Finite Fields and Their Applications 32 (2015) 233–274

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

# Finite field models in arithmetic combinatorics – ten years on

J. Wolf

*School of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom*

ARTICLE INFO

*Article history:*
Received 29 July 2014
Received in revised form 7 November 2014
Accepted 9 November 2014
Available online 26 November 2014
Communicated by Gary L. Mullen

*MSC:*
11B30
11B25
11B13

*Keywords:*
Arithmetic combinatorics

ABSTRACT

It has been close to ten years since the publication of Green's influential survey *Finite field models in additive combinatorics* [28], in which the author championed the use of high-dimensional vector spaces over finite fields as a toy model for tackling additive problems concerning the integers. The path laid out by Green has proven to be a very successful one to follow. In the present article we survey the highlights of the past decade and outline the challenges for the years to come.



**Contents**



*E-mail address:* julia.wolf@bristol.ac.uk.

http://dx.doi.org/10.1016/j.ffa.2014.11.003

## 1. Introduction

Green's 2004 survey *Finite field models in additive combinatorics* [28] must be counted amongst the most influential and widely cited papers in arithmetic combinatorics. By spotlighting an accessible toy model for a number of notoriously difficult problems in additive number theory, it inspired countless proof ideas in subsequent years and served as introductory reading material for many a graduate student.

Its main tenet was the idea that many of the problems traditionally of interest in additive number theory can be rephrased in the context of high-dimensional vector spaces over finite fields of fixed characteristic. For example, instead of counting the number of 3-term arithmetic progressions in a (finite) subset $A$ of the integers, we may choose to count the number of such progressions inside a subset $A \subseteq \mathbb{F}_3^n$, where the dimension $n$ is to be thought of as very large. The advantage of working in the latter additive group instead of the former is that it has a plentiful supply of non-trivial additively closed subsets, namely the vector subspaces of $\mathbb{F}_3^n$. These closely resemble the original space itself, making it possible to run arguments locally and facilitating especially those relying on iteration. In addition, we have the notion of orthogonality and linear independence at our disposal, which instantly adds a host of techniques from linear algebra to our toolbox.

Working in $\mathbb{F}_p^n$ for some fixed small prime $p$ thus often simplifies the problem at hand, but it does so in such a way that the principal features of the problem are preserved, meaning that solving the toy problem constitutes a significant step towards solving the problem in the integers. Because of their exact algebraic nature, arguments for the toy problem are often more accessible, highlighting the core idea which in the integers tends to be obscured by technical details. Moreover, in certain cases there is a (by now well-established if often technically challenging) procedure for transferring a proof from the model setting to the integers. Although these remarks may appear senseless if not mystifying at this point, we hope that their meaning will become more transparent to the reader through the examples provided in Section 3.

The finite field model $\mathbb{F}_p^n$, and in particular the case of characteristic $p = 2$, is also of unparallelled importance in theoretical computer science, by virtue of representing the set of strings of 0s and 1s of length $n$ under the operation of addition modulo 2. It is nigh on impossible to do justice to the multitude of applications which the ideas sketched out here have had in theoretical computer science, covering areas as diverse as