Computational Tools for Group Theory

Jeffrey Barr
Candidate for MS in Computer Science
San Diego State University
Spring 2005

Areas of Discussion

- Goals of Thesis
- Introduction to the Program
- Basic Group Theory
- Code Capabilities
  - Generation
  - Identification
  - Analysis
- Proposed future work

Goals of Thesis

- Update code originally developed by David Gibbs
- Expand capability of code to make identification more flexible
- Extend functionality and analysis capabilities available to the user.

Introduction to the Program

- Java code with Swing User Interface
- All groups stored in a JTable that represents the Cayley Table for a group
- Buttons separated
  - Generation
  - Identification and Analysis

Group Theory Basics

- Number of elements in a group is the **order** of a group
- The **identity** element e in group G results in ae=ea=a for all elements a in G.
- The **order of an element** g in group G is the smallest integer n such that $g^n = e$.

Group Theory Basics (continued)

- **Abelian Group**: A group where all elements in the group commute or for all elements a and b in group G, ab = ba.
- **Center** of a group is composed of the elements of a group that commute with all other elements in the group.
- A subset of elements in group G is a **subgroup** of G if they form a group under the same binary operation as G.
- A subgroup H is a **normal subgroup** of group G it commutes with all elements in G.

Group Theory Basics (continued)

- **Isomorphism**: A function ϕ mapping a group G to group H such that:
  - ϕ is a function from G->H
  - $\phi(ab) = \phi(a)\phi(b)$ for all a,b in G
  - ϕ is bijective
- **Automorphism**: An isomorphism of group G onto itself.
- The set of all automorphisms of group G is a group **Aut(G)**.

Code Capabilities

- Generate groups
  - Cyclic Groups
  - Defined Relationships
  - Cross Products
  - Manually entered by the user
- Identify groups
- Analysis of groups

Group Generation - Cyclic Groups

- Generated by a single element
- Result of combining elements calculated via modulus arithmetic
- Example Z_7 Group

Group Generation – Defined Relationships

- Multiple generators with relationships describing how substitutions are performed
- Capable of creating all groups including Abelian groups
- Example <2, 2, 4> or Quaternion group
  - 2 generators, order 4 and 2
    - aaaa = e
    - bb = aa
    - ba = aaab

Group Generation – Cross Products

- Combining two groups into one
- Combination pairs are created that represents the new elements in the newly generated group
- Binary operations are performed independently on the elements in the pair
- Example Z_2 x Z_4
  - Elements (0, 1) and (0, 1, 2, 3)
  - Combination pairs {(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)}
  - (0,2) * (1,3) = (1,1) or 2*7 = 5

Group Identification

- Only identification of finite groups
- Element order structure is key
- Two basic analysis methods used
  - Fundamental Theorem of Finite Abelian Groups
  - Non-Abelian Group order structure and other characteristics
- Shortcuts for groups of particular order or order structure

Code Process

- Determine if table displayed is a group
- Determine order of all the elements
- Check groups against shortcut operations
- Determine if the group is Abelian
  - Yes: Use Fundamental Theorem of Finite Abelian Groups
  - No: Use order structure and other characteristics

Fundamental Theorem of Finite Abelian Groups

"Every finite Abelian group is the direct product of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group."

Identifying Abelian Groups

- Calculate the number of Abelian groups through isomorphism using the Fundamental Theorem
- Code utilizes a form of the "Greedy Algorithm for an Abelian Group of order p^n" in order to identify the Abelian Groups

Greedy Algorithm Examples

- Group $Z_4 \times Z_2 \times Z_2$
- Group Order = 16
- Number of elements of each order:
  - Order 16: None
  - Order 8: None
  - Order 4: 8
  - Order 2: 7
  - Order 1: 1

- Group $Z_4 \times Z_4$
- Group Order = 16
- Number of elements of each order:
  - Order 16: None
  - Order 8: None
  - Order 4: 12
  - Order 2: 3
  - Order 1: 1

Non-Abelian Groups

- 41 of 45 non-Abelian groups of order 2 to 31 could be identified based upon unique order structure of elements
- Remaining 4 non-Abelian groups could be identified based upon group center and normality of subgroups.
- 10 of 45 non-Abelian groups of order 32 had unique order structure

Example: Groups of order 24

	Elements of Order						
Name	***1***	***2***	***3***	***4***	***6***	***8***	***12***
<-2, 2, 3>	1	1	2	2	2	12	4
Quaternion x Z3	1	1	2	6	2	0	12
<2, 2, 6>	1	1	2	14	2	0	4
<2,3,3>	1	1	8	6	8	0	0
<2,2,3> x Z2	1	3	2	12	6	0	0
D4 x Z3	1	5	2	2	10	0	4
D3 x Z4	1	7	2	8	2	0	4
A4 x Z2	1	7	8	0	8	0	0
<4, 6 | 2, 2>	1	9	2	6	6	0	0
S4	1	9	8	6	0	0	0
D12	1	13	2	2	2	0	4
D6 x Z2	1	15	2	0	6	0	0

Shortcuts in Identification

- Cyclic groups are only groups with at least one element whose order equals the order of the group.
- Groups of the order p^2, where p is prime, are either cyclic or a cross product of groups Z_p.
- Groups of order 2*p, where p is prime, are either cyclic or a dihedral group D_p.

Analysis Tools

- Group
  - Determine if the table has a left (row) and right (column) identity element and if they are equal. [O(n^2)]
  - Determine if every element in each row and column of the table has an inverse element. [O(n^2)]
  - Determine if every element is associative with every other element in the table. [O(n^3)]
- Abelian
  - Check if the table forms a group using the process above.
  - Check if every element in each row column combination is commutative. [O(n^2)]
- Inner Automorphism

Inner Automorphism

- For elements a, b in group G, the **conjugation** by a of b is the mapping $\phi_a(b) = a\,b\,a^{-1}$.
- This mapping is a special type of automorphism whereby ϕ_a is called an **inner automorphism** of G.
- The set of all inner automorphisms of G form a group **Inn(G)**.

Inner Automorphism Group

- Determine inner automorphism for each element in the group. [$O(n^3)$]
- Each unique inner automorphism represents an element in Inn(G). [$O(n^4)$]
- Two of the new elements a, b in the inner automorphism group are combined by calculating ($a\ b\ x\ b^{-1}\ a^{-1}$) for every x in G. [$O(n^4)$]
- The result is compared to all of the new elements in Inn(G) to determine the element that results from the combination. [$O(n^5)$]

Work for the future

- Expand analysis functions
  - Normality of Subgroups
  - Center of a group
  - Determination of Aut(G)
  - Isomorphism test between groups
- Expand Identification Code
  - More shortcuts (i.e. groups of order pq)
  - Expand the list of groups identified

Acknowledgements

- Dr. Carl Eckberg – Thesis Advisor
- Mr. William Root – Thesis Committee
- Dr. Marcus Greferath – Thesis Committee

Computational Tools for Group Theory

Jeffrey Barr
Candidate for MS in Computer Science
San Diego State University
Spring 2005