Research Statement

Neranga Fernando

My research interest lies in the area of *finite fields*, particularly, *permutation polynomials* over finite fields. Permutation polynomials have attracted a lot of attention in the last three decades due to their applications in many areas including cryptography, coding theory, combinatorics, and computer science.

My attention has also drawn to Quandle theory recently. Quandles are in general non-associative structures whose axioms correspond to the algebraic distillation of the three Reidemeister moves in knot theory. They were introduced independently in the 1980s by Joyce [38] and Matveev [45]. Quandles were used to construct representations of the braid groups.

Introduction

Let $\mathbb{F}_q$ denote the finite field of order q. It is a well-known fact that the characteristic of a finite field is prime. Let p be the characteristic of $\mathbb{F}_q$. A polynomial $f(x) \in \mathbb{F}_q$ is called a permutation polynomial (PP) of $\mathbb{F}_q$ if the induced mapping $x \mapsto f(x)$ is a permutation of $\mathbb{F}_q$. The general study of PPs started with Hermite who considered PPs over finite prime fields, but L.E. Dickson was the first person to study PPs over arbitrary finite fields. Following Dickson's work, many classes of PPs have been found, some of which include:

(1) monomials x^n

x^n is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q-1) = 1$.

(2) Dickson polynomials

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

$D_n(x,a)$ is a PP of $\mathbb{F}_q$ if and only if $\gcd(n, q^2-1) = 1$.

A key aspect of my research is finding new classes of PPs over finite fields.

Previous Research

In [34], X. Hou showed that for each integer $n \geq 0$, there exists a unique polynomial $g_{n,q} \in \mathbb{F}_p[\mathtt{x}]$ such that

$$\sum_{a \,\in\, \mathbb{F}_q} (\mathtt{x} + a)^n = g_{n,q}(\mathtt{x}^q - \mathtt{x}). \tag{1}$$

Permutation properties of the polynomial $g_{n,q}$ were first studied by X. Hou in [35]. He was interested in the positive integer triples $(n, e; q)$ for which the polynomial $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$. The results of this study indicate that the polynomial $g_{n,q}$ opens the door to many new classes of PPs in a new approach. Finding new classes of PPs is not easy in general. When I was a graduate student, my interest in the topic led me to read the three articles [33], [34], and [35] which increased my curiosity in this area of research. In [35], several families of PPs were found, but there were still many instances in which there was no theoretic explanation.

Since the polynomial $g_{n,q}$ turned out to be a rich source of PPs, I studied the permutation behaviour of the polynomial $g_{n,q}$. In my dissertation [26], I answered many of those unexplained cases that also deal with questions about $g_{n,q}$ that were not addressed in [35].

Constructing PPs of finite fields piecewise has been in discussion in numerous recent articles on permutation polynomials. I also constructed several families of PPs using the piecewise approach in my dissertation [26] that generalized some existing results (see [25] also).

In November 2014, I worked on the permutation behaviour of the polynomial $g_{n,q}$ over finite fields of even characteristic. The problem I was working on turned out to be more interesting than I thought and left me with the following question.

Let $\mathbb{F}_r \subset \overline{\mathbb{F}}_p$ and $q = r^m$. Assume that $z \in \overline{\mathbb{F}}_p$ satisfies an equation

$$\sum_{i=0}^{m-1} a_i f_i(z)^{r^i} = 0, \tag{2}$$

where $a_i \in \mathbb{F}_q$ and $f_i \in \mathbb{F}_r[\mathtt{X}]$ is q-linearized. Note that (2) is an r-linearized equation with coefficients in $\mathbb{F}_q$. Is it possible to derive from (2) a q-linearized equation with coefficients in $\mathbb{F}_r$?
This led to my colloboration with Xiang-dong Hou (See [29]). We showed that the answer to the afforementioned question is positive and such an equation indeed exists in a determinant form. We achieved a transition from an r-linearized equation with coefficients in $\mathbb{F}_q$ to a q-linearized equation with coefficients in $\mathbb{F}_r$. We used this transition to answer certain questions arising from the study of permutation polynomials defined by functional equations.

The advantage of a q-linearized polynomial $f \in \mathbb{F}_q[\mathtt{X}]$ over an r-linearized polynomial $g \in \mathbb{F}_q[\mathtt{X}]$ resides in a folklore in the study of finite fields. The conventional associate of f is a polynomial in $\mathbb{F}_q[\mathtt{X}]$ from which information about the roots of f can be easily extracted. On the other hand, the conventional associate of g is a skew polynomial over $\mathbb{F}_q$ which is not as convenient to use as the counterpart of f.

Most Recent Projects

Reversed Dickson Polynomials

The concept of the reversed Dickson polynomial (RDP) $D_n(a,x)$ was first introduced by Hou, Mullen, Sellers and Yucas in [33] by reversing the roles of the variable and the parameter in the Dickson polynomial $D_n(x,a)$. When $a \neq 0$,

$$D_n(a,x) = a^n D_n(1, \frac{x}{a^2}).$$

Hence $D_n(a,x)$ is a PP on $\mathbb{F}_q$ if and only if $D_n(1,x)$ is a PP on $\mathbb{F}_q$. When I first read [33] as a graduate student, I was captivated by the properties and the permutation behaviour of the reversed Dickson polynomials. In 2012, Wang and Yucas introduced the reversed Dickson polynomials of the $(k+1)$-th kind; see [55]. For $a \in \mathbb{F}_q$, the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ (see [23]) is defined by

$$D_{n,k}(a,x) = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} \frac{n-ki}{n-i} \binom{n-i}{i} (-x)^i a^{n-2i},$$

Motivated by articles on the RDPs of the first, second, third, and fourth kinds, I generalized numerous previously discovered results on the reversed Dickson polynomials of the $(k+1)$-th kind $D_{n,k}(a,x)$ over finite fields in [23].

I also explained the permutation behaviour of the reversed Dickson polynomials of the $(k+1)$-th kind $D_{n,k}(1,x)$ when $n = p^l + 2$ and n is a sum of odd prime powers in [20] and [18], respectively.

Self-Reciprocal Polynomials and Coterm Polynomials

The reciprocal $f^*(x)$ of a polynomial $f(x)$ of degree n is defined by $f^*(x) = x^n f(\frac{1}{x})$. A polynomial $f(x)$ is called *self-reciprocal* if $f^*(x) = f(x)$, i.e. if $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$, $a_n \neq 0$, is self-reciprocal, then $a_i = a_{n-i}$ for $0 \leq i \leq n$. Self-reciprocal polynomials have important applications in coding theory.

Coterm polynomials were introduced by Oztas, Siap, and Yildiz in [49]. They studied DNA codes over an extension ring of $\mathbb{F}_2 + u\mathbb{F}_2$ with the use of coterm polynomials.

Let R be a commutative ring with identity. Let $f(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in R[x]/(x^n - 1)$ be a polynomial, with $a_i \in R$. If for all $1 \leq i \leq \lfloor \frac{n}{2} \rfloor$, we have $a_i = a_{n-i}$, then $f(x)$ is said to be a coterm polynomial over R.

The classical way of constructing a reversible code is to find a self-reciprocal divisor of $x^n - 1$ and construct the cyclic code generated by that divisor. However, Oztas, Siap, and Yildiz explained a new way to construct reversible codes using coterm polynomials.

When p is odd, I showed in [23] that the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(1,x)$ can be written as

$$D_{n,k}(1,x) = \left(\frac{1}{2}\right)^n f_{n,k}(1-4x),$$

where

$$f_{n,k}(x) = k \sum_{j\geq 0} \binom{n-1}{2j+1} (x^j - x^{j+1}) + 2 \sum_{j\geq 0} \binom{n}{2j} x^j \ \in \mathbb{Z}[x] \tag{3}$$

for $n \geq 1$ and

$$f_{0,k}(x) = 2-k.$$

Explicit expressions for the RDPs for $k = 0, 1, 2$ and 3 appeared on several articles, and the above expression in (3) is a generalization of the previous explicit expressions for any k. When $k = 0, 1$, and 2, the self-reciprocal property of the explicit expressions had been used to find necessary conditions for the reversed Dickson polynomials to be a PP of $\mathbb{F}_q$. These observations led me to the question "when is $f_{n,k}$ a self-reciprocal polynomial?". In [21], I was able to answer the afformentioned question completely and classify all self-reciprocal polynomials arising from the reversed Dickson polynomials. As a consequence, I also obtained coterm polynomials arising from reversed Dickson polynomials.

Quandles

Quandles are algebraic structures whose axiomatization comes from Reidemeister moves in knot theory. A Quandle, X, is a set with a binary operation $(a, b) \mapsto a * b$ such that

(1) For any $a \in X$, $a * a = a$.
(2) For any $a, b \in X$, there is a unique $x \in X$ such that $a = x * b$.
(3) For any $a, b, c \in X$, we have $(a * b) * c = (a * c) * (b * c)$.

A *rack* is a set with a binary operation that satisfies (II) and (III). Racks and quandles have been studied extensively in, for example, [38, 45]. For more details on racks and quandles see the book [11].
The following are typical examples of quandles:

- A group G with conjugation as the quandle operation: $a * b = b^{-1}ab$, denoted by $X = \mathrm{Conj}(G)$, is a quandle.
- Any subset of G that is closed under such conjugation is also a quandle. More generally if G is a group, H is a subgroup, and σ is an automorphism that fixes the elements of H (*i.e.* $\sigma(h) = h\ \forall h \in H$), then G/H is a quandle with $*$ defined by $Ha * Hb = H\sigma(ab^{-1})b$.
- Any $\mathbb{Z}[t, t^{-1}]$-module M is a quandle with $a*b = ta+(1-t)b$, for $a, b \in M$, and is called an *Alexander quandle*.
- Let n be a positive integer, and for elements $i, j \in \mathbb{Z}_n$, define $i * j = 2j - i \pmod n$. Then $*$ defines a quandle structure called the *dihedral quandle*, and denoted by R_n, that coincides with the set of reflections in the dihedral group with composition given by conjugation.
- Any group G with the quandle operation: $a * b = ba^{-1}b$ is a quandle called Core(G).

My interest in quandles arose after reading the paper [12]. I had some valuable discussions on quandles with the first author of [12] that built up my spirit of inquiry. In the meantime, f-quandles were introduced.
An f-quandle is a set X equipped with a binary operation $* : X \times X \to X$ and a map $f : X \to X$ satisfying the following conditions:
For each $x \in X$, the identity

$$x * x = f(x) \tag{4}$$

holds. For any $x, y \in X$, there exists a unique $z \in X$ such that

$$z * y = f(x). \tag{5}$$

$$(x * y) * f(z) = (x * z) * (y * z) \tag{6}$$

We denote f-quandle by $(X, *, f)$.

Any $\mathbb{Z}[\omega^{\pm 1}, \beta]$-module M is an f-quandle with

$$x * y = \omega \cdot x + \beta \cdot y$$

for $x, y \in M$ with $\omega\beta = \beta\omega$, and we call it an *Alexander f-quandle* ([5, Example 2.1 item (4)]).
In general we do not require $\omega + \beta = 1$. When f is the identity map and $\beta = 1 - \omega$ above, then $(X, *)$ is a quandle and $(M, *)$ is an Alexander quandle as usual.
The productive discussions with the first author of [12] finally led to [6] where we explain the cocylce structure of the Alexander f-quandles on finite fields.
In 2017, V. G. Bardakov, I. B. S. Passi and M. Singh studied Quandle rings [4]. Motivated by their work, M. Elhamdadi, B. Tsvelikhovskiy and I further studied ring theoretic aspects of quandles [13]. We answered some open problems and confirmed a conjecture suggested in [4].

Differential Equations and Special Functions

It is shown in [44] that the Dickson polynomials of the first kind satisfy the homogeneous second order ordinary differential equaion

$$(x^2 - 4a)D_n''(x, a) + xD_n'(x, a) - n^2\, D_n(x, a) = 0$$

and the Dickson polynomials of the second kind satisfy the homogeneous second order ordinary differential equaion

$$(x^2 - 4a)E_n''(x, a) + 3xE_n'(x, a) - n(n + 2)\, E_n(x, a) = 0.$$

The curiosity to know whether the Dickson polynomials of the third kind satisfy a differential equation led me to a collaboration with S. Manukure (see [22]). We showed that the Dickson polynomials of the third kind $D_{n,2}(x, a)$ satisfy the non-homogeneous second-order linear ordinary differential equation.

$$(x^2 - 4a)\ D_{n,2}''(x, a) + 3x\ D_{n,2}'(x, a) - n^2\ D_{n,2}(x, a) = 2n\ D_n(x, a), \tag{7}$$

where $D_n(x, a)$ is the n-th Dickson polynomial of the first kind.
Moreover, we showed that the general solution to the associated homogeneous equation is enthralling since it involves the Associated Legendre functions which can be expressed in terms of the gamma function and hypergeometric functions.

Fibonacci Permutation polynomials

Fibonacci polynomials were first studied in 1833 by Eugene Charles Catalan. Since then, Fibonacci polynomials have been extensively studied by many for their general and arithmetic properties; see [1, 7, 30, 41, 42, 53, 56]. In a recent paper, Koroglu, Ozbek and Siap studied cyclic codes that have generators as Fibonacci polynomials over finite fields; see [40]. In another recent paper, Kitayama and Shiomi studied the irreducibility of Fibonacci polynomials over finite fields; see [39].
Fibonacci polynomials are defined by the recurrence relation $f_0(x) = 0,\ f_1(x) = 1$, and

$$f_n(x) = xf_{n-1}(x) + f_{n-2}(x),\ \text{for } n \geq 2.$$

The Fibonacci polyomial sequence is a generalization of the Fibonacci number sequence: $f_n(1) = F_n$ for all n, where F_n denotes the n-th Fibonacci number. Moreover, $f_n(2)$ defines the well-known *Pell numbers* $1, 2, 5, 12, 19, \ldots$. Fibonacci polynomials can also be extended to negative subscripts (see [41, Chapter 37]):

$$f_{-n}(x) = (-1)^{n+1} f_n(x).$$

In [15], one of my undergraduate research students, M. Rashid, and I gave a complete classification of self-reciprocal polynojmials arising from Fibonacci polynomials over $\mathbb{Z}$ and $\mathbb{Z}_p$, where $p = 2$ and $p > 5$. We also presented some partial results when $p = 3, 5$. We also computed the first and second moments of Fibonacci polynomials $f_n(x)$ over finite fields, which give necessary conditions for Fibonacci polynomials to be permutation polynomials over finite fields.

Polynomial $g_{n,q}$

In [16], I explained a class of permutation polynomials over $\mathbb{F}_{q^{3k}}$, where $q = 4$ and k a positive integer. I also presented a generalization.

Dembowski-Ostrom polynomials arising from reversed Dickson polynomials of the $(k+1)$-th kind

A Dembowski-Ostrom (DO) polynomial over finite field $\mathbb{F}_q$ is a polynomial that admits the following shape

$$\sum_{i,j} a_{ij} X^{p^i + p^j},$$

where $a_{ij} \in \mathbb{F}_q$. A function $f : \mathbb{F}_q \to \mathbb{F}_q$ is called planar if the mapping $X \mapsto f(X+\epsilon) - f(X) - f(\epsilon)$ induces a bijection from $\mathbb{F}_q$ to $\mathbb{F}_q$ for each $\epsilon \in \mathbb{F}_q^*$.

DO polynomials have been used in designing a public key cryptosystem known as HFE [50]. They also provide a very rich source of planar functions. It was conjectured by Rónyai and Szönyi [52] (see also [48, Conjecture 9.5.19]) that all planar functions are of "DO type". This conjecture is still open except in the case of characteristic 3 for which a counter example was given by Coulter and Matthews [9]. In 2010, Coulter and Matthews [10] classified DO polynomials from Dickson polynomials of the first and second kind and they also discussed the planarity of such DO polynomials.

In 2016, Zhang, Wu and Liu [57] classified DO polynomials from RDPs of the first kind in the even characteristic case and they also characterized APN functions among all such DO polynomials. In [14], I, together with Sartaj Ul Hasan and Mohit Pal at IIT Jammu, India, extended the results of Zhang, Wu and Liu [57] to the odd characteristic case. In fact, we were able to give a complete classification of DO polynomials arising from the composition of RDPs of the $(k+1)$-th kind and the monomial X^d, where d is a positive integer, in odd characteristic, and we further characterized planar functions among these DO polynomials.

Current Research

Polynomial $g_{n,q}$

I am currently working on the permutation polynomials over finite fields of even characteristic defined by functional equations ([19]). As time permits, I am also working on the open problems in [27].

Reversed Dickson Polynomials

Having noticed something interesting, I am trying to determine if there is a connection between reversed Dickson polynomials and Catalan numbers.

Future Research

Below are some of the topics, not limited to, that I am interested in working on in the future. I am also open to investigate other areas of Mathematics.

Polynomial $g_{n,q}$

There are still a lot of unexplained integer triples $(n, e; q)$ for which the polynomial $g_{n,q}$ is a PP of $\mathbb{F}_{q^e}$; see the tables in [27] and [29]. Coming up with criterions to explain the permutation behaviour of the polynomial $g_{n,q}$ completely is one of my main goals in the future. Orthomorphism polynomials over finite fields arising from polynomial $g_{n,q}$ would be an interesting project to work on as well.

Dickson Polynomials

In [55], Steven Wang and Joseph L. Yucas studied the permutation behavior of Dickson polynomials of the third kind. They only completely described the permutation behavior of the Dickson polynomial of the third kind over any prime field, and hinted that a similar result is expected to be true over $\mathbb{F}_{q^2}$. I am very interested in starting from where they stopped. I believe that the piecewise definition in [55, Theorem 2.10] will play a major role in future work on the permutation behaviour of Dickson polynomials over finite fields.

Reversed Dickson Polynomials

PP classification of RDPs over $\mathbb{F}_p$ and the permutation behaviour of RDPs over $\mathbb{F}_q$ when q is a prime power are two problems that I am really interested in considering in the future. It would also be handy to find more explicit conditions on k, n, and q for which the n-th reversed Dickson polynomial of the $(k+1)$-th kind $D_{n,k}(a,x)$ is a PP of $\mathbb{F}_q$.

Jacobsthal Polynomials and Integer Sequences

Having read my paper [24] on ArXiv, G. C. Greubel pointed out that the reversed Dickson polynomials of the third kind are related to Jacobsthal Polynomials and Integer Sequences. I am really interested in exploring this relationship further in the future.

Coding Theory

As mentioned before, Self-reciprocal polynomials and coterm polynomials have important applications in coding theory. I would definitely expand my work in [21] in the future since coding theory is an area that has fascinated me since I was a graduate student.

Complete Permutation Polynomials

A permutation polynomial $f(x)$ over a finite field $\mathbb{F}_q$ is called a *complete permutation polynomial*, if $f(x)+x$ is also a permutation polynomial. There are a few open problems on complete permutation polynomials that I am interested in.

Dickson Polynomials of the Second Kind

Permutation behavior of Dickson polynomial of the second kind (DPSK) has been studied in numerous recent articles. But most of the explanations of PP behavior of DPSK have been heavily based on computer software and Grobner bases. I have already conducted a computer search for the PP behaviour of DPSK of which the results suggest that it would be an interesting area to spend time on. I intend to conduct a study of the PP behavior of DPSK in future and find ways to explain its PP behavior in a manner similar to polynomial $g_{n,q}$.

Quandles

The article [13] on ring theoretic aspects of quandles left us with some new ideas and open problems. I am very interested in working on them in the future.

I also have projects on complete permutation polynomials, Dickson polynomials of the second kind, reversed Dickson polynomials, Fibonacci polynomials, and quandles which could be of interest to undergraduate students and graduate students.

References

[1] W. M. Abd-Elhameed, Y. H. Youssri, N. El-Sissi, M. Sadek, *New hypergeometric connection formulae between Fibonacci and Chebyshev polynomials*. Ramanujan J. 42 (2017), no. 2, 347–361.

[2] K. Ameur, M. Saito, *Polynomial cocycles of Alexander quandles and applications*, J. Knot Theory Ramifications 18 (2009), no. 2, 151–165.

[3] S. Abe, *On 4-cocycles of Alexander quandles on finite fields*, J. Knot Theory Ramifications 23 (2014), no. 8, 1450043, 30 pp.

[4] V. G. Bardakov, I. B. S. Passi, M. Singh, *Quandle rings*. arXiv:1709.03069, 2017.

[5] I. R. U. Churchill, M. Elhamdadi, M. Green, A. Makhlouf, *f-racks, f-quandles, their extensions and cohomology*, J. of Algebra and Its Appl., Vol. 16, no. 11 (2017).

[6] I. R. Churchill, M. Elhamdadi, N. Fernando, *Co-cylce structure of twisted Alexander quandles*, Journal of Algebra and its Applications (Available online).

[7] J. Cigler, *q-Fibonacci polynomials*. Fibonacci Quart. 41 (2003), no. 1, 31–40.

[8] S. D. Cohen, *Dickson polynomials of the second kind that are permutations*, Can. J. Math. **16** (1994), 225 – 238.

[9] R.S. Coulter, R.W. Matthews, *Planar functions and planes of Lenz-Barlotti class II*, Des. Codes Cryptogr., 10 (1997) 167-184.

[10] R. S. Coulter, R. W. Mattews, *Dembowski-Ostrom polynomials from Dickson polynomials*, Finite Fields Appl., 16 (2010) 369-379.

[11] M. Elhamdadi, S. Nelson, *Quandles—an introduction to the algebra of knots*, Student Mathematical Library, 74, American Mathematical Society, Providence, RI, 2015, x+245.

[12] M. Elhamdadi, J. MacQuarrie, R. Restrepo, *Automorphism groups of Quandles*, J. Algebra Appl. 11 (2012), no. 1.

[13] M. Elhamdadi, N. Fernando, B. Tsvelikhovskiy, *Ring theoretic aspects of quandles.* (Submitted for publication) arXiv:1805.05908

[14] N. Fernando, S.U. Hasan, M. Pal, *Reversed Dickson polynomials, Dembowski-Ostrom polynomials, and planar functions.* Accepted in Discrete Applied Mathematics (2021). arXiv: 1905.01767

[15] N. Fernando, M. Rashid, *Fibonacci Permutation Polynomials.* (submitted for publication) arXiv:1712.07723

[16] N. Fernando, *A note on the permutation behaviour of the polynomial $g_{n,q}$.* (submitted for publication) arXiv:1805.06309

[17] N. Fernando, M. Rashid, *Fibonacci Permutation Polynomials.* (submitted for publication) arXiv:1712.07723

[18] N. Fernando, *Reversed Dickson polynomials of the $(k+1)$-th kind over finite fields, II.* (submitted for publication) arXiv:1706.01391

[19] N. Fernando, *Permutation polynomials over finite fields of even characteristic defined by functional equations*, in preparation.

[20] N. Fernando, *A note on permutation binomials and trinomials over finite fields.* New Zealand J. Math. 48 (2018), 25-29.

[21] N. Fernando, *Self-reciprocal polynomials and coterm polynomials*, Des. Codes Cryptogr. 86 (2018), no. 8, 1707-1726.

[22] N. Fernando, S. Manukure, *A representation of the Dickson polynomials of the third kind by Legendre functions*, submitted. arXiv:1604.04682.

[23] N. Fernando, *Reversed Dickson polynomials of the $(k+1)$-th kind over finite fields*, J. Number Theory **172** (2017), 234 – 255. Available Online.

[24] N. Fernando, *Reversed Dickson polynomials of the third kind.* In: Gloria Scientiam. University of Kelaniya, Sri Lanka (2017), Chapter 50: 585-598. arXiv:1602.04545

[25] N. Fernando, X. Hou, *A piecewise construction of permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012), 1184 – 1194.

[26] N. Fernando, *A study of permutation polynomials over finite fields*, Ph.D. Dissertation, University of South Florida, Tampa, FL, USA (2013).

[27] N. Fernando, X. Hou, S. D. Lappano, *A new approach to permutation polynomials over finite fields,* II, Finite Fields Appl. **22** (2013), 122 – 158.

[28] N. Fernando, X. Hou, S. D. Lappano, *Permutation polynomials over finite fields involving* $\mathtt{x}+\mathtt{x}^q+\cdots+\mathtt{x}^{q^{a-1}}$, Discrete Math., **315-316** (2014), 173 – 184.

[29] N. Fernando, X. Hou, *From r-linearized polynomial equations to r^m-linearized polynomial equations*, Finite Fields Appl. **37** (2016), 14 – 27.

[30] V.E. Hoggatt, Jr., M. Bicknell, *Roots of Fibonacci polynomials.* Fibonacci Quart. 11 (1973), no. 3, 271–274.

[31] S. Hong, X. Qin, W. Zhao, *Necessary conditions for reversed Dickson polynomials of the second kind to be permutational*, Finite Fields Appl. **37** (2016), 54 – 71.

[32] X. Hou, T. Ly, *Necessary conditions for reversed Dickson polynomials to be permutational*, Finite Fields Appl. **16** (2010), 436 – 448.

[33] X. Hou, G. L. Mullen, J. A. Sellers, J. L. Yucas, *Reversed Dickson polynomials over finite fields*, Finite Fields Appl. **15** (2009), 748 – 773.

[34] X. Hou, *Two classes of permutation polynomials over finite fields*, J. Combin. Theory A, **118** (2011), 448 – 454.

[35] X. Hou, *A new approach to permutation polynomials over finite fields*, Finite Fields Appl. **18** (2012), 492 – 521.

[36] X. Hou, *Automorphism groups of Alexander quandles.* J. Algebra 344 (2011), 373-385.

[37] X. Hou, *Finite modules over $\mathbb{Z}[t,t^{-1}]$.* J. Knot Theory Ramifications 21 (2012), no. 8, 1250079, 28 pp.

[38] D. Joyce, *A classifying invariant of knots, the knot quandle,* J. Pure Appl. Alg., 23, 37-65.

[39] H. Kitayama, D. Shiomi, *On the irreducibility of Fibonacci and Lucas polynomials over finite fields.* Finite Fields Appl. 48 (2017), 420 – 429.

[40] M. E. Koroglu, I. Ozbek, I. Siap, *Optimal codes from Fibonacci polynomials and secret sharing schemes.* Arab. J. Math. (Springer) 6 (2017), no. 4, 297–308.

[41] T. Koshy, *Fibonacci and Lucas numbers with applications*. Pure and Applied Mathematics (New York). Wiley-Interscience, New York, 2001. xviii+652 pp.
[42] D. Levy, *The irreducible factorization of Fibonacci polynomials over* $\mathbb{Q}$. Fibonacci Quart. 39 (2001), no. 4, 309 – 319.
[43] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.
[44] R. Lidl, G. L. Mullen, G. Turnwald, *Dickson polynomials*, Longman Scientific and Technical, Essex, United Kingdom, 1993.
[45] S. Matveev, *Distributive groupoids in knot theory,* (Russian) Mat. Sb. (N.S.) 119(161) (1982), no. 1, 78–88, 160.
[46] T. Mochizuki, *The 3-cocycles of the Alexander quandles* $\mathbb{F}_q[T]/(T-\omega)$, Algebr. Geom. Topol. 5 (2005), 183–205.
[47] T. Mochizuki, *Some calculations of cohomology groups of finite Alexander quandles*, J. Pure Appl. Algebra (2003), 287-330.
[48] G.L. Mullen, D. Panario, *Handbook of Finite Fields. Series: Discrete Mathematics and Its Applications*, CRC Press (2013).
[49] E. S. Oztas, I. Siap, B. Yildiz, *Reversible codes and applications to DNA*, Lecture Notes in Comput. Sci., 8592, Springer, Heidelberg, 2014.
[50] J. Patarin, *Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new familiees of asymmetric algorithms*, Advances in Cryptology - Eurocrypt '96 (U. Maurer, ed.), Lecture Notes in Comput. Sci., vol. 1070 (1996) 33-48.
[51] V. Pless, *Introduction to the theory of error-correcting codes*, Third edition. Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1998. xiv+207 pp.
[52] L. Rónyai, T. Szönyi, *Planar functions over finite fields*, Combinatorica, Vol. 9 (1989) 315-320.
[53] Y. Tasyurdu, O. Deveci, *The Fibonacci polynomials in rings.* Ars Combin. 133 (2017).
[54] L. Vendramin, *Doubly transitive groups and cyclic quandles*, J. Math. Soc. Japan, 69, 2017, 3, 1051–1057.
[55] Q. Wang, J. L. Yucas, *Dickson polynomials over finite fields*, Finite Fields Appl. **18** (2012), 814 – 831.
[56] Y. Yuan, W. Zhang, *Some identities involving the Fibonacci polynomials*, Fibonacci Quart. 40 (2002), no. 4, 314 – 318.
[57] X. Zhang, B. Wu, Z. Liu, *Dembowski-Ostrom polynomials from reversed Dickson polynomials*, J. Syst. Sci. Complex., 29 (2016) 259-271.