离散空间上的
容错搜索理论

刘文安 著

科学出版社
www.sciencep.com

离散空间上的容错搜索理论

刘文安　著

科　学　出　版　社

北　京

内 容 简 介

离散空间上的容错搜索理论是一门新兴的交叉学科，它涵盖数学、通信、计算机等学科，有着重要的理论价值和广泛的应用前景. 全书分为 8 章. 第 1 章着重给出模型的分类及其研究现状；第 2 章展示寻找单目标 2 维自由提问格式模型的最优算法的方法；第 3 章阐述单目标 q 维自由提问格式模型的最优算法与数学工具；第 4 章将容错搜索方法应用到 Coin-Weighing 模型；第 5 章引入“大小受限”提问格式模型并研究其最优算法；第 6 章分析寻找单目标 q 维双区间型提问格式模型的最优算法的必要性和可能性；第 7 章和第 8 章分别介绍其他学者新近提出的“具有时滞和遗失的模型”与“对偶模型”，初步分析研究这两类模型的方法与手段. 附录给出了必备的一些基础知识.

本书可作为高等院校高年级本科生、研究生的教材或参考书,也可作为数学、通信、计算机等领域研究人员的参考书.

图书在版编目（CIP）数据

离散空间上的容错搜索理论/刘文安著. —北京：科学出版社，2007
ISBN 978-7-03-019407-7

Ⅰ.离… Ⅱ.刘… Ⅲ.①容错技术②搜索论 Ⅳ.O229 TP302.8

中国版本图书馆 CIP 数据核字（2007）第 108980 号

责任编辑：赵彦超 杨 然 / 责任校对：陈玉凤
责任印制：赵德静 / 封面设计：王 浩

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

双 青 印 刷 厂 印刷

科学出版社发行 各地新华书店经销

*

2007 年 8 月第 一 版 开本：B5(720×1000)
2007 年 8 月第一次印刷 印张：15 1/4
印数：1—3 000 字数：285 000

定价：38.00 元

前　言

搜索论是第二次世界大战中同盟国研究如何对轴心国的潜艇活动、舰队运输和兵力部署等进行甄别的过程中产生的运筹学分支. 搜索论主要是研究在资源和探测手段受到限制的情况下, 如何设计寻找某种目标的最优方案并加以实施的理论和方法. 搜索论在实际应用中也取得了不少成效, 例如20世纪60年代, 美国寻找在大西洋失踪的核潜艇“打谷者号”和“蝎子号”以及在地中海丢失的氢弹, 都是依据搜索论获得成功的.

1956年, Koopman教授的3篇创造性的论文[1~3]奠定了搜索论的基石. 正如1982年Morse[4]在怀念Koopman教授时所说的那样,“搜索论之所以能迅速地发展成为一门既相对独立又与众多学科密切相关的学科, 是因为Koopman教授没有把它局限于某种或某几种固定的方法, 而是让它奠基在少量的定义性的原理和准则上”. 因此，人们能够不断地尝试借用其他众多领域的思想、方法和技巧来解决所面临的实际问题. 这一本质决定了搜索论必然是内容丰富、成果众多且极具应用价值的领域. 正如Knuth在其个人文集《计算机程序的艺术》第三卷(主要介绍了搜索和排序算法)的引言中所说:“事实上, 我坚信程序的每一个重要方面无不包含着搜索与排序.” 是否每一个科学问题都能转化为一个搜索问题属于哲学所讨论的范畴, 然而，不容置疑的是，许多很重要的实际问题都可以转化为搜索问题. 因此, 搜索论在军事领域、空间科学与技术、信息科学、计算机科学、医药、生物学、探矿和渔业等领域都有广泛的应用[5~7].

从过去的铅笔直尺到现在的大型计算机, 从过去的肉眼观测到今天的卫星探测、遥感定位, 搜索工具和搜索方法的不断更新都对搜索论的发展起到了巨大的推动作用. 不但原有的一些搜索方法得到了显著的改进, 而且与其他学科交叉所出现的新型搜索问题也都被科学工作者们所关注.

搜索论按搜索域的性质可分为两大类：离散空间上的搜索和连续空间上的搜索. 在过去的几十年里, 它们都有很大发展. 但是，较之连续空间上的搜索问题, 离散空间上的搜索问题的研究似乎有些滞后. 正如Chudnovsky[8]指出的,“尽管搜索论已得到长足的发展, 不幸的是众多的理论研究都是针对连续模型进行的, 而对于同样具有应用价值的离散模型则知之甚少. 这或许是由于相关的研究工具

缺乏或不完善而造成的.” 因此，离散空间上的搜索问题是一个极具研究价值的课题，而离散空间上容错搜索问题的研究则更加意义重大.

“容错”概念的实质是依据未必可靠的信息来建立可靠的结果，即“不可靠的信息、可靠的计算”(unreliable information and reliable computation). 容错理论和技术的产生和发展与人们对可靠结果的追求是密不可分的，特别是在计算机与通信领域. 当人们感觉到不大可能单纯地依靠提高物理元器件的性能来提高计算结果的可靠性时，便开始考虑从信息本身和处理信息的方法入手来提高计算结果的可靠性，这就导致了容错理论和技术的产生和发展. 正如前面所说的那样，许多问题都可以转换为搜索问题，所以容错理论和技术很快就被应用到了搜索问题上，形成了一个崭新的领域——“容错搜索”. 因此，容错搜索可以认为是搜索论的新发展，也可以认为是容错理论的新应用.

我首次接触这类问题是在 1987 年. 经李蔚萱教授和沙基昌教授之手，我有幸看到黄光明教授的一篇论文，立即被论文所提出的问题吸引，后来的硕士毕业论文和博士毕业论文都是针对这一领域来进行的. 素未见面但又保持密切联系的 Pelc 教授引领我进入“离散空间上的容错搜索理论”这一崭新的领域. Pelc 教授不仅提供了大量的文献，而且介绍我认识三位博士并得到他们的博士论文[9~11].

本书的第一稿形成于 2004 年 5 月. 在为三届硕士研究生授课的基础上，经过不断修改、完善形成现在的书稿. 目前，离散空间上的容错搜索理论的框架体系尚未形成，研究内容和方法尚处于不断探索、逐步完善阶段，提出的问题远远多于已解决的问题. 本书的目的在于向读者介绍离散空间上容错搜索理论的研究背景、内容与方法，激发读者从事这一领域科学研究的热情. 全书分为 8 章. 第 1 章着重给出模型的分类以及研究现状；第 2 章展示寻找单目标 2 维自由提问格式模型的最优算法的方法；第 3 章阐述单目标 q 维自由提问格式模型的最优算法与数学工具，将第 2 章的内容推广到一般情况；第 4 章将容错搜索方法应用到 Coin-Weighing 模型；第 5 章引入更加实用的“大小受限”提问格式模型并研究其最优算法；第 6 章探讨寻找单目标 q 维双区间型提问格式模型的最优算法的可能性；第 7 章和第 8 章分别介绍了其他学者新近提出的“具有时滞和遗失的模型”与“对偶模型”，初步分析了研究这两类模型的方法与手段. 为方便读者阅读，在附录给出了必备的一些基础知识.

全书在叙述上力求深入浅出，尽量避免高深的数学知识，因此，我们对许多结果的原始证明进行了加工，以更简捷的方法重新予以证明. 书中不少内容是作

者近几年在离散空间上的容错搜索理论方面的研究成果.

感谢堵丁柱教授的指导和帮助，他不仅提供了多篇文献[12]，而且对作者写作本书进行了精心的指导. 感谢西安交通大学聂赞坎教授、徐宗本教授、徐寅峰教授的良好建议，感谢国防科技大学沙基昌教授、南开大学颜华菲教授等的关心与支持，感谢孟坤、邢淑敏和张雪丽同学为本书打印、校对所付出的辛劳，同时也对参考文献的所有作者表示衷心谢意.

本书的完成得到了国家自然科学基金(10571045)、河南省杰出青年科学基金(074100510024)、河南省教育厅自然科学基金(2007110018)等项目的资助，在此表示衷心感谢.

由于作者水平有限，书中难免会有不妥与错误之处，诚望专家学者批评指正!

刘文安

2007 年 4 月

目　录

第 1 章　离散空间上的容错搜索模型及其分类

§1.1　Rényi-Ulam 问题与纠错编码

§1.1.1　Rényi-Ulam 问题

Rényi[13],Ulam[14] 先后提出如下两个问题:

A 和 B 两人进行如下游戏: A 想了一件事, B 通过一系列提问设法猜出它. 对于 B 所提的每一个问题, A 仅以“是”或“否”作答, 并且允许 A 所给出的回答中固定比例是错误的. 试确定 B 能够正确猜出 A 所想的事情的最少提问次数.

一个人在 1 到 1000000 之间想了一个数 ($1000000 < 2^{20}$), 另一个人最多允许提问 20 个问题. 对于提问者每个问题, 假定回答者只以“是”或“否”作答. 假如提问者第一次这样问:“这个数在 1 到 500000 之间吗?”, 如果回答者回答“是”, 那么提问者第二次这样问:“这个数在 1 到 250000 之间吗?”, 否则提问“这个数在 250001 到 750000 之间吗?”, 以后就按这样的方法问下去. 显然, 提问者至多用 $\log_2 1000000$ 次提问就能够确定出这个数. 现在, 如果回答者被允许说谎一次或者两次, 那么提问者至少需要多少次提问才能确定出这个数?

Rényi 问题和 Ulam 问题可以用对策论的观点和术语统一起来, 描述成下面的 Rényi-Ulam 问题: 游戏双方回答者和提问者事先约定了两个整数 $M \geqslant 1$ 和 $e \geqslant 0$, 回答者 R 在称之为搜索空间的集合 $S = \{1, 2, \cdots, M\}$ 中选取了一个秘密数 x^*, 提问者 Q 通过提出一系列问题由回答者 R 来作答, 从而设法找出数 x^*. 对于提问者 Q 的每个问题, 回答者 R 只以“是”或“否”作答, 并且允许回答者 R 说谎至多e 次.

在 Rényi 问题中, 假定了如果总的提问次数为 n, 则允许错误回答的总次数至多为 pn, 这里 p 是一个给定的数 ($0 \leqslant p < 1$); 在 Ulam 问题中, 假定了说谎次数至多为 2.

§1.1.2　噪声通信与纠错编码

离散空间上的容错搜索理论的重要应用之一涉及通过噪声信道的双向通信. 两个通信代理人, 发送者和接收者, 事先约定 M 条消息 (一条消息通常是由 0, 1 组成的二元序列) 的一个集合, 发送者通过一个噪声信道发送其中一条消息. 由于信道是有噪声的, 这条消息的某些位在传输过程中可能失真, 此时接收者面临一个任务是恢复这条消息. 这一任务显然是不可能实现的, 如果消息可以被任意地扭曲, 幸运的是实际上失真部分往往仅是少量的. 因此, 对可能出现的扭曲, 假定一些限制是

完全合理的, 例如, 假定失真位数的一个上界, 假定给定的位被改变的概率等. 对扭曲总量的一个经典的限制是假定在传输过程中至多 e 位能被改变, 但这些错误可能发生在任何位置.

噪声信道的现实与人们对通信可靠性的期盼自然驱动人们研究, 如何对消息进行编码才能使得在提出的限制下不管怎样失真接收者总能恢复原始消息? 即**纠错编码问题** 或**抗干扰编码问题**. 这一问题最早由 Shannon[15] 和 Hamming[16] 所研究, 两者都假定发送者没有从接收者获取任何反馈信息, 即该消息的每一位在第一位发送之前均已确定. 这种模型往往被称为"非适应的"或"无反馈的". 显然, 对于这种模型, 发送者不能通过推迟计算该消息的相继位获得益处.

一个长度为 n 的 M 个二元序列的集合 C 称为一个"长度为 n 大小为 M 的 e 纠错编码", 如果发送者通过噪声信道发送一条消息 $s \in C$, 且至多 e 位能被改变, 接收者总能根据所获得的序列 s' 正确地计算 s. C 的元素称为"码字" (words of code). 人们通常希望码长 n 应该尽可能地小, 因为长度的增大会导致使用费用的增加. 因此,

- 非适应的纠错编码理论的基本问题是: 给定正整数 M 和 e, 如何找出最短的大小为 M 的 e 纠错编码?

众所周知, 一个编码的纠错容量 (error-correcting capacity) 依赖于其码字之间的最小 Hamming 距离, 这里, 两个码字之间的 Hamming 距离是其不同的位的个数. 更精确地, 一个编码是 e 纠错的当且仅当其最小 Hamming 距离 $\geqslant 2e+1$ [17]. 注意到这一特征, 非适应的纠错编码理论的基本问题具有如下等价的、纯组合的、更广泛使用的描述形式:

- 给定正整数 n 和 d, 如何找出具有最小 Hamming 距离 d 的长度为 n 的最大的二元序列集合 C?

Dobrushin[18] 和 Berlekamp[19] 考虑了另一种不同的通信装置: 用来发送消息的噪声信道具有一个相伴的无噪声无延迟的反馈信道 (noiseless delayless feedback channel, NDFC), 接收者可以利用这一反馈信道向发送者发送某些反馈信息, 假定发送者在发送第 j 位之前得到前 $j-1$ 位的反馈信息, 并且反馈信息不会失真. 这种模型往往被称为"适应的"或"带反馈的". 在这种模型中, 这两个信道具有如此不对称的特征可以解释为是由于发送者和接收者的传输功率不同所致. 例如, 如果发送者是在宇宙飞船上而接收者是在地球上, 接收者所发消息的失真现象可以忽略不计, 而发送者所发消息的失真现象也许非常严重.

无噪声无延迟的反馈信道的存在允许人们以一种交互的方式组织通信: 发送者发送一位, 等待反馈, 基于此反馈计算要发送的下一位, 如此重复进行. 这里仍

要对由噪声信道所引起的扭曲总量提出某些限制. 现在发送者所发消息的长度 (位数) 可以不同 (依赖于所得反馈信息), 此时编码策略的长度是最坏情形的位数. 与非适应情形相似, 人们期待找到有效的适应的编码策略 (coding strategies), 它能够使得在提出的限制下接收者总能恢复原始的消息. 特别地, 所谓 "适应的 e 纠错编码" (adaptive e-error correcting code), 指的是只要至多 e 位被扭曲接收者总能恢复原始消息的编码策略. 类似地,

- 适应的 e 纠错编码理论的基本问题是: 给定正整数 M 和 e, 如何找出最短的大小为 M 的适应的 e 纠错编码?

§1.1.3 Rényi-Ulam 问题与噪声通信问题的联系

假定存在针对 Rényi-Ulam 问题且对错误回答提出了某些限制的大小为 M 的搜索空间的一个搜索策略, 这一策略保证在满足所给限制条件的前提下, 提问者总能在 n 次提问之后找出回答者所选择的未知目标. 我们建立 Rényi-Ulam 问题与NDFC的如下对应关系: 将 Rényi-Ulam 问题中的提问者、回答者分别视为NDFC中的接收者和发送者; 将搜索空间的未知目标视为发送者要发送的消息; 所提的每一个问题通过无噪声无延迟反馈信道传输, 而每一个回答 YES 和 NO(分别对应 1 和 0) 通过噪声信道传输. 这样一来, 搜索策略的性质保证在满足所给限制条件的前提下, 提问者 (接收者) 总能在 n 次提问之后找出回答者所选择的未知目标 (发送者所发送的消息). 因此, Rényi-Ulam 问题中的 n 次提问总能成功找出未知目标的一个搜索策略, 必然导致NDFC中的一个具有相同纠错容量的适应的编码. 相反地, NDFC中的一个大小为 M 的长度为 n 的适应的 e 纠错编码, 也必然导致一个在错误回答次数不超过 e 的前提下, n 次提问之后总能从大小为 M 的搜索空间中找出未知目标的 Rényi-Ulam 问题的搜索策略. 更加详细的论述参考文献 [20].

至此, 我们已经看到上述两个噪声通信问题本质上等价于相对应的 Rényi-Ulam 问题: 适应的 e 纠错编码理论的基本问题等价于寻找一个允许至多 e 次错误回答时适应的 Rényi-Ulam 容错搜索问题的最优搜索策略 (即具有最少提问次数); 相似地, 非适应的 e 纠错编码理论的基本问题等价于寻找一个允许至多 e 次错误回答时非适应的 Rényi-Ulam 容错搜索问题的最优搜索策略.

应该指出的是, Rényi-Ulam 问题具有众多的实际应用背景, 所描述的与噪声通信问题的等价关系仅是其应用广泛的佐证之一. 下面是 Rényi[13] 所给的另外两个应用实例:

搜索空间为一个病人可能患有的疾病. 医生为了做出诊断, 需对病人进行一系列的检查, 每一项检查的目的在于确定病人所患的疾病是否属于给定的几种. 由于种种因素的影响, 其中某些检查可能不准确.

搜索空间为一个复杂机械的若干重要部件，已知其中一个部件有故障. 每次选择几个部件进行测试以便判断故障部件是否属于其中. 由于测试装置未必绝对精密，某些测试结果可能有差错.

Katona[21] 对 Rényi-Ulam 问题的实际应用价值进行了详细分析.

上述著名的 Rényi-Ulam 问题, 对于离散空间上的容错搜索理论研究起到了关键作用. 一方面, 众多的实际问题能够转化为这类问题；另一方面, 以这两个问题为背景而建立的离散空间上的容错搜索问题的模型分类, 语言简洁, 条理清晰, 能使众多的已知结果恰当地纳入这一理论体系之中, 同时能使有兴趣的读者清楚地发现许多具有重要意义的未解决的问题, 也能使读者根据实际需要对模型的分类加以丰富和完善.

§1.2　离散空间上的容错搜索模型的分类

§1.2.1　一种描述形式：Rényi-Ulam 模型

离散空间上的容错搜索 Rényi-Ulam 模型可以用对策论的术语描述为下面的二人对策游戏. 提问者和回答者在游戏开始以前, 就以下事项达成协议：

条款 1　搜索目标所在的范围, 即搜索空间 (search space);

条款 2　搜索目标的类型 (the type of search object);

条款 3　回答者的差错模式 (error pattern);

条款 4　提问者的提问格式 (the format of queries);

条款 5　提问者和回答者的交互程度 (the degree of interactivity).

假定回答者在搜索空间 S 中选取了搜索目标 (对提问者来说是秘密的), 接着提问者根据协议提出一系列问题而回答者根据协议作答. 如果提问者能在 k 次提问和 k 次回答之后识别出所有搜索目标, 则**提问者取胜**; 否则, **回答者取胜**. 称提问者有一个**长度为 k 的取胜策略**(winning strategy of length k) 如果他在 k 次提问和 k 次回答之后总能取胜, 不管回答者怎样作答 (只要不与协议冲突). 称一个取胜策略为**最优的**, 如果它具有最小的长度 (即最少的提问次数). 容错搜索理论的核心问题是找到给定模型的最优取胜策略. 它要求所得的最优取胜策略不仅应该理论上是最优的, 而且应该能够直接实施 (即一个具体的算法). 因此, 最优取胜策略往往是构造性的.

根据不同的应用背景, 上述协议条款 1 ~ 5 具有各种各样的不同选择, 每一种可能的组合搭配确定了一个搜索模型. 因此, 容错搜索模型具有众多的变化形式. 下面我们讨论每一项协议条款的可能的不同选择 (也许还有其他不同选择, 这里仅列举文献中已出现的可能选择）.

(1) 要确定的第一项规则是搜索空间. 我们注意到搜索空间仅依赖其大小, 而与其元素的实际意义无关. 文献中已出现过的搜索空间有：

有界空间 通常用 $\{1,2,\cdots,M\}$ 表示, M 表示搜索空间的大小.

无界空间 通常用 $\{1,2,\cdots\}$ 表示.

(2) 要确定的第二项规则是搜索目标的类型. 一般情况下取决于搜索目标的个数 N. $N=1$ 时称为**单目标**, $N\geqslant 2$ 时称为**多目标**. 多目标情况通常要求更加明确的再分类.

(3) 要确定的第三项规则是回答者的差错模式. 文献中已出现过的差错模式有：

固定差错总数 回答者在整个游戏过程中至多说谎 e 次, 这里 e 是一个固定的正整数.

全局有界的差错比例 如果整个游戏进行 n 次提问, 回答者能够说谎至多 pn 次, 这里 $p<1$ 是固定的.

前缀有界的差错比例 在前 m 次提问中回答者能够说谎至多 pm 次, 这里 $p<1$ 是固定的.

随机差错 差错次数是随机的. 即在每次回答之前, 回答者掷一枚硬币, 正面说谎, 反面不说谎.

半谎模式 回答者在整个游戏过程中至多说谎 e 次, 但仅在回答 "否" 时可以说谎, 所有回答 "是" 均保证是正确的.

(4) 要确定的第四项规则是提问者所提问题的具体形式. 最基本的形式是 "自由提问"：提问者 Q 的提问形如 "$x^*\in A$?", 这里 A 是搜索空间的一个任意子集. 如果对于提问者 Q 的每次提问, 回答者 R 只以 "YES" 或 "NO" 作答, 我们称这种问答形式为 "2 维自由提问" 格式. "2 维自由提问" 格式原始地由 Rényi 和 Ulam 提出, 但后来的众多文献, 有些放宽了这一形式, 有些采用了更加严格的限制：

q 维自由提问格式 ($q\geqslant 2$ 是任意一个固定的正整数) 提问形如 "未知目标 x^* 属于 $A_1,A_2,\cdots,A_q$ 的哪一个集合？", 这里 $A_1,A_2,\cdots,A_q$ 是搜索空间的任意一个剖分. 对于提问者 Q 的每次提问, 回答者 R 以 "i" 作答, 这里 $i\in\{1,2,\cdots,q\}$. 对于 $q=2$, 这正是 2 维自由提问格式.

比较型提问格式 提问形如 "$x<a$?", 这里 a 是搜索空间的任意一个元素. 对于提问者 Q 的每次提问, 回答者 R 只以 "YES" 或 "NO" 作答. 因此, 比较型提问格式属于 2 维搜索模型的范畴.

区间型提问格式 提问形如 "$x\in[a,b]$?", 这里 $a\leqslant b$. 对于提问者 Q 的每次提问, 回答者 R 只以 "YES" 或 "NO" 作答. 因此, 区间型提问格式属于 2 维搜索模型的范畴.

双区间型提问格式 提问形如 "$x\in[a,b]\bigcup[c,d]$?", 这里 $a\leqslant b$ 且 $c\leqslant d$. 对于提问者 Q 的每次提问, 回答者 R 只以 "YES" 或 "NO" 作答. 因此, 双区间型提问

格式属于 2 维搜索模型的范畴.

大小受限自由提问格式 提问形如 “$x \in A$?”, 这里 $|A|$ 不能超过一个给定的上界 k. 对于提问者 Q 的每次提问, 回答者 R 只以 “YES” 或 “NO” 作答. 因此, 大小受限自由提问格式属于 2 维搜索模型的范畴.

可变费用提问 提问者对不同的提问支付相应的费用, 提问总费用有一个给定的限制.

非重复提问 同一个问题不允许被重复提问.

(5) 要确定的第五项规则是提问者和回答者的交互程度.

适应的 提问者进行第 j 次提问之前已获得前 $j-1$ 次提问的答案, 即提出第 1 个问题, 等待回答; 提出第 2 个问题, 等待回答; $\cdots$

k 批提问 提问分 k 批进行, 这里 k 是一个固定的正整数. 提第一批问题然后作答, 再提第二批问题然后作答, $\cdots$

非适应的 即 1 批提问与作答, 所有提问应该一次性提出, 不等待任何回答.

§1.2.2 另一种描述形式: Coin-Weighing 模型

§1.2.1 给出了离散空间上的容错搜索 Rényi-Ulam 模型的一般化描述形式. 我们注意到提问者所提问题的具体形式是多种多样的. 那么确定这些提问形式的依据是什么呢? 对于搜索空间 $S = \{1, 2, \cdots, M\}$, 假定我们选取提问形式:

“搜索目标 x^* 属于集合 $\{1\}, \{2\}, \cdots, \{M\}$ 的哪一个?”,

则在不允许说谎的情况下 1 次提问即可找到搜索目标 x^*, 显然, 这比采用自由提问 “$x^* \in A$?” 所用的提问次数 $\lceil \log_2 M \rceil$ 要小. 然而前一个提问形式是不合理的, 后一个提问形式则是合理的. 一个提问形式是否合理, 关键在于是否存在相应的试验装置来实现它. 下面的 Coin-Weighing 模型能够使我们更容易地选取合理的提问形式.

离散空间上的容错搜索 Coin-Weighing 模型可以描述为: 给定的搜索空间中全为外观相同的硬币, 其中若干个是具有相同重量的好币 (good coins), 其他均是重量不同于好币的伪币 (counterfeit coins). 在事先明确并遵守以下条款的情况下, 如何能以最少的试验次数找出全部搜索目标 (伪币) 呢?

条款 1 搜索目标所在的范围, 即搜索空间;

条款 2 搜索目标的类型;

条款 3 试验装置的差错模式;

条款 4 试验装置的类型;

条款 5 试验过程的交互程度.

Coin-Weighing 模型与 Rényi-Ulam 模型形式上是相同的, 条款 1, 2, 5 的各种选择与 Rényi-Ulam 模型也是相同的. 所不同的是, 这里以 “试验装置的类型” 代替了 “提问者的提问格式”, 以 “试验装置的差错模式” 代替了 “回答者的差错模式”.

正是这种替代使得选取合理的提问形式变得有章可循.

在 Coin-Weighing 模型中, 试验装置一般总是取为 r 臂天平. 通常考虑 $r=1$, $r=2$, $r\geqslant 3$ 三种情况, 分别对应于1 **臂天平**(即普通的秤, 每次试验选取一个集合 A 置于其盘中)、2 **臂天平** (即每次试验选取两个等量集合 A, $B(|A|=|B|)$ 分别置于天平的左盘和右盘中) 和r **臂天平** (以后解释). 现在, 我们以非容错情形 (即不允许说谎) 为例来分析 Coin-Weighing 模型与 Rényi-Ulam 模型的联系与区别.

例 1.1 n 个硬币组成的搜索空间 $S=\{1,2,\cdots,n\}$ 中含有一个重币 x^*(假设其重量为 w_h), 其他 $n-1$ 个硬币是重量均为 $w_g(<w_h)$ 的较轻的好币. 采用 1 臂天平作为试验装置. 对于选取的一个试验集 A, 若集合 A 的重量 w_A 大于 $|A|w_g$, 则意味着 A 含有重币 x^*; 否则意味着 A 不含重币 x^*. 如果我们建立如下对应关系:

Coin-Weighing 模型	Rényi-Ulam 模型
重币 x^*	秘密数 x^*
试验者	提问者
试验装置	回答者
试验集 A	提问 "$x^*\in A?$"
反馈 "$w_A>\|A\|w_g$"	回答 "YES"
反馈 "$w_A\leqslant\|A\|w_g$"	回答 "NO"

则 Coin-Weighing 模型的一次试验恰好等价于 Rényi-Ulam 模型的一次提问. 这表明 1 臂天平正是实现自由提问 "$x^*\in A?$" 的试验装置, 因此, 自由提问 "$x^*\in A?$" 是合理的.

进一步地, 比较型提问 "$x^*<a?$"、区间型提问 "$x^*\in[a,b]?$" 和双区间型提问 "$x^*\in[a,b]\bigcup[c,d]?$" 都属于自由提问格式 "$x^*\in A?$", 其试验集 A 分别为 $A=\{j\in S|j<a\}$, $A=\{j\in S|a\leqslant j\leqslant b\}$, $A=\{j\in S|a\leqslant j\leqslant b\}\bigcup\{j\in S|c\leqslant j\leqslant d\}$. 因此, 1 臂天平也是实现比较型提问、区间型提问和双区间型提问的试验装置. 它们都是合理的提问形式.

例 1.2 n 个硬币组成的搜索空间 $S=\{1,2,\cdots,n\}$ 中含有一个重币 x^*(假设其重量为 w_h), 其他 $n-1$ 个硬币是重量均为 $w_g(<w_h)$ 的较轻的好币. 采用 2 臂天平作为试验装置. 对于选取的一个试验集 $A:B$(即集合 A, B 分别置于天平的左盘和右盘中), 则此次试验所得结果必是以下三种反馈之一 (记 $C=S-A-B$ 表示未参与本次试验的硬币集):

若试验结果为 "左重", 则意味着 "A 含有重币 x^*";

若试验结果为 "右重", 则意味着 "B 含有重币 x^*";

若试验结果为 "平", 则意味着 "C 含有重币 x^*".

如果我们建立如下对应关系：

Coin-Weighing 模型	Rényi-Ulam 模型
重币 x^*	秘密数 x^*
试验者	提问者
试验装置	回答者
试验 $A:B$	提问“x^* 属于 A, B, C 的哪一个？”
反馈“左重”	回答“$x^* \in A$”
反馈“右重”	回答“$x^* \in B$”
反馈“平”	回答“$x^* \in C$”

则 Coin-Weighing 模型的一次试验恰好对应于 Rényi-Ulam 模型的一次提问. 这表明 2 臂天平正是实现 Rényi-Ulam 模型 3 维自由提问格式的试验装置, 因此, Rényi-Ulam 模型的 3 维自由提问格式是合理的.

例 1.3 对于两目标 Rényi-Ulam 模型，什么样的提问格式是合理的呢？考虑两目标的 Coin-Weighing 模型：n 个硬币组成的搜索空间 $S=\{1,2,\cdots,n\}$ 中含有两个伪币 x 和 y, 其他 $n-2$ 个硬币是重量相等的好币. 采用 1 臂天平作为试验装置. 对试验集 $A\subseteq S$, 用记号

$$\begin{aligned}
&F(A)=\varnothing \quad &\text{表示}\quad &x\notin A, y\notin A;\\
&F(A)=X \quad &\text{表示}\quad &x\in A, y\notin A;\\
&F(A)=Y \quad &\text{表示}\quad &x\notin A, y\in A;\\
&F(A)=XY \quad &\text{表示}\quad &x\in A, y\in A.
\end{aligned}$$

Hwang[22] 根据 x, y 是否有区别并且合并本质上等价的情况后, 得到以下七个模型：

$\varnothing|X|Y|XY$ 模型 B (basic);
$\varnothing|X|Y,XY$ 模型 D (various degrees in irregularity);
$\varnothing,XY|X|Y$ 模型 C (candy factory);
$\varnothing|X,Y,XY$ 模型 G (group testing);
$Y|\varnothing,X,XY$ 模型 U (underweight);
$\varnothing,XY|X,Y$ 模型 P (parity);
$\varnothing|X,Y|XY$ 模型 Q (quantity).

借助于例 1.2 所建立的对应关系, 并把 x, y 看作两目标 Rényi-Ulam 模型要寻找的两个秘密数 (不妨认为 y 大于 x), 则

模型 G 决定了在两目标 Rényi-Ulam 模型中采用提问形式“集合 A 不含任何秘密数吗？”是合理的, 其两个回答为“YES”和“NO”;