

**LING San**  
Professor

Chair, School of Physical & Mathematical Sciences  
BA, MA, University of Cambridge  
PhD, University of California Berkeley

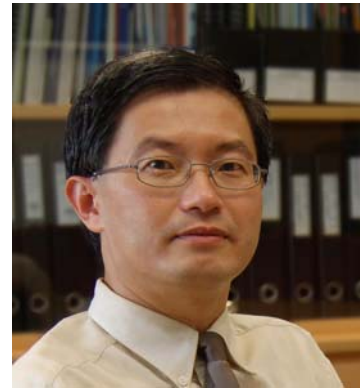
*Major Research Interest: Application of Algebra, Number Theory & Combinatorics to Coding Theory & Cryptography*

Email: [lingsan@ntu.edu.sg](mailto:lingsan@ntu.edu.sg)

<http://www.ntu.edu.sg/home/lingsan/>

Tel: (65) 6790 3753

Fax: (65) 6316 6984



Tools in algebra and number theory, such as finite rings, discrete Fourier transform, algebraic curves over finite fields, etc., have been found to provide effective new approaches to the construction and analysis of different types of codes and sequences. One focus of our research is to exploit such tools to study various classes of algebraic block codes. The following themes underlie our research – the construction of codes of good parameters, the analysis of the algebraic structure and properties of codes, and classification results. The parameters of a code determine its error-correcting capability, and several well-known bounds exist that constrain their relationship. Constructing codes that either attain such bounds, or at least with parameters better than other known codes, is one of the important problems in coding theory. Using finite fields, algebraic curves and combinatorial objects, new families of codes with good parameters as well families of optimal constant weight and constant composition codes have been obtained. An extensive study on the algebraic structure of quasi-cyclic codes has also been conducted – this is a class of codes that has found interesting applications and fascinating examples. We have also done some studies on codes over finite rings, including a complete classification of all cyclic codes over  $\mathbb{Z}_4$ . As sequences are closely related to codes, our interest in codes has also led us to study sequence families from rings and their correlation properties.

In recent years, new paradigms in coding theory, such as quantum codes, LDPC codes, space-time codes, etc., have appeared and attracted considerable interest. We are also interested in applying techniques in algebra, number theory and combinatorics to the study of these new kinds of codes. Initial investigations have yielded fruitful outcomes in quantum coding – a completely algebraic description of quantum codes has been obtained, which has the potential of facilitating the discovery of good quantum codes. Asymptotically good families have also been obtained. Some study on error-block codes has also begun recently. As algebraic and number-theoretic tools have not been used much in these new paradigms, our main interest in these topics is to use such tools to construct new good examples and to understand their structures and properties in more systematic ways.

Though motivated by applications in totally different domains, the theory of digital nets bears much resemblance with the theory of error-correcting codes. We have also recently applied finite fields and error-correcting codes to obtain digital nets of best known parameters.

Besides coding theory, investigations into application of algebraic and combinatorial techniques, as well as error-correcting codes, in certain areas of cryptography, such as perfect nonlinear functions, secret sharing schemes, cover-free families and hash functions, etc., are also underway.

Some recent work in these topics include: application of perfect nonlinear functions to secret sharing schemes, secret sharing via elliptic curves, cryptanalysis of LASH, etc.

**Selected Publications**

- S. Ling & F. Özbudak, Some constructions of  $(t,m,s)$ -nets with improved parameters. *Finite Fields Appl.* **To appear.**
- Y.M. Chee, A.C.H. Ling, S. Ling & H. Shen, The PBD-closure of constant composition codes. *IEEE Trans Inform Theory*, **53**, no. 8, 2685 – 2692 (2007)
- Y.M. Chee & S. Ling, Constructions for  $q$ -ary constant weight codes. *IEEE Trans Inform Theory* **53**, no. 1, 135 – 146 (2007)
- K. Feng, S. Ling & C. Xing, Asymptotic bounds on quantum codes from algebraic geometry codes. *IEEE Trans Inform Theory* **52**, 986 – 991 (2006)
- S. Dougherty & S. Ling, Cyclic codes over  $\mathbb{Z}_4$  of even length. *Designs, Codes and Cryptography* **39**, 127 – 153 (2006)
- S. Ling & F. Özbudak, Improved  $p$ -ary codes and sequence families from Galois rings of characteristic  $p^2$ . *SIAM J Discrete Math* **19**, 1011 – 1028 (2006)
- J. Lahtonen, S. Ling, P. Solé & D. Zinoviev,  $\mathbb{Z}_8$ -Kerdock codes and pseudorandom binary sequences. *J. Complexity* **20**, 318 – 330 (2004)
- S. Ling & J.T. Blackford,  $\mathbb{Z}_{p^{2k+1}}$ -linear codes. *IEEE Trans Inform Theory* **48**, 2592 – 2605 (2002)
- S. Ling & P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields. *IEEE Trans Inform Theory* **47**, 2751 – 2760 (2001)
- H. Chen, S. Ling & C. Xing, Asymptotically good quantum codes exceeding the Ashikhmin-Litsyn-Tsfasman bound. *IEEE Trans Inform Theory* **47**, 2055 – 2058 (2001)
- C. Xing & S. Ling, A class of linear codes with good parameters. *IEEE Trans Inform Theory* **46**, 2184 – 2188 (2000)