Meeting: 1005, Newark, Delaware, SS 5A, Special Session on Designs, Codes, and Geometries

1005-05-153 **A R Calderbank*** (calderbk@math.princeton.edu), Princeton University, Fine Hall, Room 206, Princeton, NJ 08544. *A New Approach to Kerdock and Preparata Codes.*

There is an additive group structure on $\mathbb{F}_2^m$ and a multiplicative structure that depends on the choice of a primitive irreducible polynomial $g(x)$ of degree m. Given such a polynomial $g(x)$, let $\mathcal{K}$ be the set of binary symmetric matrices P with the property that $xPy^T = (xy)^{\frac{1}{2}}P[(xy)^{\frac{1}{2}}]^T$ for all $x, y \in \mathbb{F}_2^m$. Then $\mathcal{K}$ is a Kerdock set; that is

1. $\mathcal{K}$ is a binary vector space containing 2^m Hankel matrices, and there is exactly one binary symmetric matrix P with any given diagonal dp

2. Every matrix P in $\mathcal{K}$ is nonsingular.

The Kerdock set $\mathcal{K}$ determines a classical Kerdock code over $\mathbb{Z}_4$, and a corresponding Preparata code. This description avoids the arithmetic of galois rings and leads to local decoding algorithms for Kerdock codes. (Received February 07, 2005)