Finite Fields, Computer Algebra Systems, and Non-Linear Coding

S. Engelberg[1], O. Keren[2]

[1] *Department of Electrical and Electronics Engineering, School of Engineering and Computer Science, Jerusalem College of Technology, Jerusalem, Israel, shlomoe@jct.ac.il*

[2] *School of Engineering, Bar-Ilan University, Ramat-Gan, Israel, Osnat.Keren@biu.ac.il*

We consider linear and non-linear codes. We start by developing a conservation law for codes. We then explain why linear codes, which are easy to understand and implement, are useful when one is interested in protecting data from rarely occuring random errors. By a simple argument, we demonstrate that linear codes are not a good way to protect data from an attacker. Having ruled out linear codes for this purpose, we take up non-linear codes. We explain what a finite field is and how data can be represented by elements of a finite field. We then consider codes that are non-linear functions of the data – of the elements of the finite field. We show that quadratic codes suffer from the same drawbacks as linear codes. Next we consider cubic codes. First we show that if all that one is concerned with are attackers, cubic codes are optimal. Many of the above results are due to M. Karpovsky and his co-workers. (See, for example, [2].)

Then we show how by making use of a computer algebra system we were able to formulate a conjecture that certain cubic codes provide optimal protection against attackers and some protection against certain relatively common random errors. We will then sketch the proof of this result and describe some extensions of the result [1].

References

[1] S. Engelberg and O. Keren, "A Comment on the Karpovsky-Taubin Code," *IEEE Trans. Inf. Theory*, Vol. 57, No. 12 (2011).

[2] M. G. Karpovsky and A. Taubin, "A new class of nonlinear systematic error detecting codes," *IEEE Trans. Inf. Theory*, Vol. 50, No. 8 (2004).