中山大学2021年研究生期末考试《计算复杂性》答案

**一、填空题**

1、1965、Hartmanis、Stearns、On the computational complexity of algorithms。

2、一致性模型、非一致性模型、图灵机、电路。

3、BPP：

RP：

coRP：给定一对深度为d的电路（C1,C2），电路的基域中元素个数多于2d+1，判定这两个电路是否能计算同一个多项式。

4、NP=PCP(log,O(1))。

5、对任意限定空间构造的至少为对数的函数，有。

**二、判断正误，正确的打√并给出证明，错误的打×并举出反例。**

1、（√）；

任意的NL问题可以归约到coNN问题，而coNN问题又属于P问题，所以NL属于P问题。

2、（×）只要x2与x1取相同赋值即可满足。

3、（√）设是单向函数，则已知y求x使得f(x)=y是困难的，但是验证给定x求是否有f(x)=y是高效的。

4、（√）我们先把3SAT问题归约到3次方程组，再把3次方程组归约到2次方程组。

假设3SAT问题有n个变量，m个子句，每个子句写成一个3次方程，例如(x1x2x4)可写为(1-x1)x2(1-x4)=0，则3SAT问题归约到n元3次方程组求解问题。对于上述3次方程，我们引入辅助变量t= x2(1-x4)，则该3次方程就变为(1-x1)t=0和t= x2(1-x4)，同理，对于3次方程组的其他方程也可如此处理，这样，3次方程组就变为了2次方程组。综上，F2上的多元2次方程组和3次方程组求解问题都是NPC问题。

5、（×）2-CNF-SAT是P问题

**三、名词解释**

1、P/poly：称函数f在多项式时间内利用长度为l:N→N的建议可解，如果存在一个多项式时间算法A和一个无限长的建议序列，满足以下条件。

（1）对任意，有。

（2）对任意，有。

2、Church-Turing论题：采用图灵机模型并不会损失什么：一个函数可以用图灵机计算当且仅当它可以用任意其他“合理且通用”的计算模型计算。

3、Levin归约：一对多项式时间计算的映射f和g称为R到的Levin归约，如果f是到的Karp归约，并且对任意的和，有，其中。

4、PH：对于给定正整数k和判定问题S，如果存在多项式p及多项式时间算法V，使得当且仅当

满足

则称判定问题S属于类。其中k为奇数时，是存在量词，否则，为全称量词。

多项式时间层级，记作PH，定义为所有上诉类的并集，即。

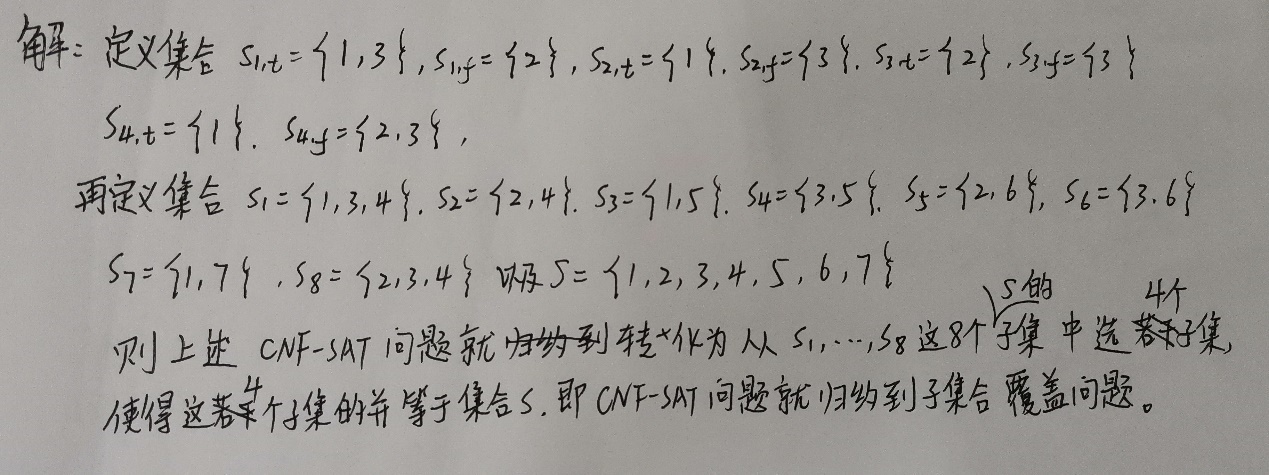
5、核心断言：一个多项式时间可计算的谓词称为函数f的困难核心，如果对任意概率多项式时间算法，任意正多项式p(.)以及所有足够大的n，有

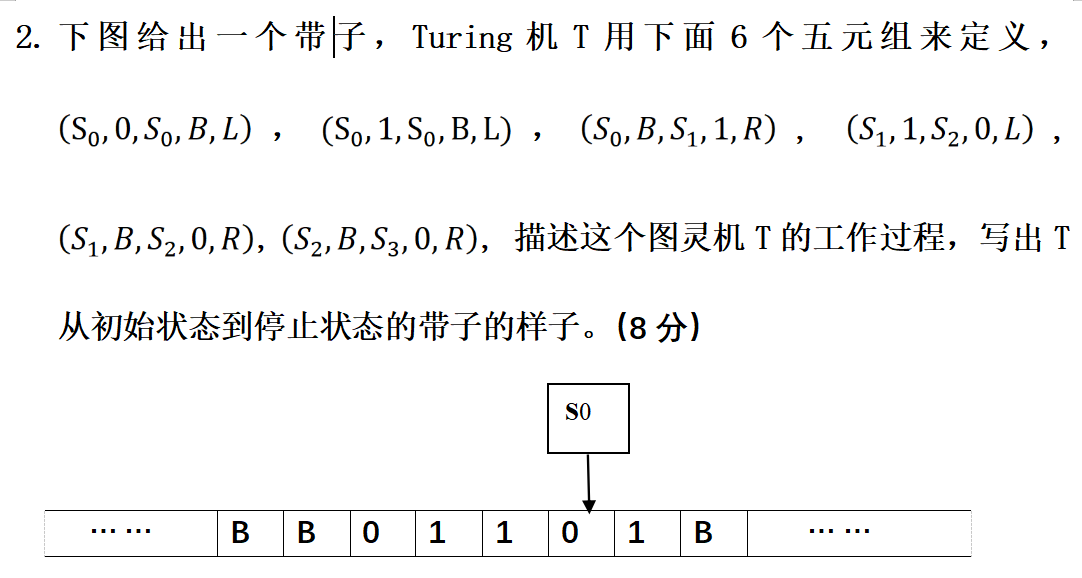
其中概率空间是随机均匀选择的所有以及算法所有可能的内部随机数。

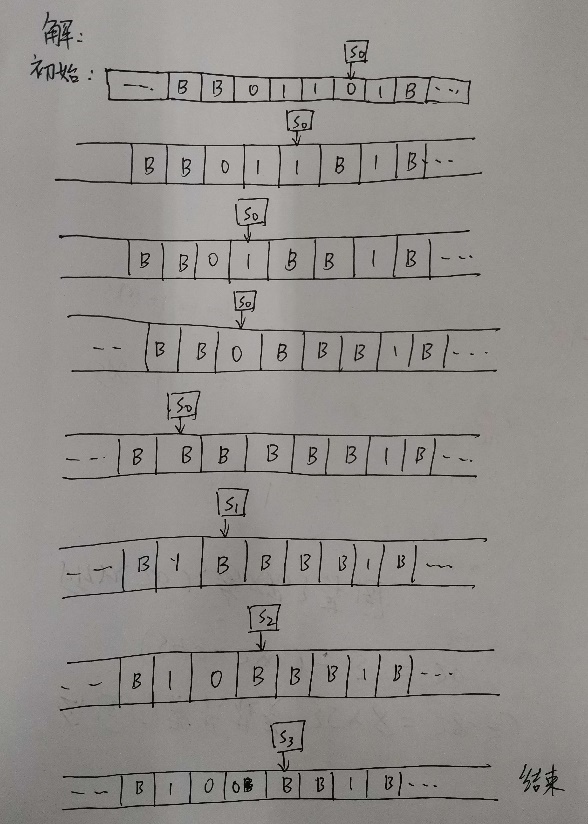
**四、解答题（25分）**

1. 将下面布尔函数的CNF-SAT问题规约到子集合覆盖问题。（9分）

Φ(x1, x2, x3, x4)= (x1x2x4)  (x1x3x4)  (x1x2x3x4)







1. RSA问题是指：给定两个大素数的乘积n和一个加密指数e以及0<y<n,计算x<n，使得 xe=y mod n。如果你知道x是RSA问题(n, e, y)的一个解，请给出x的一个交互式零知识证明协议，并分析你给出的协议的完备性（Completeness）、健壮性（Soundness）和零知识性（Zero-knowledge）。（8分）

