代数的符号理論と組合せ論およびそれらの応用

Algebraic Coding Theory, Combinatorics and their Applications

キーワード：誤り訂正符号、組合せデザイン、マトロイド/ keywords: error-correcting codes, combinatorial designs, matroids, secret sharing scheme

城本　啓介　教授　博士（理学）　/ **Keisuke SHIROMOTO** Professor, Dr. Sci.
産業基盤部門　応用数理解析分野　/ Research Field of Applied Mathematics
E-mail : keisuke@※　*Tel* : 096-342-3626　*URL* : http://www.srik.kumamoto-u.ac.jp/

●代数的符号理論とその応用

雑音のある通信路を通して情報を送受信する場合(Figure 1)において、誤りを正しく訂正するためには、様々な数学的な性質を満たす符号が必要とされる。そこで、与えられたパラメータや性質を満たすような符号の存在問題や構成問題について研究している。特に、近年は量子誤り訂正符号に関する代数的な構成法の研究を進めている。

●組合せ論とその応用

与えられた条件を満たす対象の集まりについて、主にそれらの数理構造の存在問題や構成法について研究を行うのが組合せ論であり、統計学や情報工学等に様々な応用がある。特に、符号を軸に、組合せデザインやマトロイドにおける共通な数理構造について研究することで、暗号や秘密分散法の構成法に関する応用研究を進めている。

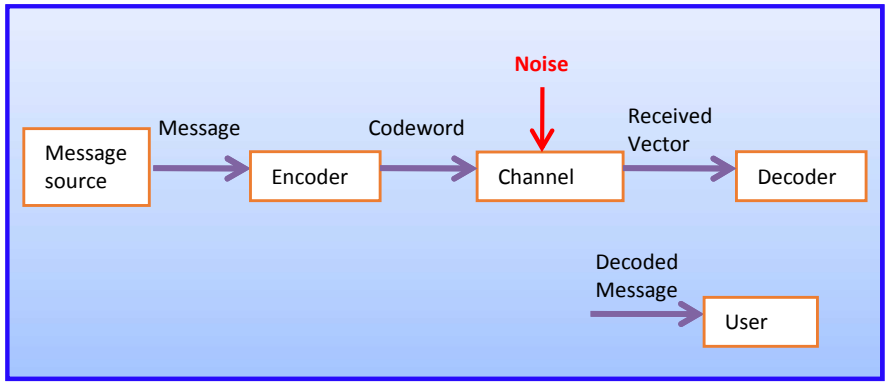

Figure 1 A general digital communication system

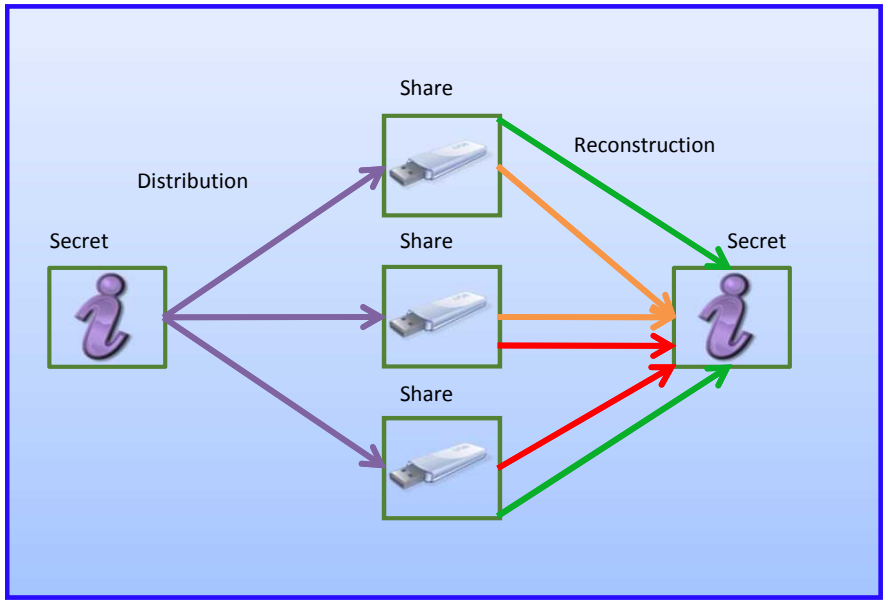

Figure 2 A secret sharing threshold scheme

Algebraic coding theory and its applications: Error-correcting codes are used to correct errors when messages are transmitted through a noisy communication channel (Figure 1). I have studied the existence problems and the constructions of linear codes with given parameters and some mathematical properties. I have recently broadened my research to algebraic constructions of quantum error-correcting codes.

Combinatorics and its applications : Combinatorics is the study of finite discrete structures with given conditions. There are a lot of applications to other areas such as statistics and computer science. I have studied common structures in combinatorial designs and matroids based on codes and been applying that research to develop some constructions of cryptography and secret sharing schemes (Figure 2).