Cryptography and Communications (2020) 12:321–323
https://doi.org/10.1007/s12095-020-00433-3

Editorial: Special issue on sequences and their applications 2018

Tor Helleseth[1] · Wai Ho Mow[2] · Zhengchun Zhou[3]

Published online: 3 April 2020

This is a special issue of the journal "Cryptography and Communications" that is devoted to recent results on sequences and their applications. Sequences have been studied for many years due to numerous and important applications in communication systems. Sequences have also close relations to coding theory, cryptography, Boolean functions and many other areas in mathematics. The contributors to this volume are researchers participating at the event "Sequences and Their Applications" (SETA 2018) held in Hong Kong, October 1-6, 2018. The authors of accepted submissions at SETA 2018 were invited to contribute to this special issue. In addition papers by the two invited speakers, Sihem Mesnager and Alexander Pott were especially invited. All papers were thoroughly reviewed to meet the high standard of the journal and the papers below were accepted after the reviewing process.

Sequence families with zero-correlation zone (ZCZ) have been extensively studied in recent years. The paper "Polyphase zero correlation zone sequences from generalised bent functions" by Dan Zhang, Matthew Parker and Tor Helleseth proposes a construction of polyphase ZCZ sequences based on generalised bent functions.

Evgeny Krengel in his contribution "One construction of perfect ternary sequences" presents a new construction of a family of perfect ternary sequences that is a generalisation of one of such known families. The implementation aspects of these sequences are also considered.

Complementary sequences with quadrature amplitude modulation (QAM) symbols have important applications in orthogonal frequency division multiplexing (OFDM) communication

✉ Tor Helleseth
Tor.Helleseth@uib.no

Wai Ho Mow
eewhmow@ust.hk

Zhengchun Zhou
zczhou@126.com

[1] Department of Informatics, University of Bergen, PO Box 7803, 5020 Bergen, Norway

[2] Department of Electronic and Computer Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong

[3] School of Mathematics, Southwest Jiaotong University, Chengdu 611756, China

systems. The title of the paper "Two constructions for 16-QAM complementary sequence sets with non-power-of-two length" by Yajing Zhou, Zhengchun Zhou, Yang Yang and Yong Wang describes the main results.

Yang Yang and Chunlei Li give three constructions of quaternary sequences with optimal odd-periodic autocorrelation magnitude in their paper "New quaternary sequences with optimal odd-periodic autocorrelation magnitude".

The contribution by Deng Tang and Xia Li entitled "A note on the minimal binary linear code" gives new constructions of some special minimal binary linear codes that can be used to construct secret sharing schemes.

The paper "Large families of sequences for CDMA, frequency hopping, and UWB" by Domingo Gómez-Peréz, Ana I. Gómez and Andrew Tirkel generalises three constructions of sequence families with bounded off peak correlation that have flexible parameters and sequence lengths suitable for wireless communications and MIMO radar.

A new design for low hit zone frequency hopping sequences (FHS) with optimal partial Hamming correlation based on t-decimation of m-sequences is presented in the paper "Decimated m-sequences families with optimal partial Hamming correlation" by Hongyu Han, Sheng Zhang, Limengnan Zhou and Xing Liu.

The Nth maximum order complexity for an infinite sequence is the length of the shortest feedback shift register that generates the first N elements in the sequence. The Nth maximum order complexity and expansion complexity of a Rudin-Shapiro-like sequence is calculated in the paper "On the Nth maximum order complexity and the expansion complexity of a Rudin-Shapiro-like sequence" by Zhimin Sun, Xiangyong Zeng and Da Lin.

The paper "On three conjectures of binary sequences with low odd-periodic autocorrelation" by Chunlei Li and Yang Yang gives a complete answer to three conjectures by Matthew Parker on low odd-periodic autocorrelation of sixteen cyclotomic binary sequences as well as constructing new binary sequences with low odd-periodic autocorrelation.

A class of additive codes is introduced, that are referred to as $\mathbb{Z}_2\mathbb{Z}_2[u, v]$-additive codes, and described in the paper "One-weight and two-weight $\mathbb{Z}_2\mathbb{Z}_2[u, v]$-additive codes" by Minjia Shi, Chengchen Wang, Rongsheng Wu, Yu Hu and Yaoqiang Chang. A MacWilliams type of identity relating the weight distributions of a code and its dual is proved. In addition some one-weight and two-weight codes are constructed.

Hyper-bent functions were first introduced by Youssef and Gong in 2001 to ensure the security in symmetric cryptography. In the invited paper "On generalised hyper-bent functions" by Sihem Mesnager, she reviews basic results on generalized hyper-bent functions and also presents new results.

The other invited paper "A direct construction of primitive formally dual pairs having subsets with unequal sizes" by Shuxing Li and Alexander Pott presents a direct construction of primitive formally dual pairs having subsets with unequal sizes in $\mathbb{Z}_2 \times Z_4^{2m}$, where $m \geq 1$. The construction recovers an infinite family that has earlier been constructed by a recursive approach. The direct construction provides new and more insight into this problem than what was known from the recursive approach.

In the paper "Frequency-hopping sequence sets with no-hit-zone through Cartesian product" by Limengnan Zhou, Hongyu Han and Xing Liu, three designs of frequency-hopping sequence sets with no-hit-zone are presented with optimal Hamming correlation properties.

The contribution "Properties of tight frames that are regular schemes" by Malcolm Egan gives some connections between tight-unit norm frames and weighted 1-designs. Finite frames have applications in signal designs and coding theory and there are connections to sequences, combinatorial designs and quantum information theory.

The paper "Binary and ternary sequences with a few cross correlations" by Yansheng Wu, Qin Yue, Xueying Shi and Xiaomeng Zhu investigates the cross correlation distribution between a p-ary m-sequence and its d-decimated sequence. The paper considers the case $p = 2$ and $p = 3$ and shows using Gauss sums that the binary sequences has two-valued cross correlations and the ternary sequences have at most three-valued cross correlations.

The authors of "Partially APN Boolean functions and classes of functions that are not APN infinitely often", Lilya Budaghyan, Nikolay S. Kaleyski, Soonhak Kwon, Constanza Riera and Pantelimon Stănică define the notion of a partial almost perfect nonlinear (APN) function and find characterizations and constructions of classes of functions satisfying this condition.

In the paper "Three deterministic constructions of compressed sensing matrices with low coherence", the authors Xiwang Cao, Gaojun Luo and Guangkui Xu present constructions of compressed sensing matrices by using algebraic and combinatorial methods that are shown to outperform Gaussian random matrices.

The authors Xia Li, Cuiling Fan and Xiaoni Du of "A family of distance-optimal minimal linear codes with flexible parameters" construct a family of linear codes. Some of the codes are distance-optimal with respect to the Griesmer bound. The codes can be used to construct secret sharing schemes.

The paper "A class of exponential sums and sequence families" by Chengju Li, Qin Yue, Yongbo Xia and Wei Peng evaluates a class of exponential sums and applies the results to determine the correlation value description. As an application, three families of binary sequences are constructed with three-valued correlation.

Correlation-immune functions are of importance for measuring the resistance of a crypto system against correlation attacks. The discrete Fourier transform of non-binary functions are studied in the paper "The Fourier spectral characterization for the correlation-immune functions over $\mathbb{F}_p$" by Zilong Wang, Jinjin Chai and Guang Gong. It is shown that a function is mth-order correlation immune if and only if its Fourier spectrum vanishes at a specific location under any permutation of the variables.

The paper "Certain sequences of arithmetic progressions and a new key sharing method" by Ch. Srikanth considers a special type of sequence of arithmetic progressions. As an application a method is proposed for how users securely can agree on secret random keys.

Fractional repetition (FR) codes allow exact uncoded repair with minimum repair bandwidth in distributed storage systems. The paper "On non-uniform flower codes" by Krishna Gopal Benerjee and Manish K. Gupta presents a general approach to construct FR codes by finite binary sequences. The constructed codes are called flower codes and conditions and constraints are discussed.