文章编号:1009-315X(2015)05-0504-04

群的判断算法设计

姜 楠,张富彬,宁春芳
(大连民族大学 计算机科学与工程学院,辽宁大连 116605)

摘 要:介绍了代数系统和群的定义以及群在计算机等领域的应用,设计了对给定集合与运算是否构成代数系统、给定的代数系统是否为半群、半群是否能够构成独异点、独异点是否能够构成群的判断算法,并进行了算法分析,完成了群的判断系统流程图;并通过Java语言实现该系统,把抽象难以理解的代数系统中的群论问题通过形象直观的程序软件表现出来。

关键词:群的判断;算法设计;系统流程图
中图分类号:O158 **文献标志码**:A

Design of Group Judgment Algorithm

JIANG Nan, ZHANG Fu-bin, NING Chun-fang
(College of Computer Science and Engineering, Dalian Nationalities University, Dalian Liaoning 116605, China)

Abstract: The definition of algebra system and group, and the applications of group in the field of computer and others are introduced. We design a given set and operation whether they constitute an algebra system, whether the given algebraic system is the semigroup, whether the semigroup can constitute a monoid, and whether a monoid can constitute the algorithm of judgment for the group. Then we analyze the algorithm and complete the flow chart of the groupjudgment system. The system is implemented through Java language, which makes the algebraic system theory, which is abstract and difficult to understand, be shown by a visual and intuitive software program.

Key words: judgment for the group; algorithm design; system flow chart

群论是研究群的结构及其应用的数学理论,是代数系统的重要分支,它不仅在物理学、化学、力学、生物学中有着广泛的应用,其应用范围也深入到科学技术的各个领域[1-2]。尤其是在计算机科学领域的研究和应用中,群论已成为非常重要的工具。而且群论也是密码学的重要理论基础,例如组合群论中有些基本问题相对于某个特定的群是困难问题,可以作为构造公钥密码体制的基础[3],还有一些对称加密算法和非对称加密算法都是以群论为理论基础的。群的理论比较抽象难以理解,本文设计了一个判断群的仿真系统。首先设计了对代数系统进行判断的算法,进而设计出判断给定的代数系统是否为群的算法,最后通过Java程序设计实现了群的判断系统。

1 系统原理

代数,也称代数结构或代数系统,是指定义有若干运算的集合。

定义1:非空集合S和S上k个一元或二元

收稿日期:2015-04-13;**最后修回日期**:2015-05-13
基金项目:全国工程专业学位研究生教育自选课题(2014-JY-106);国家民委科研项目(14DLZ012)。
作者简介:姜楠(1964-),女,山东龙口人,教授,博士,硕士生导师,主要从事信息安全研究。
通讯作者:张富彬(1992-),男,辽宁朝阳人,大连民族大学硕士研究生,主要从事信息安全研究。

运算 f_1, f_2, …, f_k 组成的系统称为一个代数系统, 简称代数。记作 $<S, f_1, f_2, \cdots, f_k>$[4]。

定义 2:群 $<G, *>$ 是一个代数系统,其中二元运算 $*$ 满足以下 3 条:

(1)结合律,即对所有的 a, b, $c \in G$,有

$a*(b*c) = (a*b)*c$ (满足结合律的代数系统为半群);

(2)含幺元,即存在一个元素 e,对任意元素 $a \in G$,有(含幺半群称为独异点);

$a*e = e*a = a$

(3)存在逆元,即对每一个 $a \in G$,存在一个元素 $a^{-1} \in G$,使

$a^{-1}*a = a*a^{-1} = e$(称 G 为群);

简单地说,群是一个具有可结合运算,存在幺元,每个元素存在逆元的代数系统[4]。

2　算法设计

2.1　代数系统的判断

代数系统的判断就是通过用户自定义的集合和运算表,判断给定的运算在相应的集合上是否封闭,如果封闭,则上述集合与运算构成代数系统,否则不能构成代数系统。判断运算封闭的函数为 judgeAlgebraicSystem(),对于给定的运算表,如果运算是封闭的,返回 true,否则返回 false。将给定的运算表中的元素和集合中的元素依次做对比验证,如果运算表中的元素均属于此集合,则此运算是封闭的。算法 2.1 具体描述如下:

(1) 给定 n 个元素的 List 类型的集合 set,给定 n 行 n 列的 List 类型的二维运算表 operationTable,计数器 count = 0,运算表循环变量 $i=0$, $j=0$,集合循环变量 $k=0$;

(2) 验证运算表中所有的元素是否属于该集合,依次取出运算表中第 i 行第 j 列元素,与集合 set 中元素对比,通过语句 operationTable.get(i).get(j).equals(set.get(k))进行判断。如果存在相等,则计数器 count ++,并且跳出 k 层循环,$j=j+1$, $i=i+1$;否则 k 层循环结束后 $j=j+1$, $i=i+1$;

(3) 直到循环结束将运算表中所有元素验证完毕,执行(4),否则执行(2)

(4) 若 count 的值与运算表中元素数量相等,则构成代数系统,返回 true,否则不能构成代数系统,返回 false。

2.2　判断给定的代数系统是否为半群

在已知给定的系统是代数系统的基础上,判断此代数系统是否为半群的函数为 judgeCombination(),根据结合律公式$(a*b)*c=a*(b*c)$设计算法,首先求出等式左侧前两个元素作用的值,然后取其值的下标,再与第三个元素进行运算,得出结果;然后求出等式右侧后两个元素作用的值,并取其值的下标,使第一个元素与之运算,得出结果,将两次的结果进行比较如果相等返回 true,如果不相等返回 false。算法 2.2 具体描述如下:

(1) 给定 n 个元素的 List 类型的集合 set,给定 n 行 n 列的 List 类型的二维运算表 operationTable,分别初始化代表三个元素的循环变量 $i=0$, $j=0$, $k=0$;

(2) 计算前两个元素运算的结果 operationTable.get(i).get(j),暂存 *temp*1 变量中,计算出 *temp*1 的值在集合中的地址下标 set.indexOf(*temp*1),暂存 add1 变量中;

(3) 进入 k 层循环,计算后两个元素作用的结果 operationTable.get(j).get(k),暂存 *temp*2 变量中,计算出 *temp*2 的值在集合中的地址下标 set.indexOf(*temp*2),暂存 add2 变量中,执行(4);

(4) 验证前两个元素运算的结果 *temp*1 与第三个值运算的值,同第一个元素与后两个值运算的值 *temp*2 运算的值是否相等,通过语句 operationTable.get(add1).get(k). equals(operationTable.get(i).get(add2))进行判断,如果两次运算的值不相等,则代数系统不满足结合律,返回 false,结束程序;如果两次运算的值相等,则 $k=k+1$, $j=j+1$, $i=i+1$;

(5) 直到所有循环运行结束,执行(6),否则回到(2);

(6)代数系统满足结合律,代数系统是半群,返回 true。

2.3　判断半群是否为含幺半群

在给定的代数系统是半群的基础上,判断其是否为含幺半群,这个判断函数为 judgeIE(),在半群中存在单位元则为含幺半群也称为独异点。对集合中任意元素 a,如果有 $a*e=a$, $e*a=a$,则此半群中存在单位元 e。

算法 2.3 具体描述如下:

(1) 给定 n 个元素 List 类型的集合 set,给定 n 行 n 列的 List 类型的二维运算表 operationTable,循环变量 $i=0$;

(2) 进入循环,计数器 count = 0,循环变量 j = 0;

(3) 如果集合中第 i 个的元素与第 j 个元素运算的值等于第 j 个元素,并且第 j 个元素与第 i 个元素运算的值也等于第 j 个元素,用语句 operationTable. get (i). get (j). equals (set. get (j)) &&operationTable. get (j). get (i). equals (set. get (j)) 进行判断,如果成立 count + + , $j = j + 1$;

(4) 如果 j 层循环完毕,判断 count 的值是否等于集合的长度,如果相等,表明此时存在单位元,此半群是含幺半群,并且将单位元 set. get(i) 返回,程序结束;否则 $i = i + 1$;

(5) 直到循环结束,执行(6),否则回到(2);

(6) 代数系统中不存在单位元,返回 false。

2.4 判断含幺半群是否为群

在给定的代数系统是含幺半群的基础上,判断其是否为群的函数是 judgeInverseElement( ),若在含幺半群中每一个元素都存在逆元,此含幺半群为群,对代数系统任意的 a 存在 $a * a^{-1} = e$, $a^{-1} * a = e$, a^{-1} 属于集合 set,则此元素存在逆元。算法 2.4 具体描述如下:

(1) 给定 n 个元素 List 类型的集合 set,给定 n 行 n 列的 List 类型的二维运算表 operationTable 与单位元 ie,设置计数器 count = 0,循环变量 i = 0, j = 0;

(2) 利用运算表,依次取出运算表中第 i 行 j 列元素, 验证集合中第 i 个元素与第 j 个元素运算的值,同第 j 个元素与第 i 个元素运算的值是否同时为单位元,通过语句 operationTable. get(i). get(j). equals (ie) &&operationTable. get (j). get (i). equals(ie) 判断,如果所得的两个值同时为单位元,则计数器 count + + ,否则 $j = j + 1$, $i = i + 1$;

(3) 直到循环结束,执行(4),否则回到(2);

(4) 如果 count 的值与集合长度相等,表明所有的元素均具有逆元,含幺半群是群,返回 true,否则表明某个元素不存在逆元,含幺半群不是群,返回 false。

3 系统实现流程

本系统是通过 Java 语言编程实现的。对于一个非空集合 G 以及定义在 G 上的代数运算所构成的系统,判断 < G, * > 其是否为代数系统,首先需要给定集合 set,以及定义在集合上的运算构成的运算表 operationTable,通过类 JudgeAlgebreicSystem 声明对象 jas,调用函数 judgeAlgebreicSystem(operationTable, set),通过算法 2.1 判断运算是否封闭,如果返回 true,则运算封闭,输出“运算封闭,是代数系统”,程序继续执行,如果返回 false,运算不封闭, < G, * > 不是代数系统,输出“不是代数系统”,程序结束。

在满足代数系统的基础上,通过类 JudgeCombination 声明对象 jc,调用 judgeCombination(operationTable, set),通过算法 2.2 判断代数系统是否满足结合律,如果程序返回 true,则表明代数系统满足结合律,此时代数系统是半群,输出“运算可结合,此代数系统是半群”,否则返回 false,代数系统不满足结合律,输出“运算不可结合,此代数系统不是半群”,程序结束。

在满足半群的基础上,通过类 JudgeIE 声明对象 jie,调用 judgeIE(operationTable, set),通过算法 2.3 判断半群是否含有单位元,如果存在,函数将单位元返回用 result 接收,并输出“单位元,此代数系统是含幺半群”,否则返回 false,输出“此代数系统不存在单位元,不是含幺半群”,程序结束。

在满足含幺半群的基础上,通过类 JudgeInverseElement 声明对象 jie2, 调用 judgeInverseElement(operationTable, set, result),通过算法 2.4 验证是否每个元素均存在逆元,如果返回 true,则表明所用元素均存在逆元,输出“所用的元素均存在逆元,此代数系统是群”,否则返回 false,输出“部分元素不存在逆元,代数系统不是群”,程序结束。

系统实现流程图如图 1 。

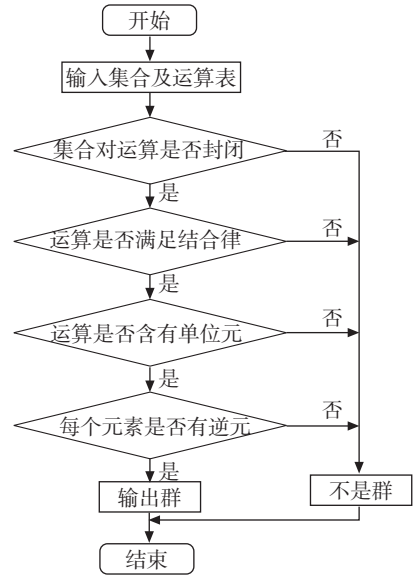

图 1 系统流程图

(下转第 521 页)

3　存在的问题与对策

通过几年的酶工程实验教学改革,实践表明,新的教学方式锻炼了学生自主查阅文献、设计实验方案的能力,提高了学生对实验课的兴趣和重视程度,有益于培养学生的团队合作精神。95 % 以上的学生对这种教学模式表示欢迎和肯定。但仍存在着一些问题:(1)学生之间自学能力和动手能力差别较大。虽然大部分学生表现很好,但仍有些学生的主动性不高,自学能力不够,不能独立完成实验的设计和操作。这就要求教师不能完全放手,对基础较差的学生应及时鼓励,亲自指导,帮助他们完成实验。(2)学生分析数据的能力不足。一部分学生只是把实验数据简单的罗列出来,没有进行数据分析和结果讨论,而分析和讨论恰恰是最重要的部分。因此,教师应加强指导学生对数据分析、结果讨论方面的练习,学会总结实验成败的关键因素。(3)由于改革后的酶工程实验时间连贯性较强,每一大组学生都是连着上实验课,因此在时间安排上,尽可能避免与其他实验课程发生冲突[7]。

总之,通过对酶工程实验教学的一系列改革措施,培养了学生实事求是、严肃认真的科学态度,提高了学生分析问题、解决问题的能力,并进一步提高了学生的科学素养和创新精神,从而达到了培养应用型创新人才的目的。

参考文献:

[1] 康静,刘玉青,关建义,等. 加强生物工程专业酶工程实验教学改革[J]. 安徽农业科学,2011,39(23):14434 – 14435.
[2]韩鸿鹏,成庆利,王丁,等. “实验助教”模式在酶工程实验教学中的应用[J]. 高师理科学刊,2013,33(2):103 – 106.
[3]周念波,李轶群,涂绍勇,等. 酶工程实验项目化教学改革探索[J]. 广东化工,2014,41(2):147 – 148.
[4]黄时海,韦春葵,杨洋,等. 酶工程实验教学的改革与实践[J]. 中国科教创新导刊,2011,25:122,124.
[5]石陆娥,章志量,沈波,等. 酶工程实验教学模式创新初探[J]. 健康研究,2011,31(3):234 – 235.
[6]吴士筠,魏艳芬,乐薇. 生物工程专业酶工程技术实验教学模式改革探索与实践[J]. 科教导刊,2014,3:122 – 123.
[7]陈文伟,刘明启,申屠旭萍. 酶工程原理课程中实验教学模式改革的探索[J]. 高等函授学报:(自然科学版),2012,25(1):39 – 40.

(责任编辑　邹永红)

(上接第 506 页)

4　结　论

群论是离散数学课程的重要组成部分,也是一种非常重要的代数系统,在很多领域都有应用,尤其是在计算机和通信以及信息安全领域有更为广泛的应用。本文主要研究给定集合与运算是否构成代数系统、是否构成半群和独异点,对给定的代数系统是否构成群的判断系统的原理与算法设计,并且编程实现了群的判断系统。该系统把抽象难以理解的代数中的群论问题通过形象直观的程序软件表现出来,不仅可以帮助学生更好的理解书本上学过的抽象的难以理解的代数系统理论,还可以提高学生的数学建模能力、算法分析设计能力和程序设计能力。既提高了学生各方面的能力,又培养了学生的学习兴趣,可以很好的提高教学质量。

参考文献:

[1] 李奴义. 浅议群论在化学中的应用[J]. 青海师范大学民族师范学院学报,2012,23(1):95 – 96.
[2] 何劼. 用群论的基础知识理解信号处理中的一些基本概念[J]. 中央民族大学学报(自然科学版), 2007, 16(3):259 – 261.
[3] 汤学明,洪 帆,崔国华. 辫子群上的公钥加密算法[J]. 软件学报,2007,18(3):722 – 728.
[4] 屈婉玲,耿素云,张立昂. 离散数学[M]. 北京:清华大学出版社,2014.

(责任编辑　王楠楠)