

# Some fundamental contributions of Gary Mullen to finite fields

Daniel Panario  
School of Mathematics and Statistics, Carleton University  
daniel@math.carleton.ca

Carleton Finite Fields Day 2017  
September 29, 2017

# Overview of Gary's research activities

Gary has served the finite fields community extensively:

- **founder and editor-in-chief** of the main journal in the area: **FFA (Finite Fields and Their Applications)**;
- editor of **at least** DCC (Designs, Codes and Cryptography); JAA (Journal of Algebra and Its Applications); The Fibonacci Quarterly, and Quasigroups and Related Systems;
- editor of many (**more than 10?**) proceedings of the main conference in the area (**the Fq series of conferences**);
- organizer of **many** finite fields conferences worldwide.

## Overview of Gary's research activities (cont.)

A rough estimate indicates that Gary has published [somewhere between 150 and 200 journal articles](#) (depending on whether you use MathSciNet, Google Scholar, etc).

He has published at least four well-known books:

- [Dickson Polynomials](#) (with R. Lidl and G. Turnwald), 1993;
- [Discrete Mathematics Using Latin Squares](#) (with C.F. Laywine), 1998;
- [Finite Fields and Applications](#) (with C.B. Mummert), 2008;
- [Handbook of Finite Fields](#) (with D. Panario), 2013.

## Overview of Gary's research activities (cont.)

His global research areas are finite fields and combinatorics, but he has papers on several other related areas including number theory, information theory, and so on.

Some of his main areas of research (and the ones we will touch here) are:

- permutation polynomials;
- polynomials with prescribed coefficients;
- combinatorial arrays; and
- of integers and polynomials.

- 1 Introduction
- 2 Permutation Polynomials**
- 3 Prescribed Coefficients
- 4 Combinatorial Arrays
- 5 Integers and polynomials
- 6 Conclusions

# Permutation polynomials over finite fields

A **permutation polynomial** (PP) over a finite field is a bijection which maps the elements of  $\mathbb{F}_q$  onto itself.

There have been massive amount of work on PPs since the 19th century, many by famous mathematicians like Hermite and Dickson. Many results have appeared on the last 30 years, in part due to the cryptographic applications of PPs.

Gary's first works on permutation polynomials (PPs) were in a series of papers in Acta Arithmetica in 1976. This included his well-known work on **permutation polynomials in several variables over finite fields**.

PPs continue to be a main topic in Gary's work over the years, even until now (first love?).

# Dickson polynomials

Undoubtedly, one of the most important and well studied families of PPs are Dickson polynomials over finite fields.

Let  $n$  be a positive integer. For  $a \in \mathbb{F}_q$ , we define the  $n$ -th Dickson polynomial of the first kind  $D_n(x, a)$  over  $\mathbb{F}_q$  by

$$D_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i}.$$

In the case  $a = 1$ , we denote the Dickson polynomials of degree  $n$  of the first kind by  $D_n(x)$ . They are PPs if and only if  $\gcd(n, q^2 - 1) = 1$ .

## Dickson polynomials (cont.)

Dickson polynomials are closely related, over the complex numbers, to **Chebyshev polynomials** through the connection  $D_n(2x) = 2T_n(x)$ . As in the case of Chebyshev polynomials, there are other kinds of Dickson polynomials over finite fields, but they remain far less understood than the first kind Dickson polynomials.

Gary's first article on Dickson polynomials and complete mappings (with H. Niederreiter) was in (not less than) our Canadian Mathematical Bulletin (1987).

Later, in 1993, he published his famous monograph **Dickson Polynomials** (with R. Lidl and G. Turnwald), that summarizes all the knowledge we had at the time on these beautiful polynomials. Gary continue to study Dickson polynomials until now, publishing new articles on them from time to time.



# When does a polynomial over a finite field permute the elements of the field?

The research on PPs intensified with the publication of the papers (with R. Lidl) [When does a polynomial over a finite field permute the elements of the field?](#) (1988, 1993) <sup>1</sup>.

These papers draw the map on PPs research for years to come: provide new constructions of PPs; enumerate PPs; give the value set of polynomials when they are not PPs; and other problems that have been researched by many (**many!**) people to these days.

Other related problems have become important these days like what is the cycle decomposition of a PP? when do we have involutions? how to characterize the fixed points of a PP?, and so on.

---

<sup>1</sup>The second one has the funny title: [When does a polynomial over a finite field permute the elements of the field? II](#)

- 1 Introduction
- 2 Permutation Polynomials
- 3 Prescribed Coefficients**
- 4 Combinatorial Arrays
- 5 Integers and polynomials
- 6 Conclusions

# Irreducible polynomials

A polynomial  $f \in \mathbb{F}_q[x]$  is **irreducible** over  $\mathbb{F}_q$  if  $f = gh$  with  $g, h \in \mathbb{F}_q[x]$  implies that  $g$  or  $h$  is in  $\mathbb{F}_q$ .

The **number** of monic irreducible polynomials of degree  $n$  over  $\mathbb{F}_q$  is

$$I_q(n) = \frac{1}{n} \sum_{d|n} \mu(d) q^{n/d} = \frac{q^n}{n} + O(q^{n/2}),$$

where  $\mu : \mathbb{N} \rightarrow \mathbb{N}$  is the Mobius function

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes,} \\ 0 & \text{otherwise.} \end{cases}$$

This is known from 150 years, but if we **prescribed some coefficient to some value**, how many irreducibles are there? **Simple, eh?**

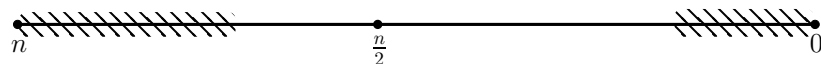
# Irreducibles with prescribed coefficients: existence and number


The starting point for this area of research is the famous **Hansen-Mullen conjecture** (1992) that asks for irreducibles over  $\mathbb{F}_q$  with **any** one coefficient **prescribed to a fix value**.

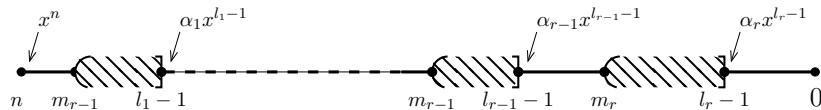
Wan (1997) proved the Hansen-Mullen conjecture using Dirichlet characters and Weil bounds.


The Pandora's box was open: there are generalizations for the existence of irreducibles with two and more coefficients prescribed; for **counting** of the number of irreducibles with prescribed coefficients; for existence and number of other special polynomials with prescribed coefficients.

On the other hand, there are also results for up to **half coefficients prescribed** (Hsu 1995) and variants:



 = coefficients prescribed to any value with total size of roughly  $\frac{n}{2} - \log_q n$



 = zero coefficients

However, **experiments show that we could prescribe almost all coefficients** and still obtain irreducible polynomials!

# Primitive polynomials with prescribed coefficients

Results exists for **primitive polynomials**: an irreducible polynomial  $f$  of degree  $n$  is **primitive** if every root of  $f$  is a primitive element.

**Hansen-Mullen conjecture for primitive polynomials**: primitive polynomials do exist with **any coefficient prescribed** to a value.

This conjecture was proved for  $n \geq 9$  by Cohen (2006), and without restrictions by Cohen and Presern (2007). There are generalizations to few prescribed coefficients but no results for the **number** of primitive polynomials with prescribed coefficients.

**Open problems**: prefix some coefficients to some values; prove that there **exist** (or give the **number** of) primitive polynomials with those coefficients prescribed to those values.

# Primitive normal polynomials with prescribed coefficients

**Primitive normal polynomials** are polynomials whose roots form a normal basis and are primitive elements. An element  $\alpha$  in  $\mathbb{F}_{q^n}$  is **normal** if  $\{\alpha, \alpha^q, \dots, \alpha^{q^{n-1}}\}$  is a basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ .

The **existence** of primitive normal polynomials was established by Carlitz (1952), for sufficiently large  $q$  and  $n$ , Davenport (1968) for prime fields, and finally for all  $(q, n)$  by Lenstra and Schoof (1987). A proof without the use of a computer was later given Cohen and Huczynska (2003).

**Hansen-Mullen (1992)** also conjecture that **primitive normal polynomials with one prescribed coefficient** exist for all  $q$  and  $n$ .

Fan and Wang (2009) proved the conjecture for  $n \geq 15$ . There are generalizations for two (norm and trace) and three coefficients.

# Primitive complete normal polynomials

An element  $\alpha$  in  $\mathbb{F}_{q^n}$  is **completely normal** if  $\alpha$  is a normal element of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_{q^d}$ , for every subfield  $\mathbb{F}_{q^d}$  ( $d|n$ ). The minimal polynomial of  $\alpha$  over  $\mathbb{F}_q$  is a **completely normal polynomial**.

**Morgan and Mullen** (1996) conjecture that for any  $n \geq 2$  and any prime power  $q$  there **exists** a completely normal primitive basis of  $\mathbb{F}_{q^n}$  over  $\mathbb{F}_q$ . This conjecture is still open; major advances have been done by Hachenberger (2001, 2010).

The methods here are **algebraic** and allow derivation of lower bounds, while for primitive normal results hybrid additive and multiplicative characters sums are employed.



- 1 Introduction
- 2 Permutation Polynomials
- 3 Prescribed Coefficients
- 4 Combinatorial Arrays**
- 5 Integers and polynomials
- 6 Conclusions

## Global areas of Gary's research

It is difficult to briefly account for Gary's combinatorial work. Here is an incomplete list of combinatorial topics he has worked on:

- Latin squares;
- MOLS (mutually orthogonal Latin squares);
- orthogonal arrays;
- covering arrays;
- $(t, m, s)$ -nets;
- frequency permutation arrays;
- hypercubes;
- mutually orthogonal hypercubes;
- several types of designs;
- frequency magic squares;
- and many more kinds of combinatorial arrays.

## Key combinatorial contributions

His work spans constructions, enumeration, characterizations and applications of this diverse list of combinatorial objects.

**Latin Squares.** One of Gary's favorite topics! His popular textbook (with C.F. Laywine) develop several discrete mathematics themes using Latin squares. Gary has also extensively contributed to the theory of MOLS.

**Ordered Orthogonal Arrays.** OOAs, introduced by Gary (with W. Schmid) in 1996, are a generalization of **orthogonal arrays**. OOAs are related to  **$(t, m, s)$ -nets**. Niederreiter (1987) introduced  **$(t, m, s)$ -nets** which have several applications in numerical integration (quasi-Monte Carlo methods) and on the theory of uniform point distributions in unit cubes.

## Key combinatorial contributions (cont.)

**Covering Arrays.** CAs are yet another variant of orthogonal arrays, useful in some applications like software testing. An important contribution of Gary from 2005 (with C. Colbourn, S. Martirosyan, D. Shasha, B. Sherwood and J. Yucas) is on the construction of strength 2 covering arrays when we have different alphabet sizes for their factors (columns).

**Hypercubes and Mutually Orthogonal Hypercubes.** Another favorite topic of Gary. He started working on hypercubes on 1985; by now he has connections from these objects to all other arrays he has worked and to diverse areas such as geometry, coding theory, and designs.

- 1 Introduction
- 2 Permutation Polynomials
- 3 Prescribed Coefficients
- 4 Combinatorial Arrays
- 5 Integers and polynomials**
- 6 Conclusions

# Relations between integers and polynomials

Similar results for the decomposition of integers into primes can be derived for the decomposition of polynomials over finite fields into irreducibles. For example studies on the

- number of irreducible factors of a polynomial (number of primes of an integer);
- largest/smallest degree irreducible factor (largest/smallest prime);
- irreducibles (primes) in arithmetic progression; and so on.

Also some classical number theoretic problems have been translated to polynomials. For example, the [twin primes conjecture](#) has been proved for all finite fields of order bigger than 2.

## Relations between integers and polynomials (cont.)

In 2002, the [twin irreducible polynomials over finite fields](#) was studied (with G. Effinger and K. Hicks). Later, in 2005 (again with G. Effinger and K. Hicks), a more detailed comparison of the “two cousins”  $\mathbb{Z}$  and  $\mathbb{F}_q[x]$  is undertaken. This included some results about [additive](#) properties for polynomials related to [Goldbach conjecture](#) and their generalizations (sum of 3 irreducibles).

Gary proposed in 1995 a candidate for the [next Fermat problem](#). Devlin suggested that if a problem is to become the Next Fermat Problem, it [would have to be simple to state, easy for the layperson to understand, likely to defy attempts at a solution for many years, and require some heavy mathematical machinery when that solution does finally come](#). Gary suggests:

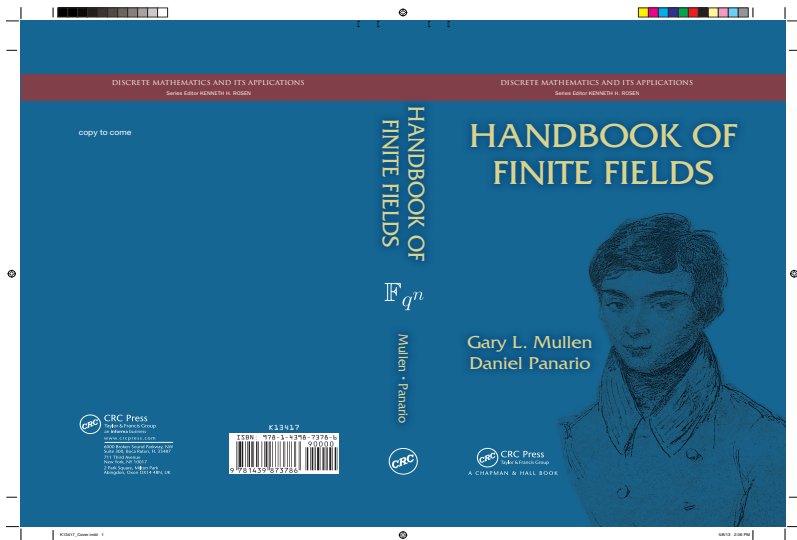
**Next Fermat Problem:** There exist  $n - 1$  MOLS of order  $n$  if and only if  $n$  is a prime power.

- 1 Introduction
- 2 Permutation Polynomials
- 3 Prescribed Coefficients
- 4 Combinatorial Arrays
- 5 Integers and polynomials
- 6 Conclusions**



After all this, then **what is Gary's most important contribution?**

After all this, then **what is Gary's most important contribution?**  
**I don't know!**



Happy 70 years young!

I wish you 70 more years of productive life!

Thank you Gary!