

1106-05-2397 **Scott Lacy*** (scott.lacy@mavs.uta.edu). *Sub-neofields of finite D-neofields.*

A neofield is a set with two binary operations similar to a field, with the addition not necessarily associative and the multiplication not necessarily commutative. Neofields offer considerable advantages in the design of cryptographic algorithms and enciphering systems, yet typically only associative structures such as groups, fields and vector spaces are used in practice. Property D cyclic neofields have a cyclic multiplicative group and are named D-neofields due to a special “divisibility” property. The existence of a D-neofield of a particular order guarantees the existence of a pair of orthogonal latin squares. D-neofields have been classified to order 20 and conjectured to exist for all orders beyond by A.D Keedwell in 1967. Many examples of larger orders have been found, including all commutative neofields to order 28. In this talk we explore the concept of a sub-neofield and consider the implication on extending neofields to much larger neofields. In particular we examine D-neofields of order 25, along with examples of their subneofields. (Received September 16, 2014)