

第 3 章 比特与逻辑



作者简介

葛宁,清华大学研究员、博士生导师、电子工程系通信研究所所长;基金委创新群体核心成员,2000—2006 年曾任清华华环公司首席科学家;中国指挥与控制学会电磁频谱安全与控制专业委员会委员、中国电子学会通信学分会委员。1993 年和 1997 年在清华大学获得学士与博士学位,1997—1998 年在加拿大多伦多大学做博士后,1998—2000 年在美国 ADC 工作任高级工程师。主要从事通信片上系统、短距离无线通信、宽带无线网络等方面的研究工作。先后负责国家科技重大专项、863 目标导向、973 课题和自然科学基金重点项目等。发表 SCI 论文 40 余篇,申请专利 20 余项,获得集成电路布图设计专有权 2 项。曾获 2017 年通信学会科学技术奖一等奖、2014 年及 2017 年吴文俊人工智能科学技术进步奖一等奖、2016 年电子学会创新团队奖。

3.1 概念与内涵

3.1.1 比特的定义

比特是信息科学学科中基本而重要的概念,它既是信息的度量单位,也是信息的重要表示形式,通常由“0”“1”两个符号组成。两个不同的事物可以通过“0”“1”这两个不同的符号表示。当一个事物处于两个不同状态之一时,我们也可以将这两个状态映射为“0”“1”不同比特。通过多个比特的组合,可以表示多个状态,简单地说 n 个比特可以表示 2^n 个状态。由于状态越多,事物的不确定性越大,从度量的角度,描述处于某一特定状态需要的比特数目也越多,因此比特可以作为度量来描述事物的不确定性。

电子工程学科以电子运动和电磁波及其与物质相互作用的理论为核心,研究信息的产生、获取、存储、显示、处理、传输、利用及其相互关系的科学。现代电子工程学科仍然以还原论为基本科学研究方法。还原论主张把高级运动形式还原为低级运动形式,将电子信息系统视为更低级、更基本的现象的集合体或组成物。“0”“1”比特高度体现了这种哲学观点,事物可以通过比特组合的序列来表示,运动可以通过比特代表的数量变化来刻画,信息可以通过以比特为单位的熵来度量。现代信息系统以数字化为特征,建立在还原论的方法上。例如,一个通信系统由信源编解码、信道编解码、调制解调器、射频与天线组成,其中信道编解码模块又由若干功能电路组成,功能电路由门电路组成,门电路由 CMOS 管组成。通俗一些,一个房间由门、窗、墙壁组成,窗户由窗框、中间的透明部分和活动构件组成,活动构件由铰链、执手、滑轮等组成。这种分解的思维方式在现代电子工程学科中取得了巨大的成功,其代表之一就是数字集成电路,上千万的门电路通过模块按照不同的层次组合成为处理器、存储器、通信单元等,构成了电子产品的核心,完成了人机界面、信息处理、无线通信等一系列现代信息核心技术,塑造了 Apple、Intel、Qualcomm 等产业巨人。

中国古代认为“无极生太极,太极生两仪,两仪生四象,四象生八卦,八卦演万物”,这从另一个角度阐述比特的由来。大体的意思是“0 生出 1,1 生出 2,2 生出 4,4 生出 8,以此类推到无穷”。虽然也是论述万物与比特的对应关系,但是与还原论微妙的区别在于东方的哲学是从整体出发的,试图把握事物的整体。以德谟克利特的原子论为代表,还原论的起源要追溯到西方古希腊哲学,还原论与整体论在历史上争论了很长时期,现在越来越走向辩证统一。在生物等复杂系统面前,有些问题只能通过综合才能解决。如何从“0”“1”比特回归到复杂系统与网络可能是未来一个值得思考的问题。

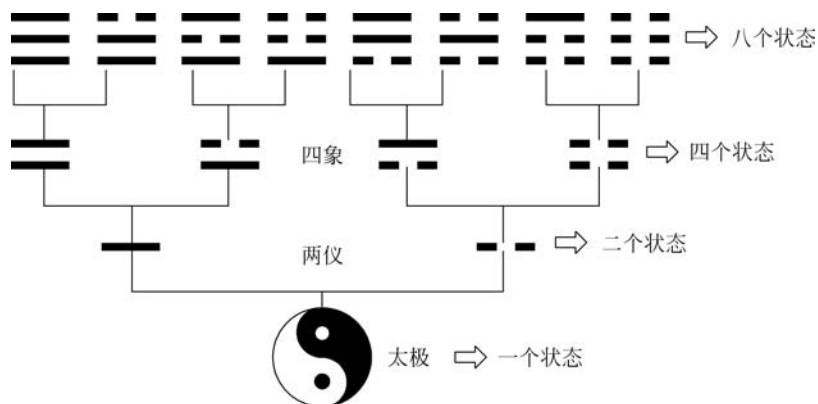


图 3.1.1 八卦图

3.1.2 比特的物理观

比特“0”“1”是客观存在的,还是人们的主观概念?这是一个哲学争论,我们这里不做讨论,也很难有结论。但是,比特这一概念的产生、应用和发展与我们客观物理世界有着紧密的联系。从某种意义上讲,比特代表了现代科学对世界的认识理念与途径。在根本问题上,物理学研究“世界是什么?如何起源、变化与发展?”,哲学思考“物质和意识谁是第一性,存在和思维有无同一性?”。物理和哲学的根本问题与比特都存在关联。

物理学一定是人类的物理学,研究的也是人类所在宇宙中的基本物理规律。作为高等生物系统的人所在的宇宙,其基本物理规律和所在状态一定要满足人类存在的条件。我们的太阳系处于一种相对平衡的状态,而地球本身作为一个开放的系统,一方面太阳为其提供了大量的能量(约 10^{17} W),另一方面 6000 K 高温的太阳辐射相对 253 K 地球辐射提供了负熵流(-10^{14} W/K)。这些条件支撑了人体作为耗散结构的存在,地球在远离平衡的非线性区形成了新的稳定的宏观有序结构。宏观的有序结构为比特概念的产生、应用和发展奠定了基础。宏观上看,地球在太阳影响下处于远离平衡态的“动态平衡”,所谓平衡态是指系统各处可测的宏观物理性质均匀(从而系统内部没有宏观不可逆过程)的状态,由于地球摆脱了这种均匀的混沌状态,才会有“无极生太极,太极生两仪”,产生白天与黑夜,春夏秋冬四季变化,“0”“1”比特所代表的“0”与“1”才有了区分的意义。

近代物理确认各种物质之间的基本的相互作用可归结为四种:引力相互作用、电磁相互作用、弱相互作用和强相互作用。基本相互作用决定物质的结构和变化过程。在强力作用下,夸克合成了核子,核子构成了原子核。在电磁力作用下,原子核和电子形成了原子,继而组成了分子,分子凝为各式各样的大块物质。这些物质在引力的作用下,形成了现在的宇宙及其运动状态。这四种力的综合作用,又决定着世界将来的演化。万物由有限的原子组成,无机物的分子量往往较小(水的分子量是 18),蛋白质是高分子量的复杂的有机物(分子量通常从五千到百万以上)。物质的有限组成,例如元素周期表,为万物

的有限比特表示提供了物理基础。相互作用是有序的起因,热运动是无序的来源,相变是有序和无序两种倾向相互竞争的结果。运动规律取决于有限的基本作用和热运动的统计规律,因此以数量关系来描述运动和物质的状态成为可能。

物质、能量、信息共同构成现实世界的三大要素。没有物质,什么也不存在;没有能量,什么也不会发生;没有信息,任何事物都没有意义。信息与物质、能量是密不可分的、紧密相关的。没有物质和能量,就不存在事物及其运动,也就无从谈起运动状态和规律,当然也就不会有运动状态和规律的表征的信息,这是信息对物质和能量的依赖性。但是,具有知识秉性的信息,作为事物及其运动状态和规律的表征的信息,可以脱离原来的物质、能量而相对独立地被人们摄取、传递、加工和处理。物质、能量与信息是一切客观事物的三个基本方面。

3.1.3 比特的数学观

物理揭示自然界的奥秘,自然界乃至社会中物质及其运动规律的刻画离不开数学。各种各样的物体及其状态在数学上往往通过集合进行描述,而物体及其状态间的运动与变化则通过集合上的关系进行刻画。

所谓集合,是由一堆个体构成的整体。例如氢、氦、锂、铍、硼等组成的化学元素集合,“1,2,3,4,...”等组成的自然数集合。集合是现代数学的基础。一方面,任何一门具体的数学都必须明确自己的研究对象。这些研究对象,就构成了一个或若干个集合。几何研究点、线、面等组成的集合,算术研究整数、分数等组成的集合,微积分研究实数、函数等组成的集合。另一方面,数学归根结底研究数与形。数有复数、实数、有理数、整数、自然数。复数可以等效为两个实数组成的数对,实数可以归结为有理数的分割,有理数又可以视为两个整数之比,整数可以归结为自然数。显然,自然数可以通过“0~9”的有限符号串表示,也可以通过“0”“1”的有限比特串表示。

由有限元素组成的是有限集,由无限元素组成的是无限集。对于有限集中的元素我们很容易通过有限符号来一一表示,这些符号可以转换为由有限比特组成的字符串,理论上,有限集中所有的元素都可以通过有限长度的比特串表示。对于无限集中的任意一个元素,例如自然数中任意一个数,我们仍然可以通过约定规则将其通过有限长度的比特串表示,但是每个元素对应的比特串长度不可能是固定的,无限集中所有的元素无法通过有限长度的比特串表示。实际上,集合也可以通过特性或符合条件来刻画。集合的枚举和条件刻画方法相结合,我们就可以利用有限的比特串来描述集合及其元素。

集合上的关系刻画了元素个性和变化规律,集合 X 与集合 Y 上的二元关系 R 相当于 X 与 Y 笛卡儿积的子集,也就是说,关系本质上就是集合。因此,有限的比特串也可以刻画集合上的关系。集合上的关系中有一类非常常用,就是函数,函数相当于输入值集合与输出值集合上的对应关系,通常情况下一个输入值对应唯一输出值。当集合元素用比特串来表示时,函数就可以看做是一串“0,1”到另一串“0,1”上的映射。由于“0,1”上的操作可以逐步简化为“与、或、非”等基本逻辑操作,函数就可以通过逻辑来计算。

更进一步,当函数以时间为输入值,以事物的状态为输出值时,就可以描述事物的运动与变化。时间通常是连续的,事物的状态也会出现连续性,如何通过离散不连续的比特来刻画连续的过程和状态,也是比特表示中的一个重要问题。它的解决可以通过电影来形象描述。一部电影在人看来是一个连续的过程,但是实际上电影是由一幅幅离散的画面组成,数字化电影中的画面又是由比特串描述的,通过高速放映还原了真实世界的写照。

在了解了比特在数学中的重要地位后,我们也应当看到比特的不足。数字计算机在处理人脑常见的视听觉信息时有很大的局限性,语音识别、图形搜索都难以达到令人满意的效果。人类的学习与智慧如何通过数字计算机实现成为前沿课题。

3.1.4 比特的电子工程观

在电子工程学科中,围绕电磁场与物质的相互作用,比特需要支撑两个核心问题:一个是电磁现象如何描述分析,另一个是电磁规律如何利用。麦克斯韦方程组建立了电磁场理论。该方程组在常规的物质、介质中表现为线性规律,也就是输出的电磁场与输入的电磁场呈比例,满足叠加性,即

$$f(A+B)=f(A)+f(B)$$

在此情况下,电磁现象具有良好的连续性,就是输入微小的误差只会引起输出微小的误差。这种情况下电磁现象涉及的物理量就可以从连续量近似为离散量,映射到比特进行研究。研究结果与真实物理现象的偏差是可以控制的。电磁现象可以用离散量来描述,启发我们思考以下问题:为什么现代电子系统都倾向用数字化方法来设计构建?电磁现象以外的社会、生物、物理研究为什么都选择数字系统作为处理平台?比特流行的电子工程基础是什么?

以比特为代表的数字电路精度和鲁棒性上有着模拟电路无法取得的优点。模拟电路依靠电容、电阻、电感的数值来完成电路功能的核心指标,由于电容、电阻、电感数值往往存在较大的偏差,例如集成电路中的电容有10%~20%的偏差,这些偏差很容易造成电路核心指标的偏离,如振荡频率、基准电压、滤波带宽等。当多个电路模块组合时,模拟电路相互耦合相互影响,电路中的噪声更加难以控制,因此大规模集成电路往往采用数字电路形式。在物理极限方面,Shannon-von Neumann-Landauer (SNL)给出1比特数据吞吐量对应的最小能量为

$$E_{\text{bit}} \geq E_{\text{SNL}} = k_{\text{B}} T \ln 2 = 0.017 \text{eV} \quad (T = 300 \text{K})$$

最小的开关尺寸为

$$x_{\text{min}} = \frac{\hbar}{\Delta p} = \frac{\hbar}{\sqrt{2m_{\text{e}} E_{\text{bit}}}} = 1.5 \text{nm}$$

可以看出,比特对应的理论最小处理能量和开关尺寸都是非常小的,实际上现代集成电路工艺在物理尺寸上已经进入nm范围了。比特及其对应的数字逻辑电路已经在电子工程领域占据了重要地位,无线通信、雷达探测、无线电导航、信号处理、媒体处理、计算机等领域都以比特为信息传输、处理、应用的核心载体。

3.2 编码映射与布尔代数

3.2.1 编码

编码从广义上讲是信息从一种形式或格式转换为另一种形式或格式的过程。狭义上可以将编码理解为将图像、语音、信号转换为具有特定格式字符序列的过程。抽象上看编码是各种集合的元素映射到字符串的过程。准确地说,有限集合 X 上的串是由 X 中的元素组成的有限序列,其中,序列是一个定义域由连续整数集合组成的特殊函数。

最简单的编码形式是有限集合 S (原始集合) 到有限集合 C (编码集合) 的映射,例如表 3.2.1 所示 ASCII 字符编码表,就是将我们计算机中常见字符进行编码,其中“空格”对应的比特序列就是“0100000”,而字符“0”对应的比特序列就是“0110000”。反过来,在计算机处理中“0100000”对应“空格”,而“0110000”对应字符“0”。

表 3.2.1 ASCII 编码表

比 特 串	字 符	比 特 串	字 符
010 0000	Space(空格)	011 0011	3
010 0001	!	...	...
010 0010	"	100 0001	A
010 0011	#	100 0010	B
...	...	100 0011	C
011 0000	0	100 0100	D
011 0001	1	...	...
011 0010	2		

再看一种编码,出版物对应的 ISBN 编码,目前的 ISBN 编码为 13 位,如图 3.2.1 所示。包括五个部分,分别是:第一组 978 或 979;第二组国家、语言或区位代码,例如中国大陆为(978-)7;第三组出版社代码,例如(978-7-)04 为高等教育出版社;第四组为书序码,例如(978-7-04-)022559 对应的书名为《信号与系统——MATLAB 综合试验》;第五组为校验码,只有一位,0~9,图 3.2.1 中为 4。ISBN 编码对全世界的正式出版物进行了规范的唯一编码,这与书名有很大的不同。如果我们以书名《信号与系统》进行搜索,则可以搜索出一系列的图书,如郑君里老师等编著的《信号与系统》(上册)(第 2 版)(ISBN: 9787040079814),奥本海姆等编著的《信号与系统》(第 2 版)(英文影印版)(ISBN: 9787121087486),奥本海姆等编著的《信号与系统》(第 2 版)(精编版)(ISBN: 9787560537726)等。

《信号与系统》(第二版)(上、下册)
 郑君里 应启珩 杨为理 著
 ISBN7-04-007981-X ISBN7-04-007983-6
 2000年5月
 高等教育出版社

本书研究确定性信号连续性时不变系统传输与处理的基本概念和基本分析方法,从时域到变换域,从端口描述到状态空间描述,以实际应用为主要依据,兼顾离散和连续信号与系统之选材。本书在讲授传统内容的过程中充分体现时代气息。经典理论的论述与最新技术之引入密切融合,以当代信息科学的观点理解、审视、组织和阐述传统内容。注重结合基本概念,大量介绍各类应用实例(如PCM通信、CDMA通信、小波变换、宏观经济增长预测、人口模型等),强烈激发起学生的学习志趣和热情。第六章信号的矢量空间分析将正文、相关等重要概念以统一的数学和物理方法讲授,使学生对信号理论的学习步入更深层次,并初步理解它们的工程应用。这些内容的选取及其讲授方法为国内、外同类教材之首创,特色鲜明。

本书结构和选材有很大灵活性,能够适应电子工程与信息科学各类专业之需要。任课教师可根据实际情况选择不同章节组成深度和学时有区别的课程。目前至少有二百余所院校多种类型专业选用本书作教材,还有更多院校指定本书为研究生入学考试必读教程。

**《信号与系统》学习辅导新书——
《教与写的记忆——信号与系统评注》**
 郑君里著
 ISBN 7-04-017387-5
 2005年8月
 高等教育出版社

本书是和君里等著《信号与系统》(第二版)的配套教学辅导书,主要内容是对第二版原著各章作详细的评注解读,注重概念理解、分析对比、历史背景和综合应用,讨论题目源于作者数十年授课实践之积累(包括讲稿、讨论题、习题、考试题等综合资料),对于协助教师备课、引导学生自学、考研综合复习以及准备海外留学都是相当理想的参考读物。

结合研究讨论,作者回忆了五十年学习与工作的感受,纵论国内外教学变革,其中对于清华园墨香的描述,读来使人如临其境,即使对信号与系统不了解的读者,阅后也会感受到本书的独特魅力。

ISBN 978-7-04-022559-4
 9 787040 225594 >
 定价 19.00元

ISBN 978-7-04-022559-4
 9 787040 225594 >
 定价 19.00元

图 3.2.1 ISBN 编码示意图

从这一编码中,我们可以看出编码的几个基本特性。

- 普适性: 由于比特串的长度可以伸缩,所有的有限集合都可以建立与比特串的对应关系。也就是说,利用计算机可以表示、存储、处理世界上绝大多数的信息。同时需要注意对于无限集合,例如一个实数,有限长度比特串无法与实数集建立一一对应关系。
- 统一性: 编码是集合 A 到集合 B 的映射关系,通常是一一映射。集合 A 中的元素与集合 B (比特串)一一对应,这种对应关系是编码最基本的要求。这种要求对于元素少的集合通常容易满足,但是对于元素众多的集合存在难度。例如,人与姓名的映射,虽然每个人有唯一的姓名,但是一个姓名并不对应唯一一个人。身份证理论上可以保证一一对应关系,但是在实际中仍然有重号现象,第二代身份证通过全国联网解决重号现象。可以看出,不同时间不同地点的分布式编码涉及相互协同分配问题具有挑战性。

- 结构性：单一比特只能代表两个元素，一般集合的元素个数都远大于 2 个，通常的办法都是利用比特(字符串)来表示多个元素。对于比特串来说，通常编码时会赋予不同位置比特不同的含义，如图 3.2.1 中的例子，不同的出版社有不同的代码对应。从根本上讲，编码的结构性是为了从编码中反演出原始集合 S 中元素的某些性质。这些性质可以用于管理，例如，出版物编码的 ISBN 中的出版社码可以用来管理不同出版社的出版物，便于查找对应的出版社，同时出版社无须协商即可避免出版物的重复编码。
- 紧凑型：编码中字符串的长度反映了编码的效率，理论上 n 比特的字符串最多可以表示 2^n 个不同的元素，这是一个简单的上限。但是，一方面，编码由于结构性的要求，其表示的元素个数难以达到上限。例如，中国的身份证是 18 位，远远超出我国很长一段时间的人口。另一方面，编码的效率与使用的频度是有关系的，应用中往往希望使用频度高的编码长度短而频度低的编码长度长。例如，在英文中常用的单词 I, get, of 等往往较短，而 electromagnetic, omnidirectional, metal-oxide-semiconductor 等专业词汇通常较长。
- 鲁棒性：采用紧凑方式的编码虽然大大提高了表示的效率，消除了原始元素刻画的冗余，但是在使用过程中个别的错误会造成巨大的差异。例如，我们写地址时如果写错了个别笔画，通过人的理解往往可以校正这样的错误，但是如果邮政编码出现错误，机器识别时就会差之毫厘谬以千里。因此，编码为了避免交流中的差错有时会有意添加冗余进行错误的检验与纠正。前面图 3.2.1 中的 ISBN 码的最后一位就是校验位，以发现 ISBN 传递过程中的错误。

3.2.2 逻辑的由来

编码解决了事物的表示问题，但是事物之间是有联系的，如何刻画事物之间的联系？下面我们来看一个反映事物关系的故事。

故事 1：父亲(A)、母亲(B)和三个孩子(C, D, E)组成一个家庭，买了一台彩电。买回来的第一个晚上，关于家中哪几个人看了电视的问题，有以下几种正确说法：

- (1) A 在看电视时， B 也在看；
- (2) D 和 E 或者两人都在看，或者他们之中有一个人看了；
- (3) B 和 C 有且只有一人看了；
- (4) C 和 D 或者两人都看，或者两人都没看；
- (5) 如果 E 看了，那么 A 和 D 也看了。

试问，这个晚上到底哪些人看了电视？

从这样一个例子，我们可以看出，通过编码我们可以将父亲、母亲、三个孩子编码为集合(A, B, C, D, E)，而将是否看电视表示为(0,1)比特。但是，只有编码没有办法解决这两个集合间的联系。

人们可以通过逻辑推理得到结果，知道父亲、母亲、三个孩子谁看了电视。那么能否

用计算机来得到逻辑推理的结果？换句话说，逻辑推理的本质是什么？

逻辑推理的本质是在处理集合元素间的关系。集合间最简单的关系是函数关系，最简单的函数是将比特串代表的不同元素映射到“0”“1”比特。通俗地说，最简单的关系就是集合元素有没有某一性质，“有”“无”构成了复杂关系的基础，解决了“有”“无”问题就可以在此基础上构建更为复杂的关系结构。在逻辑上，也可以集合元素具有“真”“假”性质，通常“真”对应于“1”，而“假”对应于“0”。

函数是自变量到因变量间的映射，我们将变量的取值限定到“0”“1”比特。最简单的函数自变量、因变量都只有一个，我们可以写为：

$$\begin{aligned} x, y &\in \{0, 1\} \\ y &= f(x) \end{aligned} \quad (3.2.1)$$

式(3.2.1)虽然是非常简单的形式，但是由于它对变量的取值有了严格的限制，就可以用“逻辑”来演绎它的具体内涵，结果只可能有四种形式。我们可以表示如表 3.2.2 所示。其中，形式 A、D 与自变量 x 无关，形式 B 是简单的恒等，形式 C 是一个有意义的函数，我们可以从直觉逻辑上称形式 C 为“非”（表示为 $\neg$ ）。

表 3.2.2 单变量逻辑函数形式

x	y (形式 A)	y (形式 B)	y (形式 C)	y (形式 D)
0	0	0	1	1
1	0	1	0	1

当自变量增加到两个时，可以写为：

$$\begin{aligned} x_1, x_2, y &\in \{0, 1\} \\ y &= f(x_1, x_2) \end{aligned} \quad (3.2.2)$$

式(3.2.2)也很简单，同样可以通过“逻辑”演绎出它的具体形式，如

表 3.2.3 两个变量逻辑函数形式

$x_1 x_2$	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
00	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
01	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
10	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
11	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

由于可以用“非”的函数符合，自变量通过“不变”和“非”两种形式，相当于在表 3.2.3 上做 4 种行置换，我们重新将表 3.2.3 通过自变量变换形式推导出来的因变量列放在一起，重新排列如表 3.2.4。形式 A、P 与两个自变量无关；形式 D、M、F、K 只与一个自变量有关；形式 B、C、E、I 在自变量“非”变换下等价，以 B 为代表称为“与”（表示为 $\wedge$ ）；形式 G、J 等价，以 G 为代表称为“异或”（表示为 $\oplus$ ）；形式 H、L、N、O 等价，以 H 为代表称为“或”（表示为 $\vee$ ）。

表 3.2.4 两个变量逻辑函数重排形式

x_1x_2	A	B	C	E	I	D	M	F	K	G	J	H	L	N	O	P
00	0	0	0	0	1	0	1	0	1	0	1	0	1	1	1	1
01	0	0	0	1	0	0	1	1	0	1	0	1	0	1	1	1
10	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1
11	0	1	0	0	0	1	0	1	0	0	1	1	1	1	0	1

什么是逻辑？简单地说，逻辑就是比特函数。前面提到的“非、与、或”等就是人们逻辑思维中常用的词汇。还有一种推理方式为“如果 x_1 ，则 x_2 ”，在逻辑中称为“ x_1 蕴含 x_2 ”（表示为 $x_1 \rightarrow x_2$ ），“ x_1 蕴含 x_2 ”相当于什么函数呢？实际上，它相当于表 3.2.4 中的形式 N，是“或”的等价类，具体可以表示为“ $(\neg x_1) \vee x_2$ ”。

3.2.3 布尔代数

在比特及其函数的基础上，为了更全面系统地研究类似结构的规律、性质，英国数学家布尔提出了布尔代数的概念（代数就是集合及其运算），其定义为：

布尔代数 B 是一个集合 A ， A 至少包含了元素 0（逻辑假）和 1（逻辑真），提供了两个二元运算 $\wedge$ （逻辑与）、 $\vee$ （逻辑或），一个一元运算 $\neg$ （逻辑非），满足下面的定律：

$$\begin{array}{ll}
 \text{结合律} & a \vee (b \vee c) = (a \vee b) \vee c \quad a \wedge (b \wedge c) = (a \wedge b) \wedge c \\
 \text{交换律} & a \vee b = b \vee a \quad a \wedge b = b \wedge a \\
 \text{分配律} & a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c) \quad a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c) \\
 \text{同一律} & a \vee 0 = a \quad a \wedge 1 = a \\
 \text{互补律} & a \vee (\neg a) = 1 \quad a \wedge (\neg a) = 0
 \end{array}$$

布尔代数捕获了集合运算和逻辑运算二者的根本性质，它处理集合运算交集、并集、补集以及逻辑运算与、或、非。最简单的布尔代数就是 0、1 两个元素的集合，以及逻辑与、或、非运算。下面我们说的布尔代数就是指 $(Z_2, \vee, \wedge, \neg, 0, 1)$ 。其中 $Z_2 \in \{0, 1\}$ 。布尔表达式就是由 0、1 元素及其与、或、非运算组成的符号串。可以用布尔表达式表示的函数称为布尔函数。可以证明，任意函数 $f: Z_2^n \rightarrow Z_2$ 都是布尔函数，也就是说，在比特级别上，函数都可以用布尔表达式描述。因此，所有的逻辑推理都可以通过布尔函数来描述，属于布尔代数的范畴。

为了解决故事 1 中的问题，我们采用布尔代数的方式来思考。首先，我们需要引入一个核心概念：命题。命题相当于一类人类陈述语言的编码，命题是能够判断真假的语句，不是说句子本身是否为肯定句、否定句，而是说句子的含义能不能判断真假。例如：“地球外有生命”，这一语句没有人能够判断真伪，因而不能称为命题。而“太阳从东方升起”就是一句命题。命题是不允许模棱两可的。

我们可以把命题用逻辑变量来表示，取值为 0 和 1。把命题 A 、 B 、 C 用逻辑联结词（与非、蕴含、相等）联结起来，就构成了简单的逻辑函数。例如“如果同学愿意听，我就

讲”。看起来很复杂,主语谓语分析起来很麻烦,我们现在做以下抽象:

编码:

A := “同学愿意听”

F := “我讲”

那么以上命题就可以表示为“ $A \rightarrow F$ ”($\neg A \vee F$),就是说 A 能够推出 F 。于是简单的命题 A 、 F 可以通过逻辑复合为复杂的命题。我们再看看更复杂的情况,假设

A := “张三参加会议”

B := “李四参加会议”

F := “我参加会议”

那么它就会有更多表示复杂的逻辑函数:

① 命题“如果张三和李四都参加会议,我就参加会议”

张三、李四都参加会议显然是一个“与”的关系,表示为 $(A \wedge B) \rightarrow F$;

② 命题“如果张三不参加会议并且李四参加会议,我就参加会议”

这也是一个蕴含的关系, A 非且 B 蕴含 F ,表示为 $(\neg A \wedge B) \rightarrow F$;

③ 命题“如果张三李四都不参加会议,我就不参加会议”

我们可以把它写成 $(\neg A \wedge \neg B) \rightarrow \neg F$;

故事 1 中的问题如何把逻辑推理转换成布尔代数。

我假设五个变量 A, B, C, D, E “=1”代表他看电视了,“=0”代表他没看电视。我们再看这五句话:

(1) A 在看电视时, B 也在看: 就是 $A \rightarrow B$;

(2) D 和 E 或两人都在看,或者他们之中有一个人看了: 就是 $D \vee E$;

(3) B 和 C 有且只有一人看了: 就是 $B \oplus C$;

(4) C 和 D 或者两人都看,或者两人都没看: 就是 $\neg(C \oplus D)$;

(5) 如果 E 看了,那么 A 和 D 也看了: 就是 $E \rightarrow (A \wedge D)$ 。

形式化为一组布尔方程组:

$$A \rightarrow B = 1$$

$$D \vee E = 1$$

$$B \oplus C = 1$$

$$\neg(C \oplus D) = 1$$

$$E \rightarrow (A \wedge D) = 1$$

我们无非就是要找一组解,就是布尔变量 $ABCDE$ 分别等于什么时,能满足上述方程组,使得这五个命题都为真。计算机通过解布尔方程就可以完成故事 1 中的逻辑推理。最笨的方法就是通过遍历布尔变量 $ABCDE$ 共 32 种取值排列,就可以求得解。

我们终于通过了一大堆逻辑推理让计算机用“0”和“1”掌握了这样一个推理的能力。我们再看一个更加复杂的逻辑故事:

故事 2: 四个代表队甲、乙、丙和丁进行比赛,观众小张、小李和小王对比赛的胜负问题进行猜测:

张说“甲只能取第三,丙是冠军”;

李说“丙只能取第二,乙是第三”;

王说“丁取第二,甲是第一”。

比赛结束后,对照真正的名字,发现他们都只猜对了一半,请问比赛的名次到底是怎样的?

如何把故事 2 中复杂的问题翻译成布尔代数呢?编码是第一步,采用六个逻辑变量来表示三句话(分前后两个半句)的真和假,分别是: A : 甲取第三; B : 丙是第一; C : 丙是第二; D : 乙是第三; E : 丁取第二; F : 甲是第一。

故事 2 中前三句话很好理解,表示甲、乙、丙三人各说对了一半,就是对应的两个命题变量异或为“1”。但是,这样的逻辑虽然故事 2 中的三句话忠实表达了,但是没有将逻辑变量间固有的逻辑关系表达出来。例如,如果甲得了第三,那么“乙是第三”就是错的,“甲是第一”也是错的。我们需要把这些话的深层含义再表示一下:

P4: A 如果对,那么 D 和 F 一定错。

P5: B 如果对,那么 C 和 F 一定错。

P6: C 如果对,那么 B 和 E 一定错。

P7: D 如果对,那么 A 一定错。

P8: E 如果对,那么 C 一定错。

P9: F 如果对,那么 A 和 B 一定错。

形式化为一组布尔方程组:

$$A \oplus B = 1$$

$$C \oplus D = 1$$

$$E \oplus F = 1$$

$$A \rightarrow (\neg D \wedge \neg F) = 1$$

$$B \rightarrow (\neg C \wedge \neg F) = 1$$

$$C \rightarrow (\neg B \wedge \neg E) = 1$$

$$D \rightarrow (\neg A) = 1$$

$$E \rightarrow (\neg C) = 1$$

$$F \rightarrow (\neg A \wedge \neg B) = 1$$

通过两个逻辑故事可以看出比特与逻辑在处理人类逻辑思维问题上的能力,通过一系列按部就班的“机械式”转换,可以将原本看似高难度的推理问题转换为简单的布尔代数,从而被计算机所解决。过程好像有些舍近求远,实际上,一旦计算机编制了逻辑推理的规则,就可以处理一些很复杂的逻辑问题。例如 Google 搜索中就有成百上千万的正则式逻辑运算支撑着人类社会的海量信息检索。

随着信息爆炸式的增长,海量信息仅仅依靠人脑来处理肯定是远远不够的,要让计算机来代替人工作,就必须通过编码抽象、布尔代数,利用计算机为人类进行计算处理。未来在布尔表达式优化、表达式判断满足、方程求解、验证不同布尔表达式等价等方面都会出现各种各样新的算法。概括地说,通过编码可以用比特来表示不同的事物与状态,代表集合中的元素,作为命题变量。逻辑就是比特上的函数,表示事物与状态间的转换,代表集合上的映射,作为逻辑推理的工具。通过比特与逻辑可以描述一般性的集合与集合上

的各种映射结构,作为代表可以将人的逻辑思维方式转换成了一种计算可以操作的语言:布尔代数,让计算机具有逻辑“思维”能力。

3.3 权重与计算

3.3.1 权重编码

比特可以通过编码的方式来对不同事物加以区分,是一种表示方法,它还可以携带各种相关的信息,如身份证中的出生年月日,IP地址对应的不同地区、机构等。有时需要进一步的抽象,我们不关心集合中具体的元素,而是忽略元素的差异,关心元素的数目。简单地说,就是如何利用比特来表示数?

故事3:一个国王想知道他手下有多少个士兵。大家议论纷纷,提出了很多种数法:

- 最简单的一种是用石子一一对应地数,每人出一个石子堆成石子堆,有多少个士兵就有多少个石子,比较每堆石子的大小就能比较士兵的多少,哪个石堆大,哪队士兵就越多,打仗时就能赢;
- 采用选票时经常用的画“正”字的思想,五个士兵对应一个石子,最后数有多少个石子和剩余未对应的士兵;
- 人天生有十个手指头,满十个石子往上进一位,不同的石子放在不同的位置上代表不同的含义,最低的代表个位,依次为十位、百位、千位……以简单的十进制的方法去数。

那么有没有一种最省石子的计数方法呢?能花费石子最少又能把士兵数清楚。我们可以这样数,类似十进制的方法采用二进制,满两个石子往上进一位,最低位代表 2^0 ,依次为 2^1 、 2^2 、 2^3 、…。十进制集满十个才能往前进一位,要多花九个石子去数一个数。可以证明二进制计数是最省石子的计数方法。

问题描述:试证明对于用 D 位 r 进制表示的整数如改用二进制表示,则需要的二进制位数 $B \leq D(r-1)$ (r 为大于1的整数, D 为正整数)。

证明:用 $\lceil x \rceil$ 表示对 x 上取整,有性质:若 $a > b$ 则 $\lceil a \rceil \geq \lceil b \rceil$

于是有 $B = \lceil \log_2 r^D \rceil = \lceil D \log_2 r \rceil = \left\lceil D(r-1) \frac{\log_2 r}{r-1} \right\rceil \leq \lceil D(r-1) \rceil = D(r-1)$,

证毕。

这就证明了二进制是最省石子的计数方法,从直观上也很好理解,二进制下一个石子就代表了很多个数,2的 n 次方,2的幂次升级是升得最快的一种方式。

故事3说明人们在计数时希望编码不仅能否表示不同的数目,而且希望编码能够比较直观地反映数的大小关系。数的大小关系实际上是集合上“序结构”的一种典型代表。

因此,好的编码必须能够反映集合上的结构,体现元素间的关系。无论是十进制、二进制编码,其核心概念是位权。所谓位权就是不同位置上的数字具有不同的权重,对于二进制而言,就是:

$$n \rightarrow b_{k-1}b_{k-2}b_{k-3}\cdots b_1b_0$$

$$n = \sum_{i=0}^{k-1} b_i 2^i$$

其中, n 是自然数,对应的二进制表示为比特串 $b_{k-1}b_{k-2}b_{k-3}\cdots b_1b_0$,长度为 k 。例如:

$$13 \rightarrow 1101$$

$$13 = 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$

我们知道,比特串是连续整数到比特的函数,每个比特在比特串中的下标就是它的位置,位权就是将位置赋予了对应的权重。这样,比特就有了数的意义。

3.3.2 算术

加减乘除的算术相当于整数集合上的一种代数结构,二进制作作为数字最常规的计算机表示方法,如何完成算术运算呢? 逻辑可以实现任意函数,当然就可以支持算术。算术可以用输入、输出的真值表形式表示,那么任何数值运算(包括正弦、余弦)都可以化简成逻辑运算,区别只是复杂程度的大小。我们从简单的一位运算开始。乘法可以直接对应成与,加法可以对应成异或运算。如

$$\begin{array}{r} + \quad 0 \quad 1 \\ 0 \quad 0 \quad 1 \\ 1 \quad 1 \quad 0 \end{array}$$

$$\begin{array}{r} \times \quad 0 \quad 1 \\ 0 \quad 0 \quad 0 \\ 1 \quad 0 \quad 1 \end{array}$$

可以看出一位的数值运算就是简单的逻辑运算。可以继续推广到多比特上,比如 n 位的加法,下面的例子可以帮助很好地理解:

假定数值运算 $F = A + B$,变量的二进制表示为

$$\begin{aligned} F &= f_{n-1}f_{n-2}\cdots f_0 \\ A &= a_{n-1}a_{n-2}\cdots a_0 \\ B &= b_{n-1}b_{n-2}\cdots b_0 \end{aligned} \tag{3.3.1}$$

则两位二进制加法可通过逻辑运算实现如下

$$\begin{aligned} f_i &= a_i \oplus b_i \oplus c_i \\ c_{i+1} &= (a_i \wedge b_i) \vee (c_i \wedge b_i) \vee (a_i \wedge c_i) \\ c_0 &= 0 \end{aligned} \tag{3.3.2}$$

其中, c 为进位。由于乘法可以转换为移位相加, 乘法也可以通过逻辑运算完成。另外, 我们还可以通过基本的逻辑运算构建比特的比较运算。

$$\begin{aligned} f_i &= (a_i \wedge \neg b_i) \vee ((a_i \oplus \neg b_i) \wedge f_{i-1}) \\ f_{-1} &= 1 \end{aligned} \quad (3.3.3)$$

如: $(A \geq B) = A$;

$$(A \neq B) = A \oplus B;$$

接下来的概念是, 有了这些运算之后怎样和第2章的电路映射上。它有各种各样的组合逻辑, 有两个最基本的表示方法, 一个是最小项, 包含全部变量的与项; 另一个是最大项, 包含全部变量的或项。一个很强的推论就是任何一个函数都可以用最小项或最大项表示进行计算。

数值计算也不是那么简单的。例如, 要问最快最省门的加法器、乘法器、除法器各是什么, 这些化简都是非常困难的, 当然加减乘除运算前人通过长时间努力已经化简得很好了, 那么考查其他运算比如 $a + b + c$ 的连加运算, 也许又需要很长时间去寻求最简化。这就是电路设计的难点, 从逻辑表达式映射成电路要花费很大的代价。

有了组合逻辑就可以计算各种各样的问题, 下面补充一下时序逻辑: 我们算一道复杂的题需要分清步骤, 要有记忆, 这种记忆就是时序逻辑, 可以用时间来代表逻辑。函数的状态不仅与现在的输入有关系, 还与过去的输入有关系, 这就是时序逻辑的概念。时序逻辑器件有计数器、累加器、控制器等, 它最核心的功能是能把状态记录下来, 每个输出不仅与输入有关系还与状态有关系, 以此扩展了计算的能力, 这是很强的特性。

3.4 不确定与信息度量

3.4.1 信息的定义

前面的介绍中, 比特作为集合元素的表示, 而逻辑是用来进行函数计算、处理比特表示的数据。集合元素的比特表示方法可以有很多种, 通过逻辑变换其表现形式更是丰富。如何去刻画表示的效率, 更进一步, 如何来度量集合上的行为? 这里需要引入信息概念, 信息是对事物不确定性的度量, 其单位为比特。它可以反映集合元素通过编码表示的效率, 也可以描述取值于集合上随机现象的不确定度。信息依赖于概率, 我们的世界总是有不确定性的, 存在着各种各样未知的因素。

故事4: 三个考生算命: 三个考生赶考, 途中问一位算命先生考试结果会怎样, 算命先生伸出一根手指头, 暗示考试的结果。

这里注意两点, 算命先生伸出“一根手指头”和“暗示考试结果”。理论上, 算命先生

“一根手指头”如果采用一一映射的原则,只能有一个结果。但是“暗示考试结果”却可以通过多种语言解释,将考试结果一一映射到不同的语言解释上。这样,一根手指就可以映射很多种可能的结果,因此才把算命搞得很玄乎。事实上,三个考生每个可能考上或考不上,一共有八种可能性,一根手指在某些解释下就可以涵盖这八种可能:比如一个考生考上对应3种可能(可以推广到 n 个考生)、有一个没考上也有 $3(n)$ 种可能,都没考上和全都考上各1种。若 n 满足 $1+1+n+n=2^n$ 就能预测全部情况,这里 n 就等于3。如果是4个考生的话,上述一根手指的预测还需想出更多的解释方法。

这里我们又遇到了比特,如果要对三个考生的考试结果编码,虽然有八种可能性,但需要3个比特就够了。这里有什么可以推广呢?我们从此开始概率的旅行。如果有 n 个考生,各有 $1/2$ 的概率考上,那么任意一种结果的概率都是 $1/2^n$ 。对于等概率事件,推广之, 2^n 种可能,每个用0和1来表示,就是 $-\log_2 1/2^n = n$ 个比特。推广一下,对等概率事件用 $-\log_2 P$ 来表示,如果不是等概率的,那么需要作一个概率上的平均为 $\sum_{i=1}^N -p_i \log_2 p_i$ 。我们从概率的角度找到了一种衡量它复杂程度或者说不确定度的方式。若共有4种可能,则2个比特就够了,16种可能需要4个比特,可能性越多,比特数越多。反过来说,比特数越多,可能性也越多。这就表明了一种集合测度,这种测度有什么用?它是对不确定性的本质刻画,在某些地方会产生意想不到的结果。

3.4.2 信息的作用

信息概念的引入对信息学科有着重要的意义,后面章节将有更为详细的讲解。我们先来看一道“奥数故事”。

故事5:造出27个球,其中知道有且仅有一个小球不合格,重量偏轻。给定一个天平可以称出两边的轻重和平衡,怎么称可以找出那个轻的小球?再问,如果不合格的小球既有可能重,也有可能轻,但一定不等重,问称三次最多可以从多少个小球中找到这个不合格的小球并知道其是轻还是重?

混到27个球中已经知道重量不合格的球是偏轻,那么称三次就能把它找出来。这个问题大家都有办法解决。第二部分难一点,如果不知道偏轻还是偏重,那么称三次总球数的极限一般说是12个,还有人挑战难度到了13个,这些数到底是从哪儿来的?学了信息论就很容易了解。比如27个球,27种可能性,很容易想它的不确定度就是 $\log_2 27$,这是球的不确定性。这个不确定性是靠每次称量来减少的,每次称量理想地有三种可能:左边轻、右边轻、一样轻重,就是 $\log_2 3$,此即每次测量能够减少的不确定度。两者相除很容易得到是3次称量。这样信息论就告诉你称3次,到此为止就可以得出结果。这是很宏观的解释,其实它还有深入的解释。信息概念还能指导称的方法与步骤:每次称量时左边轻、右边轻、一样轻重的概率都是 $1/3$ 时,得到的信息量最大,一旦偏离,得到的信息量就会减少,这样就不一定能在三次内称完。例如有人第一次称时左右各放一个球,这样一

样轻重的概率显然将非常大。

故事 5 的第二部分问如果不知道不合格球轻重,那么极限是什么? 12 还是 13? 我们同样可以从信息的角度去看,现在我们不仅要知道是哪一个球还要知道轻重,可以证明称三次的最好是 13 个,证明如下:

$$\begin{aligned}\log_2(2n) &\leq 3\log_2 3 \\ n &\leq 13.5\end{aligned}\quad (3.4.1)$$

如果没有信息的基本概念,证明这道题将会非常困难。

学了信息概念再回过头看,27 个球称法大家都会。我们现在用信息概念、进制和数字电路实践给出一个不一样的方法。我们把球从 0~26 赋予三进制的编码,当然不可能用比特来表示,我们用 0, L, R 来表示。天平称重时 0 代表不放, L 代表这个球放在左盘, R 代表放在右盘,每一次称依次对应一位,恰好每次称量时将球平均分配。若三次都是一样重,那么编号 000 就是第 0 号球将是不标准球;若对应 00L 就是对应编码的第 1 号球。它的称重结果就与它的编码一一对应。

我们还可以把天平的结果送给二进制电路,就可以用二进制给球标号,然后把三进制的思想代入进去,将称完的结果输入这样的电路就能显示最终结果,如图 3.4.1 所示。这是一个信息学科最简单的系统,但它也蕴含了我们信息学科的思想:怎样用信息代表不确定性、怎么用数值代表不同的编码、通过运算怎样把功能映射到 $\{0,1\}$ 比特上。

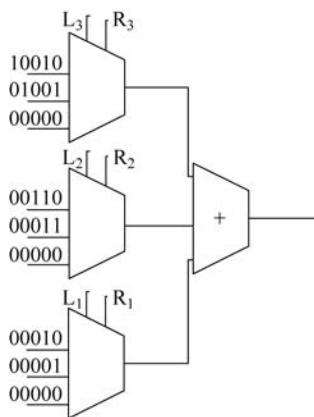


图 3.4.1 称小球电路

通过上例就能简要介绍完比特、逻辑、信息这三个概念。它们的关系如图 3.4.2 所示。比特是对事物的抽象编码,是集合元素的表示。由于集合元素之间存在各种关系,形成了代数结构、序结构等,通过逻辑完成了一般函数的功能,可以实现不同的集合结构。针对集合处理面临的不确定性,信息是对不确定性的一种测度,通过信息的单位比特可以衡量事物的不确定性。在此核心概念上,对于集合元素,当其存在复杂的性质和结构时,需要将比特串拓展为数据结构;对于复杂的函数、结构上的处理,需要进一步设计算法来实现;对于信息的传递,需要发展通信理论。

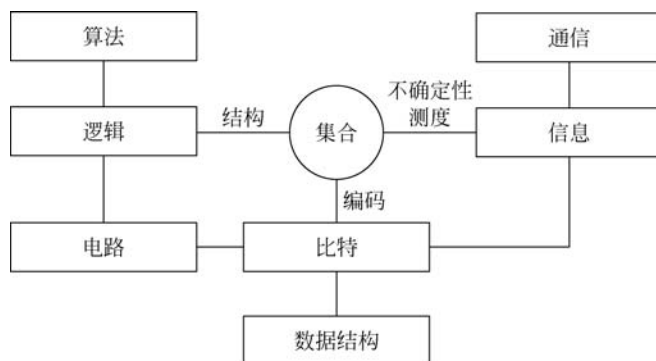


图 3.4.2 比特概念关系图

参考文献

- [1] Rosen K H. 离散数学及其应用. 袁崇义, 屈婉玲, 张桂芸, 译. 北京: 机械工业出版社, 2011.
- [2] Cover T M, Thomas J A. 信息论基础. 阮吉寿, 张华, 译. 北京: 机械工业出版社, 2008.
- [3] Katz R H, Borriello G. 现代逻辑设计. 罗嵘, 刘伟, 罗洪, 等. 北京: 电子工业出版社, 2006.
- [4] Petzold C. 编码: 隐匿在计算机软硬件背后的语言. 左飞, 薛佟佟, 译. 北京: 电子工业出版社, 2010.