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, $\mathsf{ID}(F, *)$, is as follows:

- ONE and TWO alternately pick previously unchosen 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 $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$

ONE and TWO play $\mathsf{ID}(\mathbb{Z}_5, + \mod 5)$.

Turn	ONE	TWO	Sum (mod 5)
1	2		2
2		4	1
3	3		4
4		0	4
5	1		0

Player TWO wins this play of $\mathsf{ID}(\mathbb{Z}_5, + \mod 5)$.

The "On my turf" Game

For group $(F, *)$, a subset A of F, and positive integer m, the "on my turf" game, $\mathsf{MT}_m(F, *)$, is played as follows:

- The game has m rounds
- In round $i \le m$ ONE picks a previously unchosen element o_i. Then TWO picks a previously unchosen element t_i.
- The game ends either when all elements have been chosen, or when the m-th round is complete.
- ONE wins if $o_1 * t_1 * o_2 * t_2 * \cdots$ is in A. Else, TWO wins.

The Game Tree for $\mathsf{MT}_4(\mathsf{D}_4, \circ, A)$

For a dihedral group $(\mathsf{D}_n, \circ)$ and specified subset A, analysis of the game $\mathsf{MT}(\mathsf{D}_n, \circ, A)$ depends on a corresponding addition-subtraction version of the "on my turf" game played on $\mathbb{Z}_n$, with a corresponding choice for the set A. The game tree in Figure 1 represents the legal moves in the "on my turf" game corresponding to $\mathsf{MT}_4(\mathsf{D}_4, \circ, A)$.

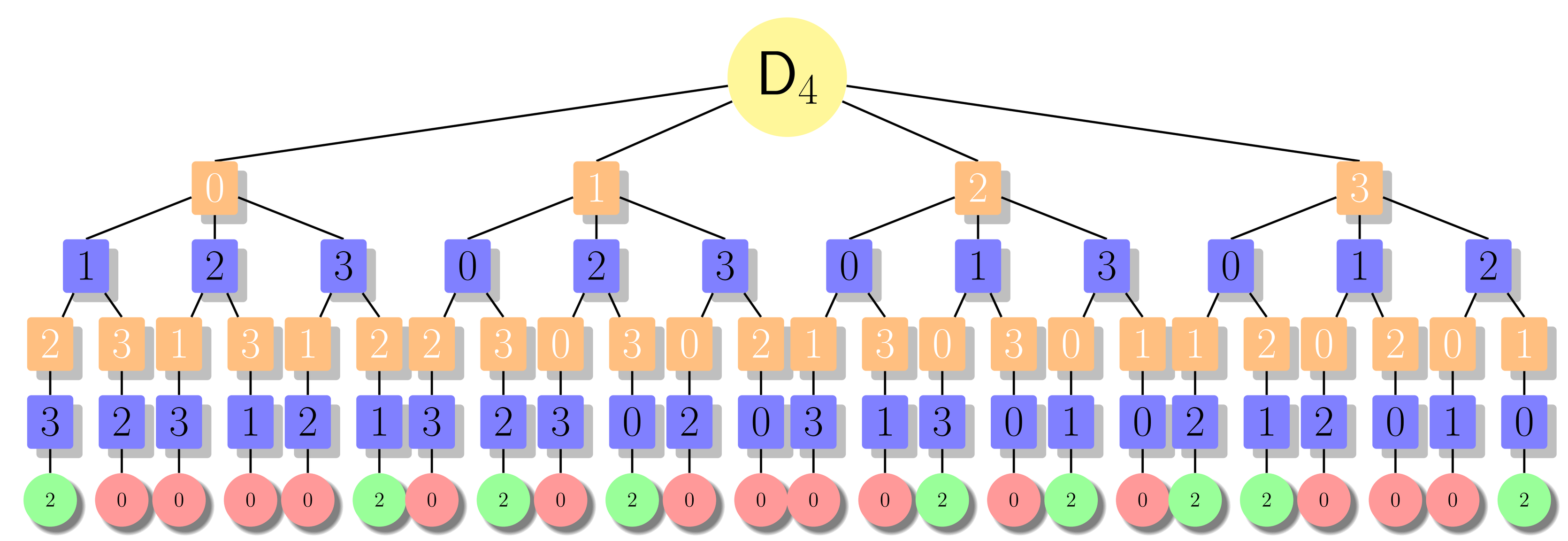

Figure 1: Game Tree for D_4: Player ONE positions are in orange, player TWO positions are in blue.

Player ONE has a winning strategy if, and only if, 0 is an element of the subset of $\mathbb{Z}_4$ corresponding to $A \subseteq \mathsf{D}_4$.

Research Objectives

For each of the two classes of games on finite groups,

1. identify the groups for which the game satisfies Zermelo's hypotheses.
2. when the game satisfies Zermelo's hypotheses, determine when player ONE has a winning strategy.

Results for Finite Abelian Groups

The odd order theorem

If $(F, *)$ is an Abelian group such that $|F|$ is an odd number then:

1. The game $\mathsf{ID}(G, *)$ satisfies the hypotheses of Zermelo's Theorem.
2. Player TWO has a winning strategy in the game $\mathsf{ID}(F, *)$.
3. Player ONE has a winning strategy in the game $\mathsf{MT}(F, *, A)$ if, and only if, the identity element is a member of A.

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:

1. The game $\mathsf{ID}(F, *)$ satisfies the hypotheses of Zermelo's Theorem if, and only if, no subgroup of $(F, *)$ is isomorphic to the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.
2. If the game $\mathsf{ID}(F, *)$ satisfies the hypotheses of Zermelo's Theorem, then player ONE has a winning strategy in the game $\mathsf{ID}(F, *)$.
3. If $(F, *)$ has a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, ONE has a winning strategy in $\mathsf{MT}_{\frac{|F|}{2}}(F, *, A)$ if, and only if, the identity element of F is in A.
4. If $(F, *)$ has no subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, ONE has a winning strategy in $\mathsf{MT}_{\frac{|F|}{2}}(F, *, A)$ if, and only if, a non-identity element a with $a * a$ the identity, is in A.

The finite Dihedral Groups

Finite dihedral groups, D_n, are defined as follows by generators and relations:

$$\mathsf{D}_n = \langle r,\ s | r^n = id,\ s^2 = id,\ (rs)^2 = \mathrm{id} \rangle.$$

These are non-abelian groups. Already for these groups the research objectives are connected with significant mathematical problems.

An example of "my turf" game on D_4

Turn	ONE	TWO	Value in D_4
1	s	sr^2	r^2
2	r	r^3	r^2
3	1	r^2	1
4	sr^3	sr	r^2

Player ONE wins this play of $\mathsf{MT}_4(\mathsf{D}_4, *, A)$ if r^2 is a member of A.

Findings for Dihedral Groups

The even index theorem

1. If $n \mod 4 = 2$, ONE has a winning strategy in $\mathsf{MT}_n(\mathsf{D}_n, \circ, A)$ if, and only if, the identity element of D_n is in A.
2. If $n \mod 4 = 0$, ONE has a winning strategy in $\mathsf{MT}_n(\mathsf{D}_n, \circ, A)$ if, and only if, $r^{\frac{n}{2}}$ is in A.

Future Work

- Determine for odd n, and a given subset A of D_n, whether ONE has a winning strategy in $\mathsf{MT}_n(\mathsf{D}_n, \circ, A)$.
- Examine the computational complexity of deciding whether ONE has a winning strategy in $\mathsf{MT}_n(\mathsf{D}_n, \circ, A)$ when n is odd.

References

[1] L. Babinkostova and M. Scheepers, *A Game on Groups and Information Security*, **Proceedings of the III International Conference on Informatics and Information Technology** (2003), 115 - 127.

[2] E. Zermelo, *Über eine Anwendung der Mengenlehre auf die Theorie des Schachspiels*, **Proceedings of the Fifth Congress of Mathematicians**, **Cambridge University Press** (1913), 501 - 504.

Acknowledgements

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