MATH422 PROPOSAL

ARDEN RASMUSSEN

Automatic Group

This is the group of finitely generated groups, which have a finite-state automata that represents the Cayley graph of the group. This seems interesting to me as a cross of computer science and group theory. It seems that the relation can be used both ways, in using group theory concepts in the application of finite state automata, and in using finite state automata to solve problems in group theory.

References.

- Automata Groups[1]
- Finite State Automata: A Geometric Approach[2]

Elliptic Curves in Cryptography

This appears to be using specially constructed groups can be considered for use in cryptography. Specifically Elliptic Curves. It seems that group theory can be used to construct secure key transfers, based off of the selection of specific groups.

References.

- Combinatorial group theory and public key cryptography[3]
- Elliptic Curve Cryptography[4]
- Elliptic Curve Cryptography[5]
- Use of Elliptic Curves in Cryptography[6]
- A Gentle Introduction to Elliptic Curve Cryptography[7]

Rubik's Cube

Many proofs involving the Rubik's cube are rooted in group theory, such as the algorithms that were used to determine the minimum number of necessary moves to solve any scramble of a rubik's cube is 20. In general the operations of rotating an edge is treated as a group which acts on the cube. Then by altering the cube so that it is in smaller and smaller subsets of the possible states, eventually the cube enters the solved state.

[1] http://cms.dm.uba.ar/Members/gcorti/workgroup.GNC/notes.pdf

[2] https://www.ams.org/journals/tran/2001-353-09/S0002-9947-01-02774-X/S0002-9947-01-02774-X.pdf

[3] https://arxiv.org/pdf/math/0410068.pdf

[4] https://eprint.iacr.org/2008/390.pdf

[5] https://www.ams.org/journals/mcom/1987-48-177/S0025-5718-1987-0866109-5/S0025-5718-1987-0866109-5.pdf

[6] https://link.springer.com/content/pdf/10.1007/3-540-39799-X_31.pdf

[7] https://www.law.upenn.edu/cf/faculty/jvagle/workingpapers/A%20Gentle%20Introduction%20to%20Elliptic%20Curve%20Cryptography.pdf

References.

- The Mathematics of the Rubik's Cube[8]
- Algorithms for solving the Rubik's cube[9]
- Group Theory and the Rubik's Cube[10]

Fractals

I like fractals, they are pretty.

References.

- Groups and analysis on fractals[11]

[8] https://web.mit.edu/sp.268/www/rubik.pdf
[9] http://www.diva-portal.org/smash/get/diva2:816583/FULLTEXT01.pdf
[10] http://people.math.harvard.edu/~jjchen/docs/Group%20Theory%20and%20the%20Rubik's%20Cube.pdf
[11] https://www2.math.uconn.edu/~teplyaev/research/NT.pdf