A Study Of Games Over Finite Groups
Liljana Babinkostova, Samuel Coskey, Dan Kondratyuk, Scott Navert, Stephanie Potter and Marion Scheepers
BOISE STATE UNIVERSITY

Introduction

Finite groups are mathematical platforms for modern cryptography. Security protocols are often vulnerable to subtle exploits. A well-chosen group can be used to foil these exploits. To identify suitable groups, attack scenarios are modeled by two-player games. This research focuses on two classes of such games. For one class of games we give a complete analysis over finite Abelian groups. We report partial results for non-Abelian groups and for the other class of games.

Game Theory

Game theory is the formal study of decision making. All games in this study satisfy the hypotheses of Zermelo’s Theorem [2]:
• The game has two players, named ONE and TWO.
• Each player has perfect information about every aspect of the game.
• The length of the game is finite.
• Each play of the game results in a win for one player.

For such games, one of the players has a winning strategy.

The “Avoid the identity” Game

For group \((F, *)\), the “avoid the identity” game, \(\text{ID}(F, *)\), is as follows:
• ONE and TWO alternately pick previously unused members of \(F\).
• The player whose selection causes the group product of all members chosen thus far to be the group identity, loses.

Example on \(Z_5 = \{0,1,2,3,4\}\)

ONE and TWO play \(\text{ID}(Z_5 + \text{mod } 5)\).

<table>
<thead>
<tr>
<th>Turn</th>
<th>ONE</th>
<th>TWO</th>
<th>Sum (mod 5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

Player TWO wins this play of \(\text{ID}(Z_5 + \text{mod } 5)\).

The “On my turf” Game

For group \((F, *)\), a subset \(A\) of \(F\), and positive integer \(m\), the “on my turf” game, \(\text{MT}(F, \cdot, A)\), is as follows:
• The game has \(m\) rounds.
• In round \(r \leq m\) ONE picks a previously unused element \(a_r\). Then TWO picks a previously unused element \(b_r\).
• The game ends either when all elements have been chosen, or when the \(m\)-th round is complete.
• ONE wins if \(a_1 \cdot b_1 \cdot a_2 \cdot b_2 \cdot \ldots \cdot a_m\) is in \(A\). Else, TWO wins.

The Game Tree for \(\text{MT}(D_4, \cdot, A)\)

Player ONE has a winning strategy if, and only if, \(0\) is an element of the subset of \(Z_4\) corresponding to \(A \subseteq D_4\).

Research Objectives

For each of the two classes of games on finite groups:
• identify the groups for which the game satisfies Zermelo’s hypotheses.
• when the game satisfies Zermelo’s hypotheses, determine when player ONE has a winning strategy.

Results for Finite Abelian Groups

For Abelian groups of even order, the theory is more delicate.

The even order theorem

If \((F, *)\) is an Abelian group such that \(|F|\) is an even number then:
• The game \(\text{ID}(G, *)\) satisfies the hypotheses of Zermelo’s Theorem.
• Player TWO has a winning strategy in the game \(\text{ID}(F, *)\).
• Player ONE has a winning strategy in the game \(\text{MT}(F, \cdot, A)\) if, and only if, the identity element is a member of \(A\).

The odd order theorem

If \((F, *)\) is an Abelian group such that \(|F|\) is an odd number then:
• The game \(\text{ID}(G, *)\) satisfies the hypotheses of Zermelo’s Theorem.
• Player TWO has a winning strategy in the game \(\text{ID}(F, *)\).
• Player ONE has a winning strategy in the game \(\text{MT}(F, \cdot, A)\) if, and only if, the identity element is a member of \(A\).

Finite dihedral groups, \(D_n\), are defined as follows by generators and relations:
\[D_n = \langle r, s | r^n = s^2 = 1, (rs)^2 = 1 \rangle\]
These are non-abelian groups. Already for these groups the research objectives are con-
ected with significant mathematical problems.

A Study Of Games Over Finite Groups
Liljana Babinkostova, Samuel Coskey, Dan Kondratyuk, Scott Navert, Stephanie Potter and Marion Scheepers
BOISE STATE UNIVERSITY

References


Acknowledgements

This research was supported by the National Science Foundation under Award No. DMS-1062857, as well as by Boise State University.