项，常用小写的英文字母 xyz 表示。个体变项的取值范围称为个体域 (或论域)。特别是，当无特殊声明时，个体域由宇宙间的一切事物组成，称为全总个体域。

谓词常项与谓词变项

表示具体性质或关系的谓词为谓词常项，用大写的英文字母 FGH 表示。表示抽象的或泛指的谓词称为谓词变项，也用大写的英文字母 FGH 表示。

N 元谓词

谓词中包含的个体词数称为元数，含有 $n(n \geq 1)$ 个个体词的谓词称为 n 元谓词。一元谓词是表示个体词性质的。当 $n \geq 2$ 时， n 元谓词表示个体词之间的关系。

0 元谓词

不带个体变项的谓词称为 0 元谓词。

量词

全称量词

对应日常语言中的“一切”，“所有的”，“任意的”等词，用符号 \forall 表示。 $\forall x$ 表示对个体域里的所有个体。 $\forall xF(x)$ 表示个体域里的所有个体都有性质 F 。

存在量词

对应日常语言中的“存在着”，“有一个”，“至少有一个”等词，用符号 \exists 表示。 $\exists x$ 表示对个体域里的个体。 $\exists xF(x)$ 表示存在着个体域中的个体具有性质 F 。

特性谓词

若一个谓词 $P(x)$ 是用来限制个体变元的取值范围，那么称谓词 $P(x)$ 为特性谓词。

对全称量词，特性谓词常作蕴含的前件，如 $\forall x(M(x) \rightarrow F(x))$

对存在量词，特性谓词常作合取项，如 $\exists x(M(x) \wedge F(x))$

1. 在不同的个体域中, 命题符号化的形式可能不一样。
2. 如果事先没有给出个体域, 都应以全总体域为个体域。
3. 在引入特性谓词后, 使用全称量词和存在量词符号化的形式是不同的。
4. 当个体域为有限集时, 如 $D = \{a_1, a_2, \dots, a_n\}$, 对于任意的谓词 $A(x)$, 都有

$$\forall xA(x) \Leftrightarrow A(a_1) \wedge A(a_2) \wedge \dots \wedge A(a_n)$$

$$\exists xA(x) \Leftrightarrow A(a_1) \vee A(a_2) \vee \dots \vee A(a_n)$$

5. 多个量词同时出现时, 不能随意颠倒它们的顺序。

字母表

字母表如下:

1. 个体常项: $a, b, c, \dots, a_i, b_i, c_i, \dots, i \geq 1$
2. 个体变项: $x, y, z, \dots, x_i, y_i, z_i, \dots, i \geq 1$
3. 函数符号: $f, g, h, \dots, f_i, g_i, h_i, \dots, i \geq 1$

4. 谓词符号: $F, G, H, \dots, F_i, G_i, H_i, \dots, i \geq 1$

5. 量词符号: \forall, \exists

6. 联结词符号: $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$

7. 括号与逗号: $(,), ,$

项

1. 个体常项和个体变项是项

2. 若 $\varphi(x_1, x_2, \dots, x_n)$ 是任意的 n 元函数, t_1, t_2, \dots, t_n 是任意的 n 个项, 则 $\varphi(t_1, t_2, \dots, t_n)$ 是项

3. 只有有限次的使用 (1)、(2)生产的符号才是项

将自然语言转换成谓词公式的步骤

1. 确定个体域, 如无特别说明, 一般使用全总个体域;

2. 根据个体域, 分析命题中的个体、个体性质以及各个个体间的关系, 确定谓词;

3. 根据表示数量的词确定量词;

4. 利用联结词将整个命题符号化

原子公式

设 $R(x_1, x_2, \dots, x_n)$ 是任意的 n 元谓词 ($n \geq 1$), t_1, t_2, \dots, t_n 是任意的 n 个项, 则称 $R(t_1, t_2, \dots, t_n)$ 是原子公式。原子公式是由项组成的 n 元谓词。

合式公式

1. 原子公式是合式公式

2. 若 A 是合式公式, 则 $(\neg A)$ 也是合式公式

3. 若 A, B 是合式公式, 则 $(A \wedge B), (A \vee B), (A \rightarrow B), (A \leftrightarrow B)$ 也是合式公式

4. 若 A 是合式公式, 则 $\exists x A, \forall x A$ 也是合式公式

5. 只有有限次地应用 (1)~(4)构成的符号串才是合式公式。在谓词逻辑中合式公式又称为谓词公式，简称为公式。

在公式 $\forall xA$ 和 $\exists xA$ 中，称 x 为指导变项， A 为相应量词的辖域。在 $\forall x$ 和 $\exists x$ 的辖域中， x 的所有出现都称为约束出现， A 中不是约束出现的其他变项的出现均称为是自由出现。

若公式 A 中无自由出现的个体变项，则称 A 是封闭的合式公式，简称闭式。

换名规则

将一个指导变项及其在辖域中所有约束出现替换成公式中没有出现的个体变项符号。

1. 改名只对约束出现的变元进行，不对自由出现的变元进行。
2. 改名必须处处进行，即对某量词约束的变元改名时，必须对原式中该变元的一切受该量词约束的约束进行改名。
3. 对受某量词约束的变元改名时新名决不能与该量词的辖域中的其它自由变元同名。
4. 改名前与改名后的约束关系保存不变。

解释

一个解释 I 由下面四部分组成：

1. 非空个体域 D 。
2. 对每一个个体常项符号指定一个 D 中的元素。
3. 对每一个函数变项符号指定一个 D 上的函数。
4. 对每一个谓词变项符号指定一个 D 上的谓词。

值得说明的是：

1. 将公式的个体常项用 I 的特定常项代替，函数和谓词用 I 的特定函数和谓词代替。
2. 被解释的公式不一定全部包含解释中的 4 部分。
3. 闭式在任何解释下都是命题。
4. 不是闭式的公式在某些解释下也可能是命题。

对于谓词公式来说：

- 永真式 (逻辑有效式)：A 在任何解释和该解释下的任何赋值下都为真
- 矛盾式 (永假式)：A 在任何解释和该解释下的任何赋值下都为假
- 可满足式：若至少存在一个解释和该解释下的一个赋值使 A 为真

命题公式中的重言式的代换实例都是永真式，命题公式中的矛盾式的代换实例都是矛盾式。

设 A, B 是谓词逻辑中的两公式，若 $A \leftrightarrow B$ 为逻辑有效式，则称 A 与 B 是等值的，记作 $A \Leftrightarrow B$ ，并称 $A \Leftrightarrow B$ 为等值式。

量词否定等值式

设 $A(x)$ 是含 x 自由出现的公式

$$1. \neg \forall x A(x) \Leftrightarrow \exists x \neg A(x)$$

$$2. \neg \exists x A(x) \Leftrightarrow \forall x \neg A(x)$$

量词辖域收缩与扩张等值式

设 $A(x)$ 是含 x 自由出现的公式， B 中不含 x 的自由出现

关于全称量词

$$1. \forall x (A(x) \vee B) \Leftrightarrow \forall x A(x) \vee B$$

$$2. \forall x (A(x) \wedge B) \Leftrightarrow \forall x A(x) \wedge B$$

$$3. \forall x (A(x) \rightarrow B) \Leftrightarrow \exists x A(x) \rightarrow B$$

$$4. \forall x (B \rightarrow A(x)) \Leftrightarrow B \rightarrow \forall x A(x)$$

关于存在量词

$$1. \exists x (A(x) \vee B) \Leftrightarrow \exists x A(x) \vee B$$

$$2. \exists x (A(x) \wedge B) \Leftrightarrow \exists x A(x) \wedge B$$

$$3. \exists x(A(x) \rightarrow B) \Leftrightarrow \forall x A(x) \rightarrow B$$

$$4. \exists x(B \rightarrow A(x)) \Leftrightarrow B \rightarrow \exists x A(x)$$

量词分配等值式

$$1. \forall x(A(x) \wedge B(x)) \Leftrightarrow \forall x A(x) \wedge \forall x B(x)$$

$$2. \exists x(A(x) \vee B(x)) \Leftrightarrow \exists x A(x) \vee \exists x B(x)$$

注意： \forall 对 \vee 无分配律， \exists 对 \wedge 无分配律，即：

$$1. \forall x(A(x) \vee B(x)) \not\Leftrightarrow \forall x A(x) \vee \forall x B(x)$$

$$2. \exists x(A(x) \wedge B(x)) \not\Leftrightarrow \exists x A(x) \wedge \exists x B(x)$$

下面两等值式成立：

$$1. \forall x \forall y A(x, y) \Leftrightarrow \forall y \forall x A(x, y)$$

$$2. \exists x \exists y A(x, y) \Leftrightarrow \exists y \exists x A(x, y)$$

其中 $A(x, y)$ 是任意的含 x, y 自由出现的谓词公式。

前束范式

设 A 为一谓词公式，若 A 具有如下形式：

$$Q_1 x_1 Q_2 x_2 \dots Q_k x_k B,$$

则称 A 为前束范式，其中每个 $Q_i (1 \leq i \leq k)$ 为 \forall 或 \exists ， B 为不含量词的谓词公式。

谓词公式化为前束范式的步骤

1. 消去联结词 $\rightarrow, \leftrightarrow$ 及多余的量词。

2. 否定深入。

3. 改名。即利用换名规则、代入规则更换一些变元的名称，以便消除混乱。

4. 量词前移。即利用量词辖域的收缩与扩张把量词移到前面，这样便可求出与公式等价的前束范式。

集合

概念

集合就是一些事物构成的整体，且任一事物是否属于一个集合是完全确定的：要么属于，要么不属于，没有模糊空间。

集合的表示

列举法（花名册法 roster）；谓词表示法（集合构造器 set builder）

符号	含义	元素
\emptyset	空集	不包含任何元素的集合
\mathbb{N}	自然数集	$\{0, 1, 2, 3, \dots\}$
\mathbb{Z}	整数集	$\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
\mathbb{Z}^+	正整数集	$\{1, 2, 3, \dots\}$
\mathbb{Q}	有理数集	$\{\frac{p}{q} \mid p, q \in \mathbb{Z}, q \neq 0\}$
\mathbb{R}	实数集	所有实数构成的集合
\mathbb{C}	复数集	所有复数构成的集合

集合中元素的三个特性

确定性：某一元素是否属于一个集合是完全确定的

互异性：同一集合中的元素是互相不同的

无序性：构成集合的各元素地位等同，无先后次序

集合之间的关系

包含 (子集)	$A \subseteq B \Leftrightarrow \forall x(x \in A \rightarrow x \in B)$
不包含	$A \not\subseteq B \Leftrightarrow \exists x(x \in A \wedge x \notin B)$
相等	$A = B \Leftrightarrow A \subseteq B \wedge B \subseteq A$
不相等	$A \neq B$
真包含 (真子集)	$A \subset B \Leftrightarrow A \subseteq B \wedge A \neq B$
不真包含	$A \not\subset B$

空集 \emptyset ：不含任何元素的集合

集合的大小

对于有限集 S ，如果 S 中恰有 n 个不同的元素，则称 n 是 S 的基数。 S 的基数记为 $|S|$ 。如果 $|S| = n$ ，则称 S 是 n 元集，它的含有 m 个 ($m \leq n$) 元素的子集称作它的 m 元子集。如果集合不是有限集，则称它是无限的。

幂集 (Power Set)

集合 S 的幂集是集合 S 所有子集的集合，记作 $P(S)$ 。

$$P(S) = \{x | x \subseteq S\}$$

集合包含关系的性质

1. 对任意集合 A ， $\emptyset \subseteq A$ 。
2. 自反性： $A \subseteq A$ 。
3. 反对称性：若 $A \subseteq B$ 且 $B \subseteq A$ ，则 $A = B$ 。
4. 传递性：若 $A \subseteq B$ 且 $B \subseteq C$ ，则 $A \subseteq C$ 。
5. 若 $|A| = n$ ，则 A 有 2^n 个子集。

集合的运算

并集： $A \cup B = \{x | x \in A \vee x \in B\}$

交集： $A \cap B = \{x | x \in A \wedge x \in B\}$

相对补集： $A - B = \{x | x \in A \wedge x \notin B\}$

对称差： $A \oplus B = (A - B) \cup (B - A)$

全集

在一个具体问题中，如果所涉及的集合都是某个集合的子集，则称这个集合为全集，记作 E (或 U)。全集具有相对性在给定问题中，全集包含任何集合，即 $\forall A (A \subseteq E)$

集合中的元素不重复出现，当允许元素重复出现时称作多重集。

设 A 与 B 为两集合，称 $\{\{a, b\} | a \in A \wedge b \in B\}$ 为 A 与 B 的无序积。记作 $A \& B$ 。为方便起见，将无序对 $\{a, b\}$ 记为 (a, b) 。

集合运算法则

幂等律	$A \cup A = A$
交换律	$A \cap A = A$ $A \cup B = B \cup A$ $A \cap B = B \cap A$
结合律	$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$
分配律	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
恒等律	$A \cup \emptyset = A$ $A \cap E = A$
支配律	$A \cup E = E$
互补律	$A \cap \emptyset = \emptyset$ $A \cup \bar{A} = E$ $A \cap \bar{A} = \emptyset$
吸收律	$A \cup (A \cap B) = A$ $A \cap (A \cup B) = A$
双重否定律	$\overline{(\bar{A})} = A$

德·摩根 (De Morgan)对偶原理

效果：将关于集合的某种性质转移到它的补集上去。

绝对补集情况：

$$\overline{B \cup C} = \bar{B} \cap \bar{C}$$
$$\overline{B \cap C} = \bar{B} \cup \bar{C}$$

相对补集情况：

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

对称差运算法则

$$\begin{aligned}A \oplus A &= \emptyset & A \oplus \emptyset &= A \\A \oplus E &= \bar{A} & A \oplus B &= B \oplus A \\A \oplus B &= (A \cup B) \cap (\bar{A} \cup \bar{B}) \\A \oplus B &= (A \cap \bar{B}) \cup (B \cap \bar{A}) \\A \cup B &= (A \oplus B) \cup (A \cap B) \\(A \oplus B) \oplus C &= A \oplus (B \oplus C) \\A \cap (B \oplus C) &= (A \cap B) \oplus (A \cap C) \\&\text{iff } A \oplus B = A \oplus C, \text{ then } B = C \\A \oplus B &= (A - B) \cup (B - A) \\A \oplus B &= (A \cup B) - (A \cap B) \\A - B &= A \cap \bar{B}\end{aligned}$$

包含排斥原理

设 S 为有限集, P_1, P_2, \dots, P_m 是 m 种性质, A_i 是 S 中具有性质 P_i 的元素构成的子集, $i = 1, 2, \dots, m$, 则 S 中不具有性质 P_1, P_2, \dots, P_m 的元素数为:

$$\begin{aligned}&|\overline{A_1 \cap A_2 \cap \dots \cap A_m}| \\&= |S| - \sum_{i=1}^m |A_i| + \sum_{1 \leq i < j \leq m} |A_i \cap A_j| - \sum_{1 \leq i < j < k \leq m} |A_i \cap A_j \cap A_k| + \dots \\&+ (-1)^m |A_1 \cap A_2 \cap \dots \cap A_m|\end{aligned}$$

证明要点: 任何元素 x , 如果不具有任何性质, 则对等式右边计数贡献为 1, 否则为 0。

推论: S 中至少具有一条性质的元素数为:

$$\begin{aligned}&|A_1 \cup A_2 \cup \dots \cup A_m| \\&= \sum_{i=1}^m |A_i| - \sum_{1 \leq i < j \leq m} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq m} |A_i \cap A_j \cap A_k| + \dots \\&+ (-1)^{m-1} |A_1 \cap A_2 \cap \dots \cap A_m|\end{aligned}$$

加法法则

如果事件 A 有 p 种产生的方式, 事件 B 有 q 种产生的方式, 则事件“ A 或 B ”有 $p + q$ 种产生的方式。

乘法法则

如果事件 A 有 p 种产生的方式，事件 B 有 q 种产生的方式，则事件“ A 与 B ”有 pq 种产生的方式。

排列与组合

排列问题：从某个集合中有序地选取若干个元素的问题

组合问题：从某个集合中无序地选取若干个元素的问题

这类问题可以根据是否有序、是否允许重复，而划分成 4 种：

1. 不允许重复的有序选取：集合的排列
2. 允许重复的有序选取：多重集的排列
3. 不允许重复的无序选取：集合的组合
4. 允许重复的无序选取：多重集的组合

排列

从 n 个元素的集合 S 中有序选取的 r 个元素叫做 S 的一个 r 排列，不同的排列总数记作 P_n^r (或 $P(n, r)$)。如果 $r = n$ ，则称这个排列为 S 的全排列，简称 S 的排列。

当 $r > n$ 时， $P_n^r = 0$ 。

对满足 $r \leq n$ 的正整数 n 和 r 有：

$$P_n^r = n(n-1) \cdots (n-r+1)$$

一个 n 元素 S 的环形 r 排列数是：

$$\frac{P_n^r}{r} = \frac{n!}{r(n-r)!}$$

如果 $r = n$ ，则 S 的环排列数是 $(n-1)!$ 。

从 n 元集 S 中无序选取的 r 个元素叫做 S 的一个 r 组合，不同组合总数记作 C_n^r ($C(n, r)$ 或 $\binom{n}{r}$)。当 $n \geq 0$ 时，规定 $C_n^0 = 1$ 。当 $r > n$ 时， $C_n^r = 0$ 。

对一切 $r \leq n$, 有 $P_n^r = r!C_n^r$, 即 $C_n^r = \frac{n!}{r!(n-r)!}$ 。

$$\forall r \leq n, \text{ 有 } C_n^r = C_n^{n-r}$$

设 S 为 n 元集, 则 S 的子集总数是:

$$2^n = C_n^0 + C_n^1 + \cdots + C_n^n$$

设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$, 从 S 中有序选取的 r 个元素叫做 S 的一个 r 排列, 当 $r = n$ 时, $n = n_1 + n_2 + \cdots + n_k$, 也叫做 S 的一个排列。

设多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$, 则 S 的 r 排列数是 k^r 。

推论: 设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$, 并且对一切 $i = 1, 2, \cdots, k$ 有 $n_i \geq r$, 则 S 的 r 排列数是 k^r 。

设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$, 且 $n = n_1 + n_2 + \cdots + n_k$, 则 S 的排列数等于 $\frac{n!}{n_1!n_2!\cdots n_k!}$ 。简记为 $\binom{n}{n_1 n_2 \cdots n_k}$ 。

设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$, S 的含有 r 个元素的子多重集叫做 S 的 r 组合。

设多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$, 则 S 的 r 组合数是 C_{k+r-1}^r 。

推论 1: 设多重集 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$, 且对一切 $i = 1, 2, \cdots, k$ 有 $n_i \geq r$, 则 S 的 r 组合数是 C_{k+r-1}^r 。

推论 2: 设多重集 $S = \{\infty \cdot a_1, \infty \cdot a_2, \cdots, \infty \cdot a_k\}$, $r \geq k$, 则 S 中每个元素至少取一个的 r 组合数是 C_{r-1}^{k-1} 。

设 $S = \{n_1 \cdot a_1, n_2 \cdot a_2, \cdots, n_k \cdot a_k\}$, $n = n_1 + n_2 + \cdots + n_k$, 则 S 的 r 组合数 N 满足:

1. 若 $r > n$, 则 $N = 0$ 。
2. 若 $r = n$, 则 $N = 1$ 。
3. 若 $r < n$, 且对一切 $i = 1, 2, \cdots, k$ 有 $n_i \geq r$, 则 $N = C_{k+r-1}^r$ 。
4. 若 $r < n$, 且存在着某个 $n_i < r$, 则对 N 没有一般的求解公式, 可以用包含排斥原理或其他的组合数学方法求解。

映射

设 A 与 B 是两个非空集合。如果按照一定的法则 f ，对于 A 中的每个元素 x ，都存在 B 中的一个确定的元素 y 与 x 相对应，那么称 f 是定义在 A 上取值于 B 中的一个映射，记作 $f: A \rightarrow B$ ， y 称为 x 在映射 f 下的象，记作 $y = f(x)$ 。对于固定的 y ， A 中适合关系式 $y = f(x)$ 的 x 的全体称为 y 的原象， A 称为映射 f 的定义域， $f(A) = \{f(x) | x \in A\}$ 称为映射 f 的值域。

若 B 是一个数集，此时映射 f 称为泛函，即定义在集 A 上的函数；若 A 与 B 都是数集， f 就是通常的函数。

设 X 为任一集合， A 是 X 的一个子集，定义

$$\chi_A(x) = \begin{cases} 0, & x \notin A \\ 1, & x \in A \end{cases}$$

则映射 $\chi_A: X \rightarrow \{0, 1\}$ 是集合 X 上的一个函数，称为 A 的特征函数。

设有映射 $f: A \rightarrow B$ 。若 $f(A) = B$ ，即对 B 中的每个元素 y 都有 A 中的元素 x ，使 $f(x) = y$ ，则称 f 是一个满射，或 A 到 B 上的映射；若对于 $f(A)$ 中的每个元 y ，都有 A 中的唯一的元 x ，使 $f(x) = y$ ，或者等价地，对于 A 中的任意不同元 x_1 与 x_2 ，都有 $f(x_1) \neq f(x_2)$ ，则称 f 是一个单射；若 f 既是满射，又是单射，即对于 B 中的每个元 y ，都有 A 中的唯一元 x ，使 $f(x) = y$ ，则称 f 是一个双射或 A 到 B 上的一一映射。

设 A 与 B 是两个非空集合，若存在一个从 A 到 B 上的一一映射，则称集合 A 与 B 是对等的，或称 A 与 B 是一一对应的，记作 $A \sim B$ 。

设 A 与 B 是两个集合，如果 $A \sim B$ ，那么就称 A 与 B 具有相同的势。集合 A 的势记为 $\overset{=}{A}$ 。

对等关系具有下述基本性质：

1. 自反性： $A \sim A$ 。
2. 对称性：若 $A \sim B$ ，则 $B \sim A$ 。
3. 传递性：若 $A \sim B$ ， $B \sim C$ ，则 $A \sim C$ 。

因此可以将势相同的集合归于同一类。

设 A 与 B 是两个集合, 若 A 对等于 B 的一个子集, 则称 A 的势小于或等于 B 的势 (或 B 的势大于或等于 A 的势), 记作 $A \leq \bar{B}$ (或 $B \geq A$)。若 $A \leq B$ 且 A 与 B 不对等, 则称 A 的势小于 B 的势 (或 B 的势大于 A 的势), 记作 $\bar{A} < \bar{B}$ (或 $\bar{B} > \bar{A}$)。

凡与正整数对等的集合称为可数集 (或可列集)。

可数集的势用 \aleph_0 表示, 读作“阿列夫零”。

任意的无限集都有一个可数子集

可数集的子集或者是有限集, 或者是可数集

推论可数集是无限集中具有最小势的一类集。

可数个可数集的并是可数集

可数集是无限集中最简单的一类集, 然而, 并非任何无限集都是可数集。

区间 $[0, 1]$ 中的点的全体构成一个不可数集。

区间 $[0, 1]$ 的点构成的集合的势称为连续统的势, 记作 \aleph (读作“阿列夫”)

实数集的势为 \aleph

伯恩斯坦 (Bernstein) 定理: 设 A 与 B 是两个非空集。若 $A_0 \subset A, B_0 \subset B$, 且 $A \sim B_0, B \sim A_0$, 则 $A \sim B$ 。

无理数集的势为 \aleph 。

康托猜想或连续统假设: 在 \aleph_0 与 \aleph 之间不存在另一种势。

非空集合 A 的幂集的势比 A 本身的势大。

闭区间套定理

设 $\{[a_n, b_n]\}$ 是 \mathbb{R} 中的闭区间列 ($n \geq 1$), 如果满足:

$$1. [a_1, b_1] \supset [a_2, b_2] \supset \dots \supset [a_n, b_n] \supset \dots$$

$$2. \lim_{n \rightarrow \infty} (b_n - a_n) = 0$$

则存在唯一实数 ξ 属于所有闭区间 $[a_n, b_n], n \geq 1$ 。

Cantor 集

Cantor 集的势为 \aleph 。

因为 Cantor 集在构造的过程中，去掉中间保留左右两侧，用 L 与 R 表示则对于 Cantor 集中的点，LR 交替出现，若 L 表示为 0，R 表示为 1，同时在前面加上 0.，Cantor 集中的点可以表示为二进制小数，也就与 $[0, 1]$ 一一对应，所以与 $[0, 1]$ 等势，势为 \aleph 。



无向图

无向图 G 是一个二元组，其中：

1. G 的顶点集 V 是非空有穷集合，其元素称为顶点或节点。
2. G 的边集 E 为 $V \times V$ 的多重子集，其元素称为无向边，简称边。

有向图

有向图 D 是一个二元组，其中：

1. 顶点集 V 是非空有穷集合，其元素称为顶点或节点。
2. 边集 E 为卡氏积 $V \times V$ 的多重子集，其元素称为有向边，简称边。
3. D 的基图：用无向边代替有向边。

n 阶图： n 个顶点的图。

零图： $E = \emptyset$ 。

平凡图： 1 阶零图。

空图： $V = \emptyset$ 。

设 $e = (u, v)$ 是无向图 $G = \langle V, E \rangle$ 的一条边，称 u, v 为 e 的端点， e 与 $u(v)$ 关联。若 $u \neq v$ ，则称 e 与 $u(v)$ 的关联次数为 1；若 $u = v$ ，则称 e 为环，此时称 e 与 u 的关联次数为 2；若 w 不是 e 端点，则称 e 与 w 的关联次数为 0。无边关联的顶点称作孤立点。

设 $e = (u, v)$ 是有向图 $D = \langle V, E \rangle$ 的一条有向边, u 为 e 的始点, v 为 e 的终点, 称 u, v 为 e 的端点, e 与 $u(v)$ 关联。无边关联的顶点称作孤立点。若有一条有向边的始点与终点重合, 称该边为环。

$G = \langle V, E \rangle$ 为无向图, $v \in V$:

- v 的度数 (度) $d(v)$: v 作为边的端点的次数之和。
- 悬挂顶点: 度数为 1 的顶点。
- 悬挂边: 与悬挂顶点关联的边。
- G 的最大度 $\Delta(G) = \max\{d(v) | v \in V\}$ 。
- G 的最小度 $\delta(G) = \min\{d(v) | v \in V\}$ 。

顶点的度数

- v 的出度 $d^+(v)$: v 作为边的始点次数之和
- v 的入度 $d^-(v)$: v 作为边的终点次数之和
- v 的度数 (度) $d(v)$: v 作为边的端点次数之和

$$D(v) = d^+(v) + d^-(v)$$

D 的最大出度: $\Delta^+(D) = \max\{d^+(v) | v \in V\}$ 。

D 的最小出度: $\delta^+(D) = \min\{d^+(v) | v \in V\}$ 。

D 的最大入度: $\Delta^-(D) = \max\{d^-(v) | v \in V\}$ 。

D 的最小入度: $\delta^-(D) = \min\{d^-(v) | v \in V\}$ 。

D 的最大度: $\Delta(D) = \max\{d(v) | v \in V\}$ 。

D 的最小度: $\delta(D) = \min\{d(v) | v \in V\}$ 。

设图 $G = \langle V, E \rangle$ 为无向图或有向图, $V = \{v_1, v_2, \dots, v_n\}$, 边数 $|E| = m$, 则:

$$\sum_{i=1}^n d(v_i) = 2m.$$

推论: 任何图 (无向或有向), 度数为基数的顶点个数是偶数。

设有向图 $D = \langle V, E \rangle$, $V = \{v_1, v_2, \dots, v_n\}$, $|E| = m$, 则:

$$\sum_{i=1}^n d^+(v_i) = \sum_{i=1}^n d^-(v_i) = m$$

多重图与简单图

1. 在无向图中，如果有 2 条或 2 条以上的边关联同一对顶点，则称这些边为平行边，平行边的条数称为重数。
2. 在有向图中，如果有 2 条或 2 条以上的边具有相同的始点和终点，则称这些边为有向平行边，简称平行边，平行边的条数称为重数。
3. 含平行边的图称为多重图。
4. 既无平行边也无环的图称为简单图。

完全图

设 $G = \langle V, E \rangle$ 是 n 阶无向简单图，若 G 中任何顶点都与其余的 $n - 1$ 个顶点相邻，则称 G 为 n 阶无向完全图，记作 K_n 。设 $D = \langle V, E \rangle$ 是 n 阶有向简单图，若对于任意的顶点 $u, v \in V (u \neq v)$ ，既有有向边 $\langle u, v \rangle$ ，又有 $\langle v, u \rangle$ ，则称 D 为 n 阶有向完全图。

子图

设 $G = \langle V, E \rangle$ ， $G' = \langle V', E' \rangle$ 是两个图：

1. 若 $V' \subseteq V$ 且 $E' \subseteq E$ ，则称 G' 为 G 的子图， G 为 G' 的母图，记作 $G' \subseteq G$ 。
2. 若 $G' \subseteq G$ 且 $V' = V$ ，则称 G' 为 G 的生成子图。
3. 若 $G' \subseteq G$ 且 $G' \neq G$ ，称 G' 为 G 的真子图。
4. 设 $V_1 \subseteq V$ 且 $V_1 \neq \emptyset$ ，以 V_1 为顶点集，以两端点都在 V_1 中的所有边为边集的 G 的子图称作 V_1 的导出子图，记作 $G[V_1]$ 。
5. 设 $E_1 \subseteq E$ 且 $E_1 \neq \emptyset$ ，以 E_1 为边集，以 E_1 中边关联的所有顶点为顶点集的 G 的子图称作 E_1 的导出子图，记作 $G[E_1]$ 。

补图

设 $G = \langle V, E \rangle$ 为 n 阶无向简单图, G 的补图 \bar{G} 定义如下: $\bar{G} = \langle V, \bar{E} \rangle$, 其中 $\bar{E} = \{(u, v) \mid u, v \in V, (u, v) \notin E\}$ 。

同构

设两个无向图 $G_1 = \langle V_1, E_1 \rangle$, $G_2 = \langle V_2, E_2 \rangle$, 如果存在双射函数 $f: V_1 \rightarrow V_2$, 使得对于任意的 $e = (u, v) \in E_1$, 当且仅当 $e' = (f(u), f(v)) \in E_2$, 并且 e 与 e' 的重数相同, 则称 G_1 与 G_2 是同构的, 记作 $G_1 \cong G_2$ 。

必要条件:

1. 边数相同, 顶点数相同
2. 度数列相同 (不计度数的顺序)
3. 对应顶点的关联集及邻域的元素个数相同

通路 & 回路

设 G 中顶点与边的交替序列 $\Gamma = V_0 e_1 V_1 e_2 \cdots e_l V_l$, 若 $1 \leq i \leq l, v_{i-1}, V_i$ 是 e_i 的端点 (当 G 是有向图, 要求 v_{i-1} 是 e_i 始点, v_i 是 e_i 终点), 则称 Γ 为顶点 v_0 到 v_l 的通路, v_0 和 v_l 分别称为此通路的起点和终点, Γ 中边的数目 l 为称为 Γ 的长度。又若 $v_0 = v_l$, 则称 Γ 为回路。

Γ 中所有边互不相同, 则称 Γ 为简单通路, 当 $v_0 = v_l$ 时, 称此简单通路为简单回路。

Γ 中除 v_0, v_l 外所有顶点互不相同, 所有的边也互不相同, 则称此通路为初级通路或路径, 当 $v_0 = v_l$ 时, 称此通路为初级回路或圈。

有边重复出现的通路称为复杂通路吗, 有边重复出现的回路称为复杂回路。

表示方法:

1. 用顶点和边的交替序列 (定义), 如 $\Gamma = V_0 e_1 V_1 e_2 \cdots e_l V_l$ 。
2. 用边的序列, 如 $\Gamma = e_1 e_2 \cdots e_l$ 。
3. 简单图中, 用顶点的序列, 如 $\Gamma = v_0 v_1 \cdots V_l$ 。

4. 非简单图中, 可用混合表示法, 如 $\Gamma = v_0v_1e_2v_2e_5v_3v_4v_5$ 。

无向图: 环是长度为 1 的圈, 两条平行边构成长度为 2 的圈。

有向图: 环和两条方向相反边构成的回路分别为长度为 1 和 2 的圈。

在无向简单图中, 所有圈的长度 ≥ 3 ; 在有向简单图中, 所有圈的长度 ≥ 2 。

圈的个数

定义意义下:

- 在无向图中, 一个长度为 l ($l \geq 3$) 的圈看作 $2l$ 个不同的圈。
- 在有向图中, 一个长度为 l ($l \geq 3$) 的圈看作 l 个不同的圈。

同构意义下:

- 所有长度相同的圈都是同构的, 因而是 1 个圈。

在一个 n 阶图 G 中, 若从顶点 u 到 $V(u \neq v)$ 存在通路, 则从 u 到 v 存在长度小于等于 $n - 1$ 的通路。

推论: 在一个 n 阶图 G 中, 若从顶点 u 到 v ($u \neq v$) 存在通路, 则从 u 到 v 存在长度小于等于 $n - 1$ 的初级通路。

在一个 n 阶图 G 中, 若存在 v 到自身的回路, 则一定存在 v 到自身长度小于等于 n 的回路。

在一个 n 阶图 G 中, 若存在 v 到自身的简单回路, 则存在 v 到自身长度小于等于 n 的初级回路。

在一个无向图 G 中, 若从顶点 u 到 v 存在通路 (当然从 v 到 u 也存在通路), 则称 u 与 v 是连通的。规定任何顶点与自身总是连通的。

在一个有向图 D 中, 若从顶点 u 到 v 存在通路, 则称 u 可达 v 。规定任何顶点到自身总是可达的。

若无向图 G 是平凡图或 G 中任意两顶点都是连通的, 则称 G 是连通图; 否则, 称 G 是非连通图。

连通分支

在无向图中，顶点之间的连通关系是等价关系。设 G 为一个无向图， R 是 G 中顶点之间的连通关系。按照 R 可将 $V(G)$ 划分成若干个等价类，设为 V_1, V_2, \dots, V_k 由它们导出的导出子图 $G[V_1], G[V_2], \dots, G[V_k]$ 称为 G 的连通分支， G 的连通分支的个数记为 $p(G)$ 。

设 D 是一个有向图，如果略去 D 中各有向边的方向后所得无向图是连通图，则称 D 是弱连通图，简称连通图。若 D 中任意两顶点至少一个可达另一个，则称 D 是单向连通图。若 D 中任何一对顶点都是相互可达的，则称 D 是强连通图。

关联矩阵

无向图

设无向图 $G = \langle V, E \rangle$, $V = \{v_1, v_2, \dots, v_n\}$, $E = \{e_1, e_2, \dots, e_m\}$, 令 m_{ij} 为 v_i 与 e_j 的关联次数，称 $(m_{ij})_{n \times m}$ 为 G 的关联矩阵，记为 $M(G)$ 。

1. 每一列恰好有两个 1 或一个 2，这是因为每条边关联两个顶点 (环关联的两个顶点重合)。
2. 第 i 行元素之和为 v_i 的度数， $\sum_{j=1}^m m_{ij} = d(v_i)$ 。
3. 所有元素之和等于 $2m$, $\sum_{i=1}^n \sum_{j=1}^m m_{ij} = \sum_{j=1}^m \sum_{i=1}^n m_{ij} = \sum_{j=1}^m d(v_j) = 2m$ 。
4. v_i 为孤立点当且仅当第 i 行全为 0。
5. e_j 与 e_k 平行边当且仅当第 j 列与第 k 列相同。

设无环有向图 $D = \langle V, E \rangle$, $V = \{v_1, v_2, \dots, v_n\}$, $E = \{e_1, e_2, \dots, e_m\}$, 令:

$$M_{ij} = \begin{cases} 1, & v_i \text{ 为 } e_j \text{ 的始点} \\ 0, & v_i \text{ 与 } e_j \text{ 不关联} \\ -1, & v_i \text{ 为 } e_j \text{ 的终点} \end{cases}$$

则称 $(m_{ij})_{n \times m}$ 为 D 的关联矩阵，记为 $M(D)$ 。

1. 每一列恰好有一个 1 和一个 -1。
2. 第 i 行 1 的个数等于 $d^+(v_i)$, -1 的个数等于 $d^-(v_i)$ 。 $M(D)$ 中所有 1 的个数等于所有 -1 的个数，且都等于 m 。

在有向图中，若存在一条边 e 以顶点 u 为始点、以 v 为终点，则称 u 邻接到 v 。

设有向图 $D = \langle V, E \rangle$, $V = \{V_1, V_2, \dots, V_n\}$, $|E| = m$, 令 $a_{ij}^{(1)}$ 为 V_i 邻接到 V_j 的边的条数，称 $(a_{ij}^{(i)})_{n \times n}$ 为 D 的邻接矩阵，记作 $A(D)$ 。

有向图的邻接矩阵有下述性质：

1. 第 i 行元素之和等于 $d^+(V_i)$, $\sum_{j=1}^n a_{ij}^{(i)} = d^+(v_i)$ 。
2. 第 j 列元素之和等于 $d^-(V_j)$, $\sum_{i=1}^n a_{ij}^{(i)} = d^-(v_j)$ 。
3. 所有元素之和等于边数 (长度为 1 的通路数), $\sum_{i=1}^n \sum_{j=1}^n a_{ij}^{(i)} = m$ 。
4. 长度为 1 的回路数为 $\sum_{i=1}^n a_{ii}^{(i)}$ 。

有向图的通路数与回路数：

设 A 为 n 阶有向图 D 的邻接矩阵，则 $A^l (\geq 1)$ 中：

$a_{ij}^{(l)}$ 为 D 中 V_i 到 V_j 长度为 l 的通路数，

$a_{ii}^{(l)}$ 为 D 中 V_i 到自身长度为 l 的回路数，

$\sum_{i=1}^n \sum_{j=1}^n a_{ij}^{(l)}$ 为 D 中长度为 l 的通路 (含回路) 总数，

$\sum_{i=1}^n a_{ii}^{(l)}$ 为 D 中长度为 l 的回路总数。

推论：设 $B_r = A + A^2 + \dots + A^r (r \geq 1)$ ，则 B_r 中元素 $b_{ij}^{(r)}$ 为 D 中 v_i 到 v_j 长度小于等于 r 的通路数， $\sum_{i=1}^n \sum_{j=1}^n b_{ij}^{(r)}$ 为 D 中长度小于等于 r 的通路 (含回路) 总数，其中 $\sum_{i=1}^n b_{ii}^{(r)}$ 为 D 中长度小于或等于 r 的回路总数。

定义 $D = \langle V, E \rangle$ 为有向图， $V = \{V_1, V_2, \dots, V_n\}$ ，令：

$$P_{tj} = \begin{cases} 1, & \text{若 } v_t \text{ 可达 } v_j, \\ 0, & \text{否则,} \end{cases}$$

称 $(p_{ij})_{n \times n}$ 为 D 的可达矩阵，记作 $P(D)$ 。性质：

1. $P(D)$ 主对角线上的元素恒为 1。
2. D 强连通当且仅当 $P(D)$ 的元素全为 1。

割集

设无向图 $G = \langle V, E \rangle$, $V' \subset V$, 若 $p(G - V') > p(G)$, 且对 V 的任何真子集 V' , $p(G - V') = p(G)$, 则称 V' 为 G 的点割集。若点割集中只有一个顶点 v , 则称 v 为割点。

又 $E' \subseteq E$, 若 $p(G - E') > p(G)$ 且对 E 的任何真子集 E' , $p(G - E') = p(G)$, 则称 E' 为 G 的边割集。简称割集。若为边割集中只有一条边 e , 则称 e 为割边或桥。

二部图

若能将无向图 $G = \langle V, E \rangle$ 的顶点集 V 划分成两个不相交的非空子集 V_1 和 V_2 , 使得 G 中的每条边的两个端点一个属于 V_1 , 另一个属于 V_2 , 则称 G 为二部图 (或偶图)。称 V_1 和 V_2 为互补顶点子集, 此时可将 G 记为 $G = \langle V_1, V_2, E \rangle$ 。

若 V_1 中每个顶点都与 V_2 中每个顶点均有且仅有一条边相关联, 则称二部图 G 为完全二部图 (或完全偶图)。当 $|V_1| = n, |V_2| = m$, 完全二部图 G 记为 $K_{n,m}$ 。

一个无向图 $G = \langle V, E \rangle$ 是二部图当且仅当 G 中没有长度为奇数的回路。

设无向图 $G = \langle V, E \rangle$, $M \subseteq E$, 若 M 中任意两条边均不相邻, 则称 M 为 G 中的匹配。若在 M 中再加入任何 1 条边就都不是匹配了, 则称 M 为极大匹配。

边数最多的匹配称为最大匹配, 最大匹配中的边的条数称为 G 的匹配数, 记为 $\beta_1(G)$, 简记为 β_1 。

设 M 为 G 中一个匹配, $v \in V(G)$, 若存在 M 中的边与 v 关联, 则称 v 为 M 的饱和点, 否则称 v 为 M 的非饱和点。若 G 中每个顶点都是 M 饱和点, 则称 M 为完美匹配。

设 $G = \langle V_1, V_2, E \rangle$ 为二部图, $|V_1| \leq |V_2|$, M 是 G 中一个最大匹配, 若 $|M| = |V_1|$, 则称 M 为 G 中 V_1 到 V_2 的完备匹配。当 $|V_1| = |V_2|$ 时, 完备匹配是完美匹配。

Hall 定理: 设二部图 $G = \langle V_1, V_2, E \rangle$ 中, $|V_1| \leq |V_2|$ 。 G 中存在从 V_1 到 V_2 的完备匹配当且仅当 V_1 中任意 k 个顶点至少邻接 V_2 中的 k 个顶点。

相异性条件

二部图 $G = \langle V_1, V_2, E \rangle$ 中，如果存在 $t > 0$ ，使得：

1. V_1 中每个顶点至少关联 t 条边。
2. V_2 中每个顶点至多关联 t 条边。

则 G 中存在 V_1 到 V_2 的完备匹配。

欧拉图

经过图（无向图或有向图）中每条边一次且仅一次并且行遍图中每个顶点的回路（通路），称为欧拉回路（欧拉通路）。存在欧拉回路的图称为欧拉图，存在欧拉通路，但无欧拉回路的图称为半欧拉图。

无向图 G 有欧拉回路，当且仅当 G 是连通图且无奇度顶点。无向图 G 有欧拉通路、但无欧拉回路，当且仅当 G 是连通图且恰有两个奇度顶点。这两个奇度顶点是欧拉通路的端点。

有向图 D 有欧拉回路，当且仅当 D 是连通的且每个顶点的入度都等于出度。有向图 D 有欧拉通路、但无欧拉回路，当且仅当 D 是连通的，且除了两个顶点外，其余顶点的入度均等于出度。这两个特殊的顶点中，一个顶点的入度比出度大 1，另一个顶点的入度比出度小 1。任何欧拉通路以前一个顶点为终点，以后一个顶点为始点。

哈密顿图

经过图中每个顶点一次且仅一次的通路称为哈密顿通路，闭合的哈密顿通路称为哈密顿回路。存在哈密顿回路的图称为哈密顿图，具有哈密顿通路而无哈密顿回路的图称为半哈密顿图。

设无向图 $G = \langle V, E \rangle$ 是哈密顿图， V_1 是 V 的任意非空子集，则：

$$P(G - V_1) \leq |V_1|$$

推论：设无向图 $G = \langle V, E \rangle$ 中有哈密顿通路， V_1 是 V 的任意非空子集，则 $p(G - V_1) \leq |V_1| + 1$ 。

无向哈密顿图的一个充分条件

设 G 是 $n(n \geq 3)$ 阶无向简单图，如果 G 中任何一对不相邻的顶点的度数之和都大于等于 $n - 1$ ，则 G 中存在哈密顿通路。如果 G 中任何一对不相邻的顶点的度数之和都大于等于 n ，则 G 中存在哈密顿图。

有向图的哈密顿通路

在 $n(n \geq 2)$ 阶有向图 $D = \langle V, E \rangle$ 中，如果所有有向边均用无向边代替，所得无向图含有生成子图 K_n ，则有向图 D 中存在哈密顿通路。

平面图

如果图 G 能画在平面上使得除顶点处外没有边交叉出现，则称 G 是平面图。画出的这种不出现边交叉的图称为 G 的一个平面嵌入。没有平面嵌入的图称作非平面图。

平面图的面与次数

设 G 是一个平面嵌入：

- G 的面：由 G 的边将平面划分成的每一个区域。
- 无限面 (外部面)：面积无限的面，用 R_0 表示。
- 有限面 (内部面)：面积有限的面，用 R_1, R_2, \dots, R_k 表示。
- 面 R_i 的边界：包围 R_i 的所有边构成的回路组。
- 面 R_i 的次数： R_i 边界的长度，用 $\deg(R_i)$ 表示。

平面图的所有面的次数之和等于边数的 2 倍。

设 G 为一个简单平面图，如果在 G 中任意不相邻的两个顶点之间再加一条边，所得图为非平面图，则称 G 为极大平面图。若在非平面图 G 中任意删除一条边，所得图为平面图，则称 G 为极小非平面图。极大平面图必连通，极小非平面图必为简单图。

$n(n \geq 3)$ 阶简单平面图是极大平面图当且仅当它连通且每个面的次数都为 3。

欧拉公式

设 G 为 n 阶 m 条边 r 个面的连通平面图，则有：

$$N - m + r = 2$$

设 G 是有 p ($p \geq 2$) 个连通分支的平面图，则：

$$N - m + r = p + 1$$

设 G 为 n 阶 m 条边的连通平面图，每个面的次数不小于 l ($l \geq 3$)，则：

$$M \leq \frac{l}{l-2}(n-2)$$

设 G 为有 p ($p \geq 2$) 个连通分支的平面图，且每个面的次数不小于 l ($l \geq 3$)，则：

$$M \leq \frac{l}{l-2}(n-p-1)$$

推论： K_5 和 $K_{3,3}$ 不是平面图。

设平面图 G ，有 n 个顶点， m 条边和 r 个面， G 的对偶图 $G^* = \langle V^*, E^* \rangle$ 如下：

在 G 的每一个面 R_i 中任取一个点 v_i^* 作为 G^* 的顶点。

$$V^* = \{v_i^* \mid i = 1, 2, \dots, r\}$$

对 G 的每一条边 e_k ，若 e_k 在 G 的面 R_i 与 R_j 的公共边界上，则作边 $e_k^* = (v_i^*, v_j^*)$ ，且与 e_k 相交。

若 e_k 为 G 中的桥且在面 R_i 的边界上，则作环 $e_k^* = (v_i^*, v_i^*)$ 。

$$E^* = \{e_k^* \mid k = 1, 2, \dots, m\}$$

无向树

不含回路的连通无向图称为无向树，简称树。每个连通分支均是树的非连通无向图称为森林。平凡图称为平凡树。树中度数为 1 的顶点称为树叶，度数大于等于 2 的顶点称为分支点。

设 $G = (V, E)$ 是 n 阶 m 条边的无向图，则下面各命题是等价的：

1. G 连通且不含回路。
2. G 的每对顶点之间有唯一的一条路径。
3. G 是连通的且 $m = n - 1$ 。
4. G 中无回路且 $m = n - 1$ 。
5. G 中无回路，但在任两个不相邻的顶点之间增加一条边，就形成唯一的一条初级回路。
6. G 是连通的且每条边都是桥。

n 阶非平凡的树中至少有 2 片树叶。

设 $G = (V, E)$ 是无向连通图， T 是 G 的生成子图并且是树，则称 T 是 G 的生成树。

生成树 T 的树枝： G 在 T 中的边。

生成树 T 的弦： G 不在 T 中的边。

生成树 T 的余树：所有弦的集合的导出子图。

设 n 阶连通无向图有 m 条边，则它的生成树有 $n - 1$ 条边，余树有 $m - n + 1$ 条边。

任何无向连通图都有生成树。

主成分分析

内积和范数

对于实向量 \mathbf{x} 和向量 \mathbf{y} ：

1. 向量 \mathbf{x} 和向量 \mathbf{y} 的内积：

$$\langle \mathbf{x}, \mathbf{y} \rangle = \mathbf{x}^T \mathbf{y} = \sum_{i=1}^n x_i y_i$$

2. 向量 \mathbf{x} 的范数：

(a) L_0 范数 (也称 0 范数)： $\|\mathbf{x}\|_0$ 定义为 \mathbf{x} 中非零元的个数。

(b) L_1 范数 (也称和范数或 1 范数)： $\|\mathbf{x}\|_1 = \sum_{i=1}^n |x_i|$ 。

(c) L_2 范数 (也称欧氏范数或 2 范数): $\|\mathbf{x}\|_2 = \left(\sum_{i=1}^n |x_i|^2\right)^{1/2}$ 。

(d) L_∞ 范数 (也称无穷范数): $\|\mathbf{x}\|_\infty = \max\{|x_1|, |x_2|, \dots, |x_n|\}$ 。

(e) L_p 范数 (也称 Hölder 范数): $\|\mathbf{x}\|_p = \left(\sum_{i=1}^n |x_i|^p\right)^{1/p}, p \geq 1$ 。

求解步骤

主成分求解步骤如下:

1. 求样本均值 $\bar{\mathbf{x}} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_p)$ 和样本的协方差矩阵 \mathbf{S} 。
2. 求解特征方程 $|\mathbf{I} - \mathbf{S}| = 0$, 解得 p 个特征根 $\lambda_1, \lambda_2, \dots, \lambda_p$ 。
3. 求每个特征值对应的单位正交特征向量 $\boldsymbol{\alpha}_i (k=1, 2, \dots, k)$, 解得 $\boldsymbol{\alpha}_i = (\alpha_{1i}, \alpha_{2i}, \dots, \alpha_i)^T$ 。
4. 写成主成分的表达式:

$$\mathbf{f}_i = \alpha_{1i} (\mathbf{x}_1 - \bar{\mathbf{x}}_1 \mathbf{1}) + \alpha_{2i} (\mathbf{x}_2 - \bar{\mathbf{x}}_2 \mathbf{1}) + \dots + \alpha_{pi} (\mathbf{x}_p - \bar{\mathbf{x}}_p \mathbf{1})$$

SVD 分解与 Moore-Penrose 逆矩阵

假设我们有一个矩阵 $A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$ 。

第一步计算 \mathbf{U}

计算矩阵 $AA^T = \begin{bmatrix} 2 & 2 & 0 \\ 2 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix}$ 。

对其进行特征分解, 分别得到特征值 $4, 0, 0$ 和对应的特征向量 $\left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right]^T, \left[-\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}, 0\right]^T, [0, 0, 1]^T$, 可以得到:

$$U = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

第二步计算 $\Sigma^{m \times n}$

$\Sigma_{mn} = \begin{bmatrix} \Sigma_1 & 0 \\ 0 & 0 \end{bmatrix}$, 其中 $\Sigma_1 = \text{diag}(\sigma_1, \sigma_1, \dots, \sigma_r)$ 是将第一步求出的非零特征值从大到小排列后开根号的值, 这里:

$$\Sigma = \begin{bmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix}$$

第三步计算 V

已知 $\text{rank}(A) = 1$ 。

$$\text{计算 } V_1 = A^T U_1 \Lambda^{-1} = \left[\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right]^T$$

将 V_1 拓展为酉矩阵 (也就是正交矩阵, 但是支持复数形式) 得到:

$$V = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}$$

最终, 我们可以得到 A 的奇异值分解:

$$A = U \Sigma V^T = \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{bmatrix}^T = \begin{bmatrix} 1 & 1 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$$

计算 Moore-Penrose 逆矩阵

$$A^+ = V \Sigma^+ U^T$$

回归

已知: $y = \beta_0 + \beta_1 x_i$

简单回归的最小二乘估计

$$\hat{\beta}_0 = \bar{y} - \hat{\beta}_1 \bar{x}$$
$$\hat{\beta}_1 = \frac{\sum_{i=1}^n x_i y_i - n \bar{x} \bar{y}}{\sum_{i=1}^n x_i^2 - n (\bar{x})^2}$$

多元回归的帽子矩阵法

$$\hat{\beta} = (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T \mathbf{y}$$
$$\hat{\mathbf{y}} = \mathbf{X} (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T \mathbf{y}$$

其中称 $\mathbf{H} = \mathbf{X} (\mathbf{X}^T \mathbf{X})^{-1} \mathbf{X}^T$ 称为帽子矩阵，它是对称幂等阵，即：

$$\mathbf{H}^T = \mathbf{H}, \quad \mathbf{H}^n = \mathbf{H}, \quad (\mathbf{I} - \mathbf{H})^n = \mathbf{I} - \mathbf{H}$$

代数系统

群

若在一个非空集合 G 上定义了一个运算，记为“ \cdot ”，称为乘法，并满足下列条件：

1. 结合律成立，对任意 $a, b, c \in G$ ，有 $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ 。
2. 有单位元素 (幺元) $e \in G$ ，满足：对任意 $a \in G$ ，有： $a \cdot e = e \cdot a = a$ 。
3. G 中任意元素 a 均有逆元素 $a^{-1} \in G$ ，满足： $a \cdot a^{-1} = a^{-1} \cdot a = e$ 。

则称 G 对于运算“ \cdot ”构成一个群，或简称 G 为一个群。只满足 1) 为半群，只满足 1) 和 2) 为带幺半群。

若上述定义的运算为加法，则将运算符号“ \cdot ”改为“ $+$ ”，幺元改为零元，逆元改为负元。

若群 G 对于上述运算还有交换律成立，即对于任意 $a, b \in G$ ，有 $a \cdot b = b \cdot a$ ，则称 G 为交换群（或称 Abel 群）。

群是一种代数系统，它是由一个非空集合与一个运算构成的。若集合不同，构成的群当然不同。对同一个集合，运算不同则构成的群也不同。

按群 G 具有元素的个数 (元数) 多少分为无限群与有限群。

有限群实例：含有 n 个元素的有限集上的所有可逆映射（称为 n 元置换），对于映射的乘法构成一个群，称为 n 元置换群，或称为 n 次对称群，记为 S_n 。 S_n 的每一个元素可以表示成一个 n 元置换：

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & \cdots & n \\ J_1 & j_2 & j_3 & \cdots & j_n \end{bmatrix}$$

其中, $j_1, j_2, j_3, \dots, j_n$ 为 $1, 2, 3, \dots, n$ 的某个排列。

无限群实例: 非空集合 U 到其自身的所有可逆映射 (或称为变换), 对于映射的乘法构成群, 称为集合 U 的全变换群, 记为 S_u 。当 U 为无限集时, S_u 为无限群。 S_u 的非空子集, 若对于映射的乘法也构成群, 则称为变换群。

群有以下简单性质:

1. 任意一个群的单位元是唯一的。群的任意元的逆元也是唯一的。
2. 若 (G, \cdot) 是一个群, 则对任意 $a, b \in G$, 方程 $a \cdot x = b$ 与 $y \cdot a = b$, 均有唯一解。
3. 消去律成立, 即:

$$\begin{aligned}A \cdot x = a \cdot y &\Rightarrow x = y \\X \cdot a = y \cdot a &\Rightarrow x = y\end{aligned}$$

群中可以定义幂:

$$\begin{aligned}A^1 &= a, a^{n+1} = a^n \cdot a \\A^0 &= e, a^{-n} = (a^{-1})^n, n > 0\end{aligned}$$

子群

如果群 G 的非空子集 H 对于 G 上定义的运算也构成一个群, 则称 H 为 G 的子群。

设 G 是任意一个群, e 是 G 的单位元, 则单位元群 $\{e\}$ 是 G 的子群, 且 G 本身也构成 G 的子群。这两个特殊的子群, 称为 G 的平凡子群。除此之外, G 的其他子群 H 可称为非平凡子群。

群 G 的非空子集 H 是 G 的子群的充要条件是:

1. 对任意 $a, b \in H$, 有 $a \cdot b \in H$ 。
2. 对任意 $a \in H$, 有 $a^{-1} \in H$ 。

群 G 的非空子集 H 是 G 的子群的充要条件是: 对任意 $a, b \in H$, 有 $a \cdot b^{-1} \in H$ 。

设 H 是群 G 的子群, 对任意给定的 $a \in G$, 记:

$$\begin{aligned}AH &= \{a \cdot h \mid \forall h \in H\} \\Ha &= \{h \cdot a \mid \forall h \in H\}\end{aligned}$$

分别称为 H 的左陪集与右陪集。

若群 G 中子群 H 的任意左陪集同时又是 H 的右陪集，也就是说， H 能够与 G 的任意元素 a 交换，即对任意 $a \in G$ 有：

$$aH = Ha$$

则称 H 为 G 的正规子群。

交换群的任意子群均是正规子群。

正规子群 H 可以定义左陪集的乘法运算：

$aH \cdot bH = aHb \cdot H = abH \cdot H = abH$ 对任意 $a, b \in G$ ， G 中所有 H 的左陪集构成的集合对于上述乘法运算构成群。

设 G 与 G' 是两个群，如果有一个 G 到 G' 上的一一对应 σ ，对于 G 与 G' 的运算，有：

$$\sigma(x \cdot y) = \sigma(x) \circ \sigma(y)$$

对任意 $x, y \in G$ 均成立。那么，就称 G 同构于 G' ，记为 $G \cong G'$ ，称满足上述条件的映射为同构映射（简称同构）。

同构把 G 的单位元变为 G 的单位元，把 G 的逆元变为 G 的逆元。

三维空间刚体运动

旋转向量

三维空间中的旋转也可以表示为向量绕着某一个单位向量旋转一个具体角度。因此，可以用一个旋转轴和一个旋转角进行刻画，其旋转方向为旋转轴的方向。因此，只使用一个向量即可进行描述，其方向与旋转轴一致，长度等于旋转角，这种向量称为旋转向量（或轴角 angle-axis），正好为三维：

$$\phi = \theta \mathbf{n}$$

其中 θ 表示旋转角度， \mathbf{n} 表示单位旋转向量。

罗德里格斯公式：旋转向量到旋转矩阵

$$\mathbf{R} = \cos \theta \mathbf{I} + (1 - \cos \theta) \mathbf{n} \mathbf{n}^T + \sin \theta \mathbf{n}^\wedge.$$

同样, 对于变换矩阵, 可用一个旋转向量和一个平移向量进行描述, 正好为六维。

旋转矩阵到旋转向量的转换:

$$\begin{aligned}\operatorname{tr}(\mathbf{R}) &= 3 \cos \theta + (1 - \cos \theta) \operatorname{tr}(\mathbf{n}\mathbf{n}^T) \\ &= 3 \cos \theta + (1 - \cos \theta) \|\mathbf{n}\|_2^2 \\ &= 3 \cos \theta + (1 - \cos \theta) \\ &= 1 + 2 \cos \theta\end{aligned}$$

从而 $\theta = \arccos \frac{\operatorname{tr}(\mathbf{R})-1}{2}$, 同时, 由 $\mathbf{R}\mathbf{n} = \mathbf{n}$ 可得:

$$(\mathbf{R} - \mathbf{I})\mathbf{n} = 0, \|\mathbf{n}\|_2 = 1$$

即通过旋转矩阵的迹求旋转角度, 通过旋转矩阵的特征值求单位旋转向量。轴角的表示也有奇异性, 比如转 30 度与转 390 度的轴角表示是一样的。

四元数

$$\begin{aligned}\mathbf{q} &= W + xi + yj + zk \\ S &= W \in \mathbb{R}, \mathbf{v} = (x, y, z)^T \in \mathbb{R}^3 \\ \mathbf{q} &= (s, x, y, z)^T = \begin{pmatrix} S \\ \mathbf{v} \end{pmatrix}\end{aligned}$$

对于 ijk 有:

$$\begin{cases} Ij = k, ji = -k \\ Jk = i, kj = -i \\ Ki = j, ik = -j \\ I^2 = -1, j^2 = -1, k^2 = -1 \end{cases}$$

对 $\mathbf{q} = (s, \mathbf{v}^T)^T$, 若 $s = 0$ 则称 \mathbf{q} 为虚四元数, 或纯虚四元数; 若 $\mathbf{V} = \mathbf{0}$, 则称 \mathbf{q} 为实四元数。令 $\mathbf{q}_a = (s_a, \mathbf{v}_a^T)^T, \mathbf{q}_b = (s_b, \mathbf{v}_b^T)^T$ 。

四元数的基本运算:

$$\text{加减法: } \mathbf{q}_a \pm \mathbf{q}_b = \begin{pmatrix} s_a \pm s_b \\ \mathbf{v}_a \pm \mathbf{v}_b \end{pmatrix}。$$

$$\text{乘法: } \mathbf{q}_a \mathbf{q}_b = \begin{pmatrix} s_a s_b - \mathbf{v}_a^T \mathbf{v}_b \\ s_a \mathbf{V}_b + s_b \mathbf{v}_a + \mathbf{V}_a \times \mathbf{V}_b \end{pmatrix}。$$

$$\text{模长: } \|\mathbf{q}\| = \|s\|, \|\mathbf{q}_a \mathbf{q}_b\| = \|\mathbf{q}_a\| \|\mathbf{q}_b\|。$$

数乘: $k\mathbf{q} = (ks, kv^T)^T$ 。

共轭: $\mathbf{q}^* = \begin{pmatrix} s \\ -\mathbf{v} \end{pmatrix}$, $\mathbf{q}\mathbf{q}^* = \mathbf{q}^*\mathbf{q} = (s^2 + \mathbf{v}^T\mathbf{v}, \mathbf{0})^T = \|\mathbf{q}\|^2 + 0i + 0j + 0k = \|\mathbf{q}\|^2$ 。

逆: $\mathbf{q}^{-1} = \frac{\mathbf{q}^*}{\|\mathbf{q}\|^2}$, $\mathbf{q}\mathbf{q}^{-1} = \mathbf{q}^{-1}\mathbf{q} = 1$ 。

若 $\|\mathbf{q}_a\| = \|\mathbf{q}_b\| = 1$, 则 $(\mathbf{q}_a\mathbf{q}_b)^{-1} = \mathbf{q}_b^{-1}\mathbf{q}_a^{-1}$ 。

单位四元数表示旋转: 单位四元数实际上具有三个自由度, 对应于三维空间中的旋转。

将三维空间中的点 $\mathbf{P}(x, y, z)$ 用虚四元数 $\mathbf{p} = (0, x, y, z)^T$ 表示, 以及一个由四元数 \mathbf{q} 指定的旋转, 则旋转后的点 \mathbf{p}' 可表示为:

$$\mathbf{p}' = \mathbf{q}\mathbf{p}\mathbf{q}^{-1}$$

上述乘法均为四元数乘法, 结果 \mathbf{p}' 也是虚四元数, 其虚部就是旋转后点的坐标。

任意单元四元数描述了一个旋转, 该旋转也可用旋转矩阵或旋转向量表示。

三维空间中, 从四元数到旋转矩阵的变换关系为:

$$\mathbf{R} = \mathbf{v}^T + s^2\mathbf{I} + 2s\mathbf{v}' + (\mathbf{v}^\wedge)^2$$

三维空间中, 绕单位向量 \mathbf{n} 逆时针旋转 θ , 对应于单位四元数 $\mathbf{q} = (\cos \frac{\theta}{2}, \mathbf{n}^T \sin \frac{\theta}{2})^T$ 。