Equivalence Classes of Functions Over Finite Fields

Tim Wraight
School of Mathematical and Geospatial Sciences
RMIT University

Highly nonlinear functions over finite fields are very important in fields of Coding and Cryptography. To be useful these functions need to be resistant to differential and linear cryptanalysis. Functions that are resistant are called Perfect Nonlinear(PN) and Almost Perfect nonlinear (APN). APN functions are some of the best types of functions to use for cryptography and coding, but as they get bigger it gets harder and harder to tell if they different. We need to be able to group these functions into equivalence classes to understand if they are different from one another. Different applications of these unctions has led to the development of lots of different notions of equivalence. For Vectorial Boolean Functions, two definitions of equivalence have become most important in recent years. They are Carlet-Charpin-Zinoviev (CCZ) equivalence and Extended affine (EA) Equivalence. For my AMSI vacation scholarship, I went about researching these Classes of equivalence under the supervision of Professor Kathy Horadam at RMIT in Melbourne.

EA equivalence implies CCZ equivalence but the converse does not hold. Generally it is hard to determine when CCZ- Equivalent functions are EA-in-equivalent. EA is defined in terms of composition and addition of functions, while CCZ equivalence is defined in terms of mappings of graphs of functions.

This problem of defining whether CCZ- equivalent functions are EA in-equivalent has become much more needed after recent breakthroughs. It was thought that new functions were to be found in the power functions and it was conjectured that APN functions fell into one of 6 EA-in-equivalent classes, but there has been many new discoveries recently of new families of APN functions that are EA-in-equivalent to any power functions. These functions are also now becoming very intricate so it is very hard to prove EA-inequvalence to known functions.

This scholarship has been a fantastic opportunity for me. It allowed me to begin research

Tim received an AMSI Vacation Scholarship in December 2008
See: www.ice-em.org.au/vs09.html

and develop some background before I began honours. I also greatly enjoyed being able to attend CSIRO's Big Day In. It was a great experience been able to present to and hear presentations of other students of like minds from around the country.

The work I undertook on this project will contribute to research for my Honours project this year, in which I will continue the study of equivalence classes. I thank AMSI for giving me the great opportunity to do this project.

Tim received an AMSI Vacation Scholarship in December 2008
See: www.ice-em.org.au/vs09.html