Designs, Codes and Cryptography (2022) 90:1595–1597
https://doi.org/10.1007/s10623-022-01058-8

Book Review: "Designs from Linear Codes", second edition, by Cunsheng Ding and Chunming Tang, World Scientific, 2022

Vladimir D. Tonchev[1]

Accepted: 9 May 2022 / Published online: 11 June 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

This book is an updated and expanded edition of the monograph [2] written by Dr. Cunsheng Ding. The book gives a comprehensive treatment of the interplay between the theory of linear codes and combinatorial t-designs, and is intended to be a reference for postgraduates and researchers in the areas of combinatorics, coding theory, and communications engineering. The reader is assumed to have basic knowledge of linear algebra and finite fields. For convenience of the reader, Chapter 1 introduces the main mathematical concepts and techniques that are used throughout the rest of the book.

A natural way to associate a linear code L over a finite field $GF(q)$ with a given t-design $\mathcal{D}$, is by defining L as the linear span over $GF(q)$ of an incidence matrix A of $\mathcal{D}$. This simple construction is motivated by the possibility of majority-logic decoding of the dual code $L^{\perp}$. Since the dimension of L is equal to the q-rank of A, the drawback of this approach is that although one can easily compute the q-rank of a design with relatively small parameters, there are very few known infinite classes of designs whose q-rank is known. A second approach to link a t-design with a given linear code L is by considering the supports of all codewords of a given Hamming weight $w > t$ as blocks of a t-design (called a design *supported* by L), and find sufficient conditions which guarantee that t is greater than 0. A simple sufficient condition is for the code L to be invariant under a permutation group acting t-homogeneously or t-transitively on the set of code coordinates. It follows from the classification theorem of finite simple groups that the largest t for which one can obtain a nontrivial t-design by this construction is $t = 5$. The only linear codes that support 5-designs due to the 5-transitive property of their automorphism groups are the extended Golay codes of length $n = 12$ ($q = 3$) and $n = 24$ ($q = 2$), and the perfect Golay codes of length 11 and 23 are the only codes that support 4-designs due to the 4-transitivity of their automorphism groups. Examples of linear codes that admit a 3-transitive or 3-homogeneous group include the Reed-Muller codes and the extended quadratic-residue codes of length $n = q + 1$, when $q \equiv 3 \pmod 4$.

The most powerful known sufficient condition for a linear code to support a t-design is the Assmus-Mattson theorem [1]. The conditions of this theorem require that the minimum

Communicated by the Editors-in-Chief.

✉ Vladimir D. Tonchev
tonchev@mtu.edu

1 Michigan Technological University, Houghton, MI 49931, USA

distance of the code is greater than the number of distinct nonzero weights in its dual code. The largest value of t for which there are linear codes that support t-designs due to the Assmus-Mattson theorem is $t = 5$, and there are finitely many known such codes, all being extremal self-dual binary, ternary, or quaternary (over $GF(4)$ or Z_4) codes.

The difficult part of applying the Assmus–Mattson theorem is the computation of the weight distribution of the code. Apart from the case of extremal self-dual codes whose weight distribution is uniquely determined by their minimum weight, finding the weight distribution of a linear code in general is an extremely difficult problem, particularly when the question is about finding the weight distribution for an infinite class of codes rather than a single code with moderately sized parameters.

The first edition of the monograph [2] treats in detail recent advances in computing the weight distributions of infinite families of linear codes that support 2-designs and 3-designs by the Assmus–Mattson theorem. These infinite families include BCH codes and their subfield subcodes and trace codes, codes defined by maximal arcs in finite projective planes, and other linear codes with various types of regularity. Many of these advances were due to the author of the monograph, Dr. Cunsheng Ding, and his collaborators, and inspired a host of research papers in this area.

The second edition [4] of the monograph, co-authored by Cunsheng Ding and Chunming Tang, has been motivated by some important recent advances in the construction of t-designs from linear codes that were made after the publication of the first edition, namely:

- The discovery of infinite families of near MDS codes that support infinite families of 2-designs and 3-designs [3];
- The discovery of the first known infinite family of linear codes that support 4-designs [5];
- A generalization of the Assmus-Mattson theorem that can be used for the construction of infinite families of codes which do not satisfy the assumptions of the original Assmus-Mattson theorem, but nevertheless support t-designs [6].

Some sporadic near MDS codes, including the ternary perfect Golay code which was discovered in 1949, as well as some infinite families of near MDS codes have been found during the last 70 years. However, the question of the existence of an infinite family of near MDS codes that hold t-designs with $t \geq 2$ has been an open problem for 70 years. The paper [3] by Cunsheng Ding and Chunming Tang settled this long-standing problem by discovering an infinite family of near MDS codes over $GF(3^s)$ that support an finite family of 3-designs, and yet another infinite family of near MDS codes over $GF(2^{2s})$ that support an infinite family of 2-designs.

Until very recently the largest t for which infinite families of codes supporting t-designs were known was $t = 3$, and the existence of an infinite family of codes that support t-designs with $t > 3$ was an open question for over 70 years. The paper [5] by the authors of the second edition of the monograph made a breakthrough in this direction, by presenting the first infinite family of linear codes that support 4-designs.

These topics are treated in two new chapters (Chaps. 15, 16) that had been added to the 14 chapters from the first edition. In addition, several chapters from the first edition have been extended by adding new material, and a new section Notes has been added at the end of each chapter for providing further relevant information and references. A new Appendix A describes some new sporadic 4-designs and 5-designs supported by linear codes. Another new Appendix C has been added that gives a quick introduction to elementary number theory, groups, rings, and finite fields, and provides many exercises on these topics, which makes the monograph also usable as a textbook for an advanced upper level graduate course in coding theory or design theory.

References

1. Assmus E.F. Jr., Mattson H.F. Jr.: New 5-designs. J. Combin. Theory Ser. A **6**, 122–151 (1969).
2. Ding C.: Designs from Linear Codes. World Scientific, Singapore (2019).
3. Ding C., Tang C.: Infinite families of near MDS codes holding t-designs. IEEE Trans. Inf. Theory **66**(9), 5419–5428 (2020).
4. Ding C., Tang C.: Designs from Linear Codes, 2nd edn World Scientific, Singapore (2022).
5. Tang C., Ding C.: An infinite family of linear codes supporting 4-designs. IEEE Trans. Inf. Theory **67**(1), 244–254 (2021).
6. Tang C., Ding C., Xiong M.: Codes, differentially δ-uniform functions and t-designs. IEEE Trans. Inf. Theory **66**(6), 3691–3702 (2020).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.