For favour of Posting

THE HONG KONG UNIVERSITY OF SCIENCE & TECHNOLOGY

Department of Mathematics

SEMINAR ON PURE MATHEMATICS

Semifields and their relations to finite geometry, coding theory, and cryptography

by

Prof. Lukas Koelsch

University of South Florida

(Based partly on joint work with Faruk Göloğlu)

Abstract

This talk is about algebraic objects called *semifields* which are, roughly speaking, fields where multiplication is not assumed to be associative or commutative. I will start by giving a brief survey of connections of finite semifields to finite geometry, coding theory, and cryptography.

The biggest open conjecture in semifields theory, due to Kantor, asks if the number of inequivalent finite semifields is bounded by a polynomial in the size of the semifield. This conjecture has wide ranging implications, for instance on the ubiquity of rank-metric codes and certain projective planes. I shall present recent advances on the conjecture, in particular several new constructions of semifields that I have found in recent years that gener-alize more than a dozen known constructions of semifields. We also discuss the special case of *commutative* semifields, which have intimate relations to highly nonlinear functions that can be used in symmetric cryptography, as well as group theoretic methods to determine if given semifields are inequiv-alent or not.

Date : 5 March 2025 (Wednesday)

Time : 10:00 - 11:00 a.m.

Zoom Meeting : https://hkust.zoom.us/j/9832399155 (Passcode: 322024)

All are Welcome!