免责声明

由于离散数学本质是一门数学~~（废话）~~，所以记公式的作用其实不是很大，而且很多时候公式的使用是看感觉的。。。当然，不记公式肯定是不行的，所以本文档主要用于查阅和宽泛的复习，很多细节和概念我也没涉及了

以及编辑的时候时间紧张加上能力有限，所以可能会有错误，如果发现请和我联系(19211332@bjtu.edu.cn)

命题逻辑

亿些细节

- 感叹句不是命题！无论它多像它就不是！
- 诸如“既。。。又。。。”、“虽然。。。但是。。。”、“不但。。。而且。。。”、“一面。。。一面。。。”的都是合取联结词
- 对于“除非q，否则非p”类的**有逻辑关系**的语句，可以考虑这么一句话在什么时候是假的

  举个例子：“除非我在做梦，否则我不会AKIOI”（~~这其实是一个梗~~），q:我在做梦，p:我AKIOI

  那么我们可以考虑一下上面这句话在什么情况下是错的呢？其实就是“我AKIOI但我不在做梦”，这个对应的是$p=1,q=0$，也就是只有$\begin{cases} p=1 \\ q=0 \end{cases}$的时候为假，所以$p,q$的关系是$p \to q$

  这种方法是我在离散期中之前想到的，在考场上第一次运用了，感觉效果还行233

  对于有的其他语句，也可以换成“只有 才 ”句式判断，这样只要记住“只有q才p”对应$p \to q$就行

等值式模式

公式名	内容
双重否定律	$\neg\neg A \Leftrightarrow A$
幂等律	$A \wedge A \Leftrightarrow A$ $A \vee A \Leftrightarrow A$
交换律	$A \wedge B \Leftrightarrow B \wedge A$ $A \vee B \Leftrightarrow B \vee A$
结合律	$(A \vee B) \vee C \Leftrightarrow A \vee (B \vee C)$ $(A \wedge B) \wedge C \Leftrightarrow A \wedge (B \wedge C)$
分配律	$A \wedge (B \vee C) \Leftrightarrow (A \wedge B) \vee (A \wedge C)$ $A \vee (B \wedge C) \Leftrightarrow (A \vee B) \wedge (A \vee C)$
德摩根律	$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$ $\neg(A \wedge B) \Leftrightarrow \neg A \vee \neg B$
吸收律	$A \vee (A \wedge B) \Leftrightarrow A$ $A \wedge (A \vee B) \Leftrightarrow A$ 吸收律可以使用分配律和同一律、零律结合着证
零律	$A \vee 1 \Leftrightarrow 1$ $A \wedge 0 \Leftrightarrow 0$ 零律的意义是变量没作用
同一律	$A \wedge 1 \Leftrightarrow A$ $A \vee 0 \Leftrightarrow A$ 同一律的意义是常量没作用
排中律	$A \vee \neg A \Leftrightarrow 1$
矛盾律	$A \wedge \neg A \Leftrightarrow 0$
蕴涵等值式	$A \to B \Leftrightarrow \neg A \vee B$
等价等值式	$A \leftrightarrow B \Leftrightarrow (A \to B) \wedge (B \to A)$
假言易位	$A \to B \Leftrightarrow \neg B \to \neg A$ 就是逆否命题
等价否定等值式	$A \leftrightarrow B \Leftrightarrow \neg A \leftrightarrow \neg B$
归谬论	$(A \to B) \wedge (A \to \neg B) \Leftrightarrow \neg A$ 如果一个命题可以同时得到相反的结论那么就是错的

一些补充的

- $\leftrightarrow$本质就是一个同或，可以用$A \leftrightarrow B \Leftrightarrow (\neg A \wedge \neg B) \vee (A \wedge B)$化简（不过不推荐）
- 吸收律的一种证明

$$
\begin{aligned}
A \vee (A \wedge B) &\Leftrightarrow (A \wedge 1) \vee (A \wedge B) \\
&\Leftrightarrow A \wedge (1 \vee B) \\
&\Leftrightarrow A
\end{aligned}
$$

优先级

$() > \neg > \wedge > \vee > \rightarrow > \leftrightarrow$

~~U1S1，用容易混淆优先级的运算符而不打括号的都是baka~~

范式

范式名称	项的名称	项的符号	项取值	项之间的联结关系
主析取范式	极小项	m_i	成真赋值	析取
主合取范式	极大项	M_i	成假赋值	合取

举个例子说明m_i和M_i是怎么取值的：

如果两个变量$b_1 b_0$的公式f在01、10下为真，其他为假，那么：$i = (01)_2, (10)_2$时$f = 1$，所以f的主析取范式包括m_1、m_2；$i = (00)_2, (11)_2$时$f = 0$，所以f的主合取范式包括M_0、M_3。化简之后只需要写出所有取1/取0的就行，即$f = \prod(M_0, M_3) = \sum(m_1, m_2)$

也就是$m_i = 1$表示的是取值为$(i)_2$时公式为真，M_i表示的是取值为$(i)_2$时公式为假

（感觉上面讲得不好。。。觉得多做几道题就能理解了看文字反而不好理解）

一些规律

- 两个范式可以互换

  $\prod_{j \in J}(M_j) = \sum_{i \in I}(m_i)$，$I$和$J$之间的元素互补，比如对于两个变量$I = \{1, 2\}$那么$J = \{0, 3\}$

  这个公式可以用来化简一些运算
- 极大项和极小项之间本身可以互换

  $\neg m_i \Leftrightarrow M_i$，因为$m_i$和$M_i$两个针对的是一个取值$(i)_2$的真/假，所以两个一定是互反的
- 主合取范式没有项用1表示

  主析取范式没有项用0表示

联结词完备集概念

定义：设S是一个联结词集合，如果任何的n元真值函数都可以由仅含S中的联结词构成的公式组成，那么S是联结词完备集

另外，n元函数的真值表有2^{2^n}种，也就是n元函数本质不同的有2^{2^n}种

与非$p \uparrow q \Leftrightarrow \neg(p \wedge q)$；或非$p \downarrow q \Leftrightarrow \neg(p \vee q)$

证明一个集合是完备的可以使用等价的方式，即如果想要证明S是完备的，已知S'是完备的，可以通过证明S的每一个符号都可以通过S'里面的符号**等价**来证

比如$S=\{\uparrow\}$，$S'=\{\neg,\wedge\}$，那么$\neg p \Leftrightarrow \neg(p \wedge p) \Leftrightarrow p \uparrow p$，
$p \wedge q \Leftrightarrow \neg\neg(p \wedge q) \Leftrightarrow \neg(p \uparrow q) \Leftrightarrow (p \uparrow q) \uparrow (p \uparrow q)$

命题的推理

推理的定义等

$A_1, A_2, \cdots, A_k$推出B的推理正确当且仅当$\{A_1, A_2, \cdots A_k\} \rightarrow B$重言

另外

- $\{A_1, A_2, \cdots A_k\} \rightarrow B$和$\{A_1, A_2, \cdots A_k\} \rightarrow B$等同
- $\{A_1, A_2, \cdots A_k\} \Rightarrow B$和$\{A_1, A_2, \cdots A_k\} \models B$等同

推理的方式

如果想要证明$\Gamma \models B$方法有三：

- 运用**等价**运算证明$\Gamma \rightarrow B$是重言的
- 运用推理定律一步步推：$\Gamma \Rightarrow \cdots \Rightarrow B$
- 运用自然推理系统

实际上第二种是第三种的特例，而第一种本质是第一章的内容，所以这里主要介绍第三种

推理定律

有一些推理定律，在证明的时候会被经常用到

公式里面会附上一些个人的理解用于记忆

名字	公式
附加律	$A \Rightarrow A \vee B$ 顾名思义就是附加式子
化简律	$(A \wedge B) \Rightarrow A$ 顾名思义就是化简式子
假言推理	$(A \rightarrow B) \wedge A \Rightarrow B$ 是我们日常使用的一种推理方式
拒取式	$(A \rightarrow B) \wedge \neg B \Rightarrow \neg A$ A能推出B但是B是假的所以A是假的
析取三段论	$(A \vee B) \wedge \neg B \Rightarrow A$ A或B真，现在B假所以A真
假言三段论	$(A \rightarrow B) \wedge (B \rightarrow C) \Rightarrow (A \rightarrow C)$ A能推出B，B能推出C，所以A能推出C
等价三段论	$(A \leftrightarrow B) \wedge (B \leftrightarrow C) \Rightarrow (A \leftrightarrow C)$ A与B等价，B与C等价，所以A与C等价
构造性两难	$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (A \vee C) \Rightarrow (B \vee D)$ A能推出B，C能推出D， A或C正确，那么B或D正确
构造性两难 （特殊形式）	$(A \rightarrow B) \wedge (\neg A \rightarrow B) \Rightarrow B$ 无论如何都可以推出B，那么B就是对的
破坏性两难	$(A \rightarrow B) \wedge (C \rightarrow D) \wedge (\neg B \vee \neg D) \Rightarrow (\neg A \vee \neg C)$ A能推出B，C能推出D，B或D错误，那么A或C错误
破坏性两难 （自创特殊形式）	$(A \rightarrow B) \wedge (C \rightarrow B) \wedge \neg B \Rightarrow (\neg A \vee \neg C)$

最后一个会在有的题里面遇到，但是本质上其实就是两难，所以也没必要记住

自然推理系统推理方式

这里总结了证明过程中会用到的一些规则（也就是做题的时候右边写的东西）

- 前提引入：在引入前提的时候使用
- 合取引入规则：可以看作一种推理定律，即$A \wedge B \Rightarrow A \wedge B$
- 推理定律使用：$T < i > < j > XXX$表示这一步是通过$< i >$和$< j >$通过XXX规则（包括合取引入）/定律/等价（如果不知道的话XXX直接写成“置换”即可）得到的
- 结论引入：任何结论都可以在后面作为前提引入，一般不说明，在使用推理定律的时候默认使用
- 附加前提引入：一般用在附加前提证明法，如果结论需要证明$p \rightarrow q$，那么可以通过“将p作为前提引入证明q”的方式完成证明
- 结论的否定引入：一般用在归谬法，这样需要最后得到一个矛盾式，且一般是得到的某个式子和结

论的合取

一阶逻辑

一阶逻辑命题符号化

由于这里的定义对后面的理解比较重要，所以特别提一下

一些定义：

- 个体词

  表示具体/特定的称为个体常项，一般用$a, b, c...$表示

  表示泛指的称为个体变项，一般用$x, y, z...$表示

  个体域（或者论域）表示个体变项的取值范围

  全总个体域指宇宙间一切事物，如果不特殊说明个体域那么就是全总个体域
- 谓词

  确定的关系的是谓词常项

  抽象的或者泛指的关系称为谓词变项

  n元谓词表示谓词里面个体变项的数量是n。0元谓词就是命题

有（**且这门课上仅有**）两个量词：全称量词$\forall$、存在量词$\exists$，意义高中学过

在讨论的时候有时候需要限制量词的范围，比如谓语$M(x)$表示x有M的性质（比如“x是人”），$F(x)$是一个需要被判断的谓词（比如“x使用左手写字”），那么“存在/所有人使用左手写字”可以转成下面形式：

- 可以在整体的论域上限制”所有人类“，然后直接写$\exists xF(x)$、$\forall xF(x)$即可
- 如果不想限制整体论域的话，那么可以写

  $\exists x[M(x) \wedge F(x)]$、$\forall x[M(x) \rightarrow F(x)]$

  这里一定要注意不要写错了形式！

一阶逻辑命题的解释

先给一阶语言$\mathscr{L}$做个说明

$\mathscr{L}$中项指：个体常项/变项、公式中的项被个体常项和变项填充后的式子、前两者有限次复合得到的式子

公式包括了项和谓词，并且经过一些逻辑符号、量词的复合

变元和辖域：在公式$\forall xF(x)$、$\exists xF(x)$中，称x为指导变元，F为量词的辖域，在辖域下的所有x都称为约束出现，其他的x都称为自由出现。注意对于$x \vee \forall xF(x)$，两个出现的x的意义是不同的，解释的时候就需要特别注意

解释：

可以看作对公式里的东西的赋值。解释需要处理：

- 个体域，每一个解释都应当限制了（总）个体域D_I
- 个体常项，每一个个体常项α一定被赋予了意义$\overline{\alpha}$
- 函数，每一个函数f一定被赋予了定义$\overline{f}$
- 谓语，每一个谓语F一定被赋予了含义$\overline{F}$
- 自由出现的个体变项，同一个自由出现的个体变项x都应该被替换成$\sigma(x)$

另外，约束出现的变项一定不能被指定，自由出现的变项一定要被指定

代换实例：

定义：设A_0是含命题变项$p_1, p_2, \cdots, p_n$的命题公式，$A_1, A_2, \cdots, A_n$是n个谓词公式，用A_i代替A_0中的p_i得到的公式称为A_0的代换实例。使用代换实例可以化简一些式子，例如重言式的代换实例都是重言式、矛盾式的代换实例都是矛盾式

一阶逻辑等值式和置换规则

代换实例规则

（名字是自己取的）

重言式的代换实例都是重言式、矛盾式的代换实例都是矛盾式

注意，**可满足式的代换实例不一定是可满足式！**

量词否定等值

$\neg\exists xF \Leftrightarrow \forall x\neg F$、$\neg\forall xF \Leftrightarrow \exists x\neg F$

辖域扩张等值

下面G表示G内没有x出现

$\forall x[F(x) \vee G] \Leftrightarrow \forall xF(x) \vee G$

$\forall x[F(x) \wedge G] \Leftrightarrow \forall xF(x) \wedge G$

$\forall x[F(x) \to G] \Leftrightarrow \exists xF(x) \to G$

$\forall x[G \to F(x)] \Leftrightarrow G \to \forall xF(x)$

$\exists x[F(x) \vee G] \Leftrightarrow \exists x F(x) \vee G$

$\exists x[F(x) \wedge G] \Leftrightarrow \exists x F(x) \wedge G$

$\exists x[F(x) \rightarrow G] \Leftrightarrow \forall x F(x) \rightarrow G$

$\exists x[G \rightarrow F(x)] \Leftrightarrow G \rightarrow \exists x F(x)$

也就是对于辖域扩张/收缩的情况，只有$F(x)$出现在$\rightarrow$左端时需要变号

量词分配等值

名字记住

$\forall x[A(x) \wedge B(x)] \Leftrightarrow \forall x A(x) \wedge \forall x B(x)$

$\exists x[A(x) \vee B(x)] \Leftrightarrow \exists x A(x) \vee \exists x B(x)$

可以使用自然语言理解，也可以从有限个体域下的量词消去规则去理解

注意只有 $\forall$对应$\wedge$ 和 $\exists$对应$\vee$ 这两个，其他的类似形式的式子是不可逆的

换名规则和代替规则

本质都是取别名，换名规则是换约束出现的变项，代替规则是换自由变项

前束范式

将公式中的全部量词提前到前面就是前束范式，前束范式是一定存在的

有限域的量词消去

对于有限域$\Gamma=\{x_1, x_2, \cdots, x_n\}$，$\exists x A(x) \Leftrightarrow A(x_1) \vee A(x_2) \vee \cdots \vee A(x_n)$，$\forall x A(x) \Leftrightarrow A(x_1) \wedge A(x_2) \wedge \cdots \wedge A(x_n)$

相同量词的交换

$\forall x \forall y F(x, y) \Leftrightarrow \forall y \forall x F(x, y)$

$\exists x \exists y F(x, y) \Leftrightarrow \exists y \exists x F(x, y)$

一阶逻辑推理

除了上面的等值之外还有一些工具：

推理定律

$\forall x A(x) \vee \forall x B(x) \Rightarrow \forall x[A(x) \vee B(x)]$

$\exists x[A(x) \wedge B(x)] \Rightarrow \exists x A(x) \wedge \exists x B(x)$

$\forall x[A(x) \rightarrow B(x)] \Rightarrow \forall x A(x) \rightarrow \forall x B(x)$

$\forall x[A(x) \rightarrow B(x)] \Rightarrow \exists x A(x) \rightarrow \exists x B(x)$

注意这里的公式内部和外部的符号，比较容易错

量词操作

- US($\forall-$)：全称量词消去，比如$\forall x F(x)$推理出：$F(y)$或$F(c)$
- UG($\forall+$)：全称量词引入，比如$A(y)$（注意这里一定要需要保证y是可以**任意取值**的自由变量）推出$\forall x A(x)$
- ES($\exists-$)：存在量词消去，比如$\exists x A(x)$推理出$A(c)$，注意这里c被限制成了“特定的满足A的个体常项”，不是任意的量，所以不能再在US上使用c
- EG($\exists+$)：存在量词引入，比如$A(c)$可以推出$\exists x A(x)$，原则上需要c是一个个体常项