An Investigation into Combinatorial Equivalents of the Maximum Distance Separable Conjecture: An Approach Through (t,m,s)-Nets and Orthogonal Arrays

Daniel Kaiser, University of Michigan. Research supervisor: Dr. Steven B. Damelin, Mathematical Reviews, The American Mathematical Society.

Introduction

In our project, we have explored connections to the Maximum Distance Separable (MDS) Conjecture, a conjecture intimately connected to many diverse areas of mathematics ranging from projective geometry to coding theory. The MDS Conjecture, first proposed by Segre in 1955 [5], loosely states: "For a given prime power q and integer k between 2 and q, if one is given a k by n matrix, M, then the largest possible n such that any given k-many subset (not submatrix!) of column vectors of M is linearly independent is q+1, unless q is even and moreover k is 3 or q-1, then the largest such n is q+2." In our research we are interested specifically in using combinatorial designs, especially (t,m,s)-nets in base b and orthogonal arrays, to find an equivalence to the MDS conjecture. We intend for this equivalence to complement other recent equivalences to the conjecture in terms of special codes (matrices) called Reed-Solomon codes, and also one in terms of algebraic rings [6].

Figure 1: Diagram of Construction Equivalents

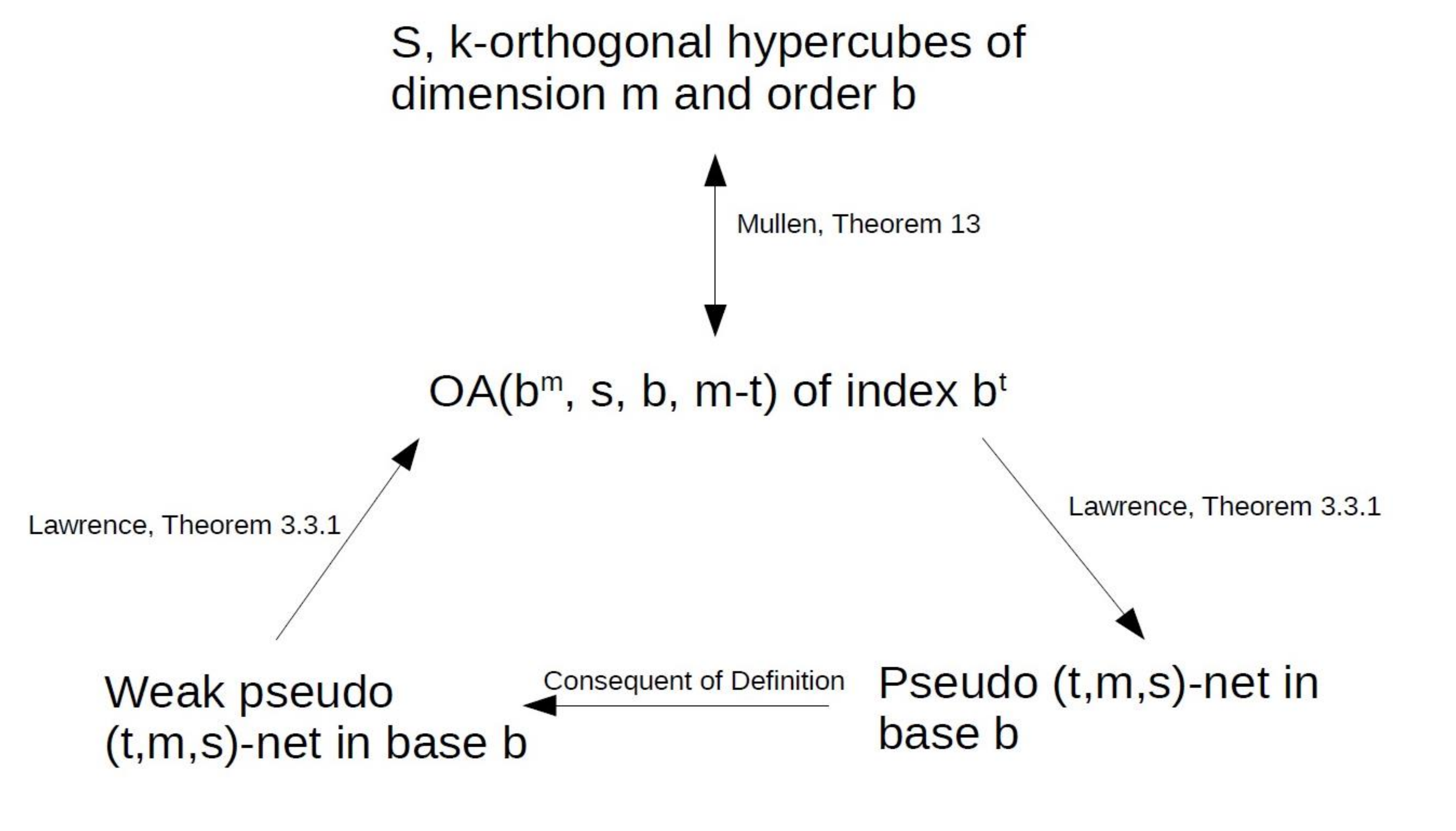

Figure 2: Example of MDS code and Connection to Theorem

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \in \mathrm{Mat}(6, 8, \mathbb{F}_2)$$

This matrix, also an MDS code with k=6, gives rise to construction of 8 binary hypercubes of dimension 6, each of which are 4-orthogonal, from which we can apply the above theorem.

Methods

We work over F_q, the finite field of order q where q is a given prime power. Given an integer n≥2, F_q^n will be the set of vectors in F_q of length n. For positive integers 2≤k≤n, we say that a set of vectors $A \subseteq F_q^n$ is k-independent if all its subsets with at most k elements are linearly independent. We are interested in the maximal possible cardinality of a k-independent subset of F_q^n which we call $Ind_q(n,k)$. Having wished to reformulate $Ind_q(n,k)$, combinatorial designs and their literature were investigated. Primary literature sources were drawn from various papers by Damelin[1], Mullen[3] and Niederreiter [4], as well as a notable 1995 University of Wisconsin – Madison thesis from Mark Lawrence [2]. Specifically, the various construction conditions and their equivalences of these objects, most notably Niederreiter and Lawrence's contributions to this field, were investigated most heavily; the following weaker version of a theorem from Lawrence was the focus of the project: For a given positive integer s, the following ultimately equivalent structures can be constructed:

- A set of s, k-orthogonal hypercubes of dimension m and order b
- An orthogonal array OA(b^m, s, b, m-t) of index b^t
- A pseudo (t, m, s)-net in base b
- A weak pseudo (t, m, s)-net in base b

for given positive integers t,m and b, where b is furthermore a prime power.

Results and Conclusions

We have come to understand the $Ind_q(n,k)$ quantity and its relation to linear independence, and hence to MDS codes, as well as various combinatorial designs and objects related to linear codes and the Maximum Distance Separable Conjecture. With our new-found understanding, we hope to further our research by continuing investigations along comparable approaches to the aforementioned $Ind_q(n,k)$ quantity versus (t,m,s)-nets and orthogonal arrays. We are working on connecting these two quantities to give a more rigorous equivalence of the MDS conjecture, albeit in the language of combinatorial designs.

Poster References:

1) Damelin, Steven, et al., *The Number of Linearly Independent Binary Vectors with Applications to the Construction of Hypercubes and Orthogonal Arrays, Pseudo (t,m,s)-nets and Linear Codes*, Monatsh. Math. 141(2004), 277-288.
2) K. M. Lawrence, *Combinatorial Bounds and Constructions in the Theory of Uniform Point Distributions in Unit Cubes, Connections with Orthogonal Arrays and a Poset Generalization of a Related Problem in Coding Theory*, Ph.D. Thesis, University of Wisconsin, 1995.
3) G. L. Mullen, *Orthogonal Hypercubes and Related Designs*, J. Statist. Planning and Inference, 73 (1998), 177-188.
4) H. Niederreiter, *Point sets and sequences with small discrepancy*, Monatsh. Math. 104 (1987), 273–337.
5) Segre, Beiamino, *Ovals in a Finite Projective Plane*, Canad. J. Math., 7 (1955), 414-416.
6) Sun, J., Damelin, S., Kaiser, D., arXiv:1611.02354, preprint.

UNDERGRADUATE RESEARCH OPPORTUNITY PROGRAM
UNIVERSITY OF MICHIGAN