Editorial

A decade of Finite Fields and Their Applications

The journal *Finite Fields and Their Applications* (FFTA) began publication in 1995, and in this special issue, we provide a flavor of some of the huge volume of finite field-related activity that has taken place in the last decade. This activity has occurred in a wide variety of areas, including of course finite field theory itself, along with algebraic coding theory, cryptography, combinatorial design theory, and algebraic geometry over finite fields, as well as in various algorithmic and computational areas.

We first, in alphabetical order by author, briefly describe each of the papers appearing in this special issue. The article by S. Ball and J. Hirschfeld reviews some bounds on the maximum size of \((n, r)\)-arcs in \(\text{PG}(2, q)\), sets of \(n\) points with at most \(r\) points on a line. An \((n, r)\)-arc in \(\text{PG}(k-1, q)\) is a set \(K\) of \(n\) points with the property that every hyperplane is incident with at most \(r\) points of \(K\) and there is some hyperplane incident with exactly \(r\) points of \(K\). An \((n, n-d)\)-arc in \(\text{PG}(k-1, q)\) is equivalent to a linear \([n, k, d]\)-code for which any two columns of a generator matrix are linearly independent. The aim of this article is to formulate the bounds on plane \((n, r)\)-arcs as bounds that look familiar to coding theorists, to survey recent improvements, and to list a number of open problems.

Roots of irreducible, primitive or normal polynomials of degree \(n\) over the finite field \(F_q\) containing \(q\) elements generate \(F_{q^n}\) algebraically, multiplicatively or additively, respectively, so these types of polynomials are of great significance in practice. In any particular situation, it has generally been possible computationally to demonstrate the existence of such polynomials over \(F_q\) under explicit constraints on the coefficients (not actually forbidden), for example, sparse polynomials. Although theoretical validation of such existence properties has usually been lacking, in the last decade, a number of explicit theorems of this type have been established. Some of these results are described in S. Cohen’s article.

Q. Cheng’s paper surveys various algorithms that efficiently construct elements of provable high order in small characteristic finite fields. M. Fried first generalizes exceptional covers of curves to any normal variety \(Y\). Then he shows that all exceptional covers of \(Y\) form an exceptional tower. His use of subtowers helps separate classical exceptional covers from unsolved problems. Generalizing exceptional to pr-exceptional (possibly reducible) gives some dramatic effects: relations with Serre’s open image.
theorem, the Guralnick-Thompson genus 0 problem, and universal relations between 
Poincaré series.

A. Garcia and H. Stichtenoth provide a survey on recursive towers of function fields 
over finite fields with many rational places. These towers are more elementary, more 
explicit, and easier to understand than constructions of curves with many points based 
on classfield towers or modular curves. They also open the door to make asymptotically 
good long codes more explicit.

Classical coding theory has involved the study of linear codes over finite fields, but 
in the last dozen years, codes over rings have taken a prominent place in the coding 
literature. Whether over fields or over rings, self-dual codes have been among the best-
known and most widely studied codes. W. Huffman surveys current research regarding 
self-dual linear codes of small to moderate lengths over fields of orders 2 and 3, and 
over all four commutative rings with unity of order 4.

The article by A. Lauder explains two of the major achievements of the last ten 
years in the study of zeta functions of varieties over finite fields of characteristic $p$. 
Namely, a $p$-adic cohomological proof of the rationality of these zeta functions and 
a proof that the so-called “unit root zeta functions”-attached to families of varieties 
are $p$-adic meromorphic. These works resolve two open problems that arose from the 
pioneering investigations of Dwork in the 1960s. W. Li and Y. Meemark consider Cayley 
graphs on $PGL_2(F_q)$ modulo three kinds of abelian subgroups. Using representations 
of $PGL_2(F_q)$, the eigenvalues of these graphs are obtained. Character sum estimates 
are then employed to conclude that two types of graphs are Ramanujan, while the third 
type is almost Ramanujan.

Cryptosystems that use the group of points on an elliptic curve over a finite field 
are now widely deployed in practice. The paper by A. Menezes surveys recent devel-
opments in analyzing the security of elliptic curve systems and other systems that use 
hyperelliptic curves over finite fields and bilinear pairings. The paper by H. Nieder-
reiter surveys recent developments concerning the construction of $(t, m, s)$-nets and 
$(t, s)$-sequences which are important for quasi-Monte Carlo methods in scientific com-
puting. Various interesting connections with coding theory are also discussed in this 
paper.

Difference systems of sets are combinatorial structures that arise in connection with 
code synchronization. In his paper, V. Tonchev surveys recent constructions and open 
problems concerning difference systems of sets obtained as partitions of cyclic difference 
sets. Q. Xiang surveys recent results on difference sets and $p$-ranks and Smith 
normal forms of certain incidence matrices arising in combinatorics.

The above survey papers serve to illustrate the extremely wide array of finite field 
topics that have recently been considered. As further evidence of the tremendous volume 
of finite field-related activity that has occurred in the past decade since the inception 
of FFTA in 1995, we now list a number of finite field-related books that have been 
published in this decade. We also include a few books that although published prior to 
the start of FFTA, have had profound influences on the recent development of finite 
field theory and its many applications. In each of several categories, we list books in 
alphabetical order by author. Some of these books could of course be listed in several 
categories, but we will avoid such duplication.
We begin by first listing books dealing with both finite field theory as well as applications. These include [3,9,12,14,15,24,25,27,30,33,36,43,47–49,51,54,56,58]. Numerous books have also been written concerning various aspects of algebraic coding theory. These include but are not limited to [2,5,20,28,29,31,44–46,52,53,55,60].

Recent combinatorial design theory books include [1,4,6,7,17–19]. A number of books dealing with theoretical as well as applied aspects of cryptography have recently been published. These include [10,16,23,34,35,42,53,59].

Beginning in 1991 and continuing every two years, there has been a series of international finite field conferences affectionately known as the Fq n series. Proceedings volumes related to these conferences have been published as follows: Fq 1 (Las Vegas) [38]; Fq 2 (Las Vegas) [39]; Fq 3 (Glasgow) [8]; Fq 4 (Waterloo) [41]; Fq 5 (Augsburg) [22]; Fq 6 (Oaxaca) [40]; and Fq 7 (Toulouse) [37]. Other conference proceedings volumes include [11,13].

There are also several recent textbooks related to the theory and application of finite fields. These include [21,26,32,50,57].

On behalf of the entire finite field community, I would like to take this opportunity as Editor-in-Chief to sincerely thank you for making \textit{Finite Fields and Their Applications} the great success that it is. A very special thanks goes to the members of the FFTA Editorial Board, who have provided truly outstanding leadership and advice during the entire life of the journal. Without their support, the journal would simply not exist. Thanks are also due to the huge number of referees who have so generously given large amounts of their time to carefully referee and review papers for the journal.

A special thanks is also due to you, the readers, for submitting an ever-increasing number of high-quality papers. In addition, a very warm thanks goes to the personnel first at Academic Press, then beginning in 2001 at Elsevier, for their efforts and support in making the journal happen. A very special thanks goes to the staff in the FFTA Editorial Office located in San Diego.

Last, but certainly not least, I thank the members of the FFTA Editorial Board for reading an earlier version of this article and for pointing out additional finite field-related books that I had originally not included, as well as for their comments that greatly improved this article.

With great optimism and enthusiasm, we look forward to the next decade and to publishing yet another special issue of FFTA in 2015 to celebrate our second decade of success!

\textbf{References}


Gary L. Mullen
Department of Mathematics,
The Pennsylvania State University,
University Park, PA 16802, USA
E-mail address: mullen@math.psu.edu.