《面向计算机科学的离散数学补充资料》

普遍有效性和可满足性

黄民烈　aihuang@tsinghua.edu.cn

清华大学计算机系

K 个体域：指元素个数为 k 的个体域；

K 可满足/普遍有效：在 k 个元素的个体域上可满足/普遍有效。

定理 1　公式在一个个体域中可满足性和普遍有效性依赖于其中的个体域的个数

举例说明：

（a）可满足性

1）在(k)个体域上可满足，但不在(k-1)个体域上可满足

$$\mathrm{k}=2: \exists x P(x) \wedge \exists x \neg P(x)$$

$$\mathrm{k}=3: \exists x P(x) \wedge \exists x\left(\neg P(x) \wedge G(x)\right) \wedge \exists x\left(\neg P(x) \wedge \neg G(x)\right)$$

$$\begin{aligned} k=4: & \exists x P(x) \wedge \exists x\left(\neg P(x) \wedge G(x)\right) \wedge \\ & \exists x\left(\neg P(x) \wedge \neg G(x) \wedge R(x)\right) \wedge \\ & \exists x\left(\neg P(x) \wedge \neg G(x) \wedge \neg R(x)\right) \end{aligned}$$

2）在无穷个体域中可满足，但不在有穷个体域中可满足

$$\forall x \neg R(x,x) \wedge \forall x\, \forall y \forall z \left(\mathrm{R(x,y)} \wedge R(y,z) \to R(x,z)\right) \wedge$$
$$\left(\forall x \exists y R(x,y)\right)$$

其中 R 表示<关系(**偏序**)。在(0,1) 这样的集合上可满足；在(0,1] 这样的集合上不可满足（在 x=1 的时候）；在{1,2,3}有限集合上不可满足。

（b）普遍有效性

1）在任何一个不空的个体域中：

$$\forall x \mathrm{P(x)} \to \exists y P(y)$$

2）在 k 个体域上普遍有效，但不在 k+1 个体域中普遍有效

$$\mathrm{k}=1: \forall x P(x) \vee \forall x \neg P(x)$$
$$\mathrm{k}=2: \forall x P(x) \vee \forall x\left(\neg P(x) \vee G(x)\right) \vee \forall x\left(\neg P(x) \vee \neg G(x)\right)$$
$$k=3: \forall x P(x) \vee \forall x\left(\neg P(x) \vee G(x)\right) \vee$$
$$\forall x\left(\neg P(x) \vee \neg G(x) \vee R(x)\right) \vee$$
$$\forall x\left(\neg P(x) \vee \neg G(x) \vee \neg R(x)\right)$$

3）在有穷个体域中普遍有效但在无穷个体域中不普遍有效

$$\left(\forall x\, \exists y R(x,y) \wedge \forall x\, \forall y \forall z \left(\mathrm{R(x,y)} \wedge R(y,z)\right) \to R(x,z)\right)$$
$$\to \exists x R(x,x)$$

同样的这个公式，在有穷个体域，传递关系,且任意 x 都存在 y 满足 R(x,y)，则关系必然存在 x 满足 R(x,x)。例如两个元素的个体域{a，b}，满足关系 R 的集合可以是{<a,b>,<b,b>}。

但在无穷集合上，传递关系,且任意 x 都存在 y 满足 R(x,y)却无法推导出来存在 x 满足满足 R(x,x)。例如实数集合 R、(0,1)，可以定义严格的<关系(偏序)。

定理 2　一个公式在一个个体域中是可满足或普遍有效的，那么在个体数相同的个体域中也是可满足或普遍有效的。

说明：

1. 假设 D 和D'为两个个体数目相同的个体域。则D和D'之间可以建立一一对应的关系。即，D中的元素x可以对应D'中唯一的x'。
2. 设 $a=\{x_1,x_2,\ldots,x_n\}$ 为 D 的任一子集，则在 D' 中存在唯一对应 $a'=\{x_1',x_2',\ldots,x_n'\}$。
3. 假设D中任意谓词$P(x_1,x_2,\ldots,x_n)$,则在D'存在对应的谓词：

   $P'(x_1',x_2',\ldots,x_n')$，并且

   $$P(x_1,x_2,\ldots,x_n)\leftrightarrow P'(x_1',x_2',\ldots,x_n')$$
4. 任何公式$A(x_1,x_2,x_3,\ldots,x_n)$其中有任一谓词公式 $P(x_{i1},x_{i2},\ldots,x_{im})$ 在另一个体域上公式 A 变成$A(x_1',x_2',\ldots,x_n')$，对应的构造谓词公式$P'(x_{i1}',x_{i2}',\ldots,x_{im}')$，只要在$x_1,x_2,\ldots,x_n$的某个解释下的$P(x_{i1},x_{i2},\ldots,x_{im})$的真值与$x_1',x_2',\ldots,x_n'$的对应解释下$P'(x_{i1}',x_{i2}',\ldots,x_{im}')$的真值相同即可。
5. 因此，若P可以作为某个公式在D中的解释，则P'也可以作为该公式在D'的解释。反之亦然。
6. 如果原公式是普遍有效的，那么新公式也是普遍有效的。
7. 因此，任意公式在两个个体域中的可满足性和普遍有效性是相同的。

严格证明需要采用数学归纳法，施归纳于逻辑连接词和量词的数目。

注意：公式 A 可能由 P、Q、R 这样的子公式构成，每个子公式对应的个体子集是不同的。

定理 3 公式 A 为 k 普遍有效，则¬A为 k 不可满足。反之亦然。

定理 4 假设公式 A 为 k 可满足，则 A 是 k+1 可满足。

证明：

假设A在k个体域 $D=\{x_1,x_2,\ldots,x_k\}$ 中可满足，而$D'=\{x_1',x_2',\ldots,x_{k+1}'\}$ 为$k+1$个体域，D'' 为D'的任一k个个体的子集（即任意去掉一个元素即可）。

1. 根据定理 2，我们可以在D和D''中建立一一对应关系，即D中任何一个个体x_i对应D''中x_i' 。
2. 进行如下构造：先给定D中一个a_1，对于D'中任意元素

   即若x'在D''中，则x'对应D中的某个且唯一一个x；否则，对应到D中元素a_1。
3. 则对D中任何谓词公式$P(y_1,y_2,\ldots,y_n)$，可以按照此方法构造D'的对应谓词公式，使得

   $$P(y_1,y_2,\ldots,y_n)\leftrightarrow P'(y_1',y_2',\ldots,y_n')$$

   其中每一个x_i'都可以对应到D上的一个元素。
4. 因为A在D上可满足，所以存在系列的个体域子集$A_1,A_2,\ldots,A_m$，以及$P_1,P_2,\ldots,P_m$，使得A为真。自然地，在D'也存在这样的$A_1',A_2',\ldots,A_m'$，以及$P_1',P_2',\ldots,P_m'$使得A为真。

定理 4 假设公式 A 为 k 普遍有效，则 A 是 k-1 普遍有效(K>1)。

证明：为前述定理的对偶定理

1. $\neg\mathbf{A}$为$k-1$可满足，则$\neg\mathbf{A}$公式k可满足；(定理 4)
2. $\neg\mathbf{A}$公式k不可满足，则$\neg\mathbf{A}$公式$k-1$不可满足；(逆否定理)
3. $\mathbf{A}$公式k普遍有效，则$\mathbf{A}$公式$k-1$普遍有效。(定理 3)