网络与信息安全概论（4） —— 习题与思考题

**2. 通过重写规则一步一步证明： 可以转换为法式。**

证明：

**…** (1)

**…** (2)

**…** (\*)

证毕，对原式依次进行R2（1次）、R3（1次）和R4（1次），即可得法式(\*)。

**3. 设 ，，将简约为法式。**

解：

**…** (1)

**…** (2)

**…** (3)

对原式依次进行R2（1次）、R3（1次）和R4（1次），得到(3)式，(3)不存在违规二元组，所以(3)为原式的法式。其中 。

4. **设 ，，将简约为法式。**

解：

原式中存在与，违反NF2，所以为半法式。

1. 首先使用重写规则，对中的进行改写：

（R2）

（R3）

（R3）

（R4）

**…** (\*)

对于改写后的式子(\*)，依旧存在与，其下标分别为。所以最大违规二元组(a , b)=(1,4)。

1. 对(\*)中的使用3次R1，使用3次R4，最后对与使用一次R5：

（R1, R4）

（R1, R4）

（R1, R4）

（R5）

这里。

**5. （思考题）为什么与不是不变子群距离函数？**

解：不变子群距离函数应该有以下三个性质：

1. 有效性，;
2. 非平凡性，;
3. 不变性，

令，且有：

；

；

则*w*是的法式形式，。令，

此时， 。因为对于元素，其中 的值发生变化，即元素均向右移动1位，使原来刚好满足的等式，由于下标k的增大（+1），而等式右边结果变小(值由原先s - 1变成s)，不再满足子群距离函数的条件。

所以有：

即不为不变子群距离函数，同理可证同样不为不变子群距离函数。同样，可以用举反例证明。

**6. （思考题）证明：根据二元组的最大性，通过下标的移动可以由子字*c*得到不含违规二元组的子字*d*。**

证明：，*(a, b)*为*w*最大违规二元组。

对而言，需要进行次R1规则重写，每一次均有：

对而言，需要进行次R4规则重写，每一次均有：

即应用R1，a字母不会改变，同a字母交换的则会减1；应用R4，b字母不会改变，同b字母交换的则会加1。小于a大于b的元素则不发生变化，只有[a, b]之间的字母形成的字才会发生变化，即子字c发生变化。当分别在下标为r和s处相遇时，使用R5规则重写，即可获得关于w的法式。

**7. （思考题）证明【引理 1】中的最后部分：*，，，*。**

证明：对于*w*，左乘，得：

当时，对上式应有m-1次R1重写规则，此时有：

…(1)

(1)式最终要将现向右移动一位，即需要再使用一次R1重写规则，根据R1重写规则：。所以对应于(1)，会有如下变化：

, …(2)

(2)式即为法式，无法再使用R1对t进行重写，过程中有： t + m – 1> im，t + m < im+1，证毕。同理，对于*，，*只需将上述和步骤中的重写规则由R1变成R4，并重复步骤即可得到结论。

1. 最终代码由于行数较多，作业附件中会由一份java文件，文件内有相关的代码注释易于理解。