Quasi-Cyclic Codes

San Ling
Division of Mathematical Sciences
School of Physical & Mathematical Sciences
College of Science
Nanyang Technological University
Singapore

Coding theory is concerned with the successful transmission of data through a noisy channel and the correction of errors in corrupted messages. It has wide applications in data storage, telecommunication, etc.

One of the most important classes of classical error-correcting block codes is that of cyclic codes. A cyclic code over $\mathbb{F}_q$ of length n is a vector subspace C of $\mathbb{F}_q^n$ with the property that $(c_1, \ldots, c_{n-1}, c_0) \in C$ whenever $(c_0, c_1, \ldots, c_{n-1}) \in C$. It is well known that every cyclic code over $\mathbb{F}_q$ of length n can be naturally regarded as an ideal in the ring $\mathbb{F}_q[X]/\langle X^n - 1\rangle$. This identification allows algebraic tools to be effectively used to study the properties of such codes and enables such codes to have efficient encoding and decoding, thus making them particularly suitable for practical use.

The class of quasi-cyclic codes over finite fields is a generalization of cyclic codes. A quasi-cyclic code over $\mathbb{F}_q$ of length n and index ℓ, where ℓ divides n, is a vector subspace C of $\mathbb{F}_q^n$ such that $(c_0, \ldots, c_{n-1}) \in C$ implies $(c_\ell, \ldots, c_{n-1}, c_0, \ldots, c_{\ell-1}) \in C$. (When $\ell = 1$, we land back in the case of a cyclic code.) Like cyclic codes, quasi-cyclic codes also afford nice algebraic structures. (In fact, quasi-cyclic codes enjoy several different algebraic descriptions, while cyclic codes essentially have only the algebraic description given above.) Yet, unlike cyclic codes, for which it is not known whether an "asymptotically good" family exists, "asymptotically good" families of quasi-cyclic codes are known to exist. Many of the linear codes with the best known parameters also belong to this class. Quasi-cyclic codes are also known to have connections with other types of codes such as convolutional codes and LDPC codes.

In this talk, we shall first give a very brief introduction to the theory of error-correcting codes, before zooming in on quasi-cyclic codes through a few different algebraic lenses and discussing some applications of these different approaches.