ARITHMETIC PROPERTIES IN TWO DIFFERENT STRUCTURES: CHARACTERIZATION OF POLYNOMIALS AND r-FREE INTEGERS

VEASNA KIM

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN APPLIED MATHEMATICS

DEPARTMENT OF MATHEMATICS SCHOOL OF SCIENCE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2022
KMITL-2022-SC-D-001-111

Thesis Title	Arithmetic Properties in Two Different Structures: Characterization of Polynomials and r-Free Integers
Student Name	Veasna Kim
Student ID	62605009
Degree	Doctor of Philosophy (Applied Mathematics)
Department	Mathematics
Year	2022
Thesis Advisor	Asst. Prof. Dr. Sukrawan Mavecha
Thesis Co-Advisors	Prof. Dr. Vichian Laohakosol Assoc. Prof. Dr. Teerapat Srichan

Abstract

In this dissertation, there are two different parts, the first part is about a divided-difference characterization of polynomials over a finite field of characteristic two, the second part is about the distribution of r-free integers in Beatty sequences.

In the first part, let $\mathbb{F}$ be a finite field of characteristic 2 and let n be an integer ≥ 3. For a function $f : \mathbb{F} \to \mathbb{F}$, if there is a function $h : \mathbb{F} \to \mathbb{F}$ such that the divided difference $f[x_1, \ldots, x_n]$ on any n distinct elements of $\mathbb{F}$ satisfies $f[x_1, \ldots, x_n] = h(x_1 + \cdots + x_n)$, then f is a polynomial of degree at most n over $\mathbb{F}$. This result complements an earlier work of Davies and Rousseau.

In the second part, let $r \geq 2$ be a fixed integer. A positive integer n is called r-free if in its canonical representation into prime powers each exponent is $< r$. The integer 1 is considered to be r-free. We consider $Q_r(x; \alpha, \beta)$, the number of r-free integers lying in a Beatty sequence $\lfloor \alpha n + \beta \rfloor, 1 \leq n \leq x$, for an irrational $\alpha > 1$ with bounded partial quotients, and $\beta \in [0, \alpha)$. We prove that, as $x \to \infty$, $Q_r(x; \alpha, \beta) = \frac{x}{\zeta(r)} + O(x^{(r+1)/2r} \log^3 x)$, which improves Victorovich's result in the case of square-free integers. Moreover, we also prove there exist infinitely many consecutive square-free numbers of the forms $\lfloor \alpha n + \beta \rfloor, \lfloor \alpha n + \beta \rfloor + 1$, which improves Dimitrov's result in 2019.

Keywords : Divided-difference, Finite field, Characteristic 2, Polynomial, Beatty sequence, r-free number, Square-free number.

Acknowledgements

I would like to express my heartfelt gratitude to my advisor, Assistant Professor Dr. Sukrawan Mavecha and my co-advisors Professor Dr. Vichian Laohakosol and Associate Professor Dr. Teerapat Srichan, respectively from King Mongkut's Institute of Technology Ladkrabang, Kasetsart University and Kasetsart University, for ancillaries of my PhD study and associated research, for their endurance, kind-hearted, enthusiasm and immense knowledge. Their supervisions helped me in all time of research and writing of this dissertation. Their kinding care always make me feel so warm and comfortable in my PhD life. I could not have fantasized having the amazing advisors and mentors for my PhD study like my Lecturers.

In addition, I would like to thank Associate Professor Dr. Boonrod Yuttanan, the thesis chairman from Prince of Songkla University and Assistant Professor Dr. Puttha Sakkaplangkul, Associate Professor Dr. Puntani Pongsumpun and Assistant Professor Dr. Thawachai Khumprapussorn, from King Mongkut's Institute of Technology Ladkrabang, for their precious time out of busy schedule to be my thesis commitee.

Moreover, I would like to express my honorable sincerity and appreciation to King Mongkut's Institute of Technology Ladkrabang for financial support during my PhD study and research.

Afterwards, I would like to acknowledge to Ministry of Education, Youth and Sport (Cambodia) which allowed me to pursue postgraduate studies as a state framework teacher.

Subsequently, I would like to thank Associate Professor Dr. Suppawadee Prugsapitak from Prince of Songkla University for her help and encouragement before my PhD study.

Before the last, I would like to thank to all my lecturers of the mathematics department, school of science, KMITL for teaching me along my study. I also would like to thank to all friends for their supports.

First and foremost, I wish to thank to my family, my beloved wife Rachna Neang and my little baby daughter Narasana for always giving a helping hand, supporting, encouraging me in my study and research.

Veasna Kim,

Table of Contents

List of Tables

Table **Page**

Notations

Throughout this thesis, the following symbols is adopted.

Symbol	Meaning
$\mathbb{R}$	the set of real numbers
$\mathbb{N}$	the set of positive integers
$\mathbb{Z}$	the set of integers
$\mathbb{Q}$	the set of rational numbers
$\mathbb{C}$	the set of complex numbers
$\mathbb{F}$	the field $\mathbb{F}$
$\lvert\mathbb{F}\rvert$	the cardinality of $\mathbb{F}$
$\mathbb{F}_q$	the finite field of order q
$\mathbb{F}_{2^\ell}, GF(2^\ell)$	the finite field of oder 2^ℓ with charateristic 2 or Galois field of oder 2^ℓ
$\mathrm{ch}(\mathbb{F})$	the characteristic of $\mathbb{F}$
$\mathbb{Z}/p\mathbb{Z}$	the integer modulo p
$\mathbb{F}[x]$	the set of polynomial in x with coefficients in $\mathbb{F}$
$[\mathbb{F}]^{=n}$	the set of n distinct elements $x_1, \ldots, x_n$ in $\mathbb{F}$
$f : K \to K$	the function f over K
$f(x)$	the polynomial f in x
$f(a)$	the value of f at the point a
$\deg f$	the degree of the polynomial f
$\sum S$	the sum of all elements in the set S
$x(m; i_1 : i_m)$	the elements in $\mathbb{F}_{2^\ell}$ such that $x(m; i_j : i_m) := \alpha^{i_1} + \alpha^{i_2} + \cdots + \alpha^{i_m}$ for $m \in \{1, 2, \ldots, \ell\}, 0 \le i_1 \le i_2 \le \cdots \le i_m \le \ell - 1$
$f[x_1, \ldots, x_n]$	the n-th order divided-difference on n distict elemnts $x_1, \ldots, x_n$
$f[X]$	the divided-defference $f[X] = f[x_1, \ldots, x_n]$ where $X = \{x_1, \ldots, x_n\} \in [\mathbb{F}]^{=n}$
$[a_0; a_1, \ldots, a_j]$	the simple form of continued fraction
P	the finite set of prime numbers
$[x]$	the greatest integer function on real number x which is the greatest integer less than or equal x
$\lfloor f(n) \rfloor$	the series of integers such that each n-th term is the greatest integers less than or equal $f(n)$
$\mathbb{N}^c$	the Piateske-Shapiro sequence $\mathbb{N}^c = \{\lfloor n^c \rfloor : n \in \mathbb{N}, c \in \mathbb{R}, c > 1\}$
$[a, b)$	$[a, b) = \{x \in \mathbb{R} : a \le x < b\}$
$\zeta(s)$	Riemann zeta function
$\mu(n)$	Möbius function
$\sigma_\alpha(n), \sigma(n), d(n)$	divisor function

$\varphi(n)$	Euler phi function
$\omega_\alpha(x)$	Characteristic function
$\gcd(a,b), (a,b)$	the greatest comon divisor of a and b
$\bar{x}$	the modulo residul class x
$S(N,\alpha)$	the number of positive integers $n \leq N$ such that $\lfloor \alpha n \rfloor$ and $\lfloor \alpha n \rfloor + 1$ are square-free
$A_c^2(x)$	the number of quadruples d,t,u,v of positive integers satisfying the conditions $t^2v - d^2u = 1, \quad d^2u \leq x^c, \quad x^{c/2} < dt \leq x^{2c/3}$
$A_c^3(x)$	the number of quadruples d,t,u,v of positive integers satisfying the conditions $t^2v - d^2u = 1, \quad d^2u \leq x^c, \quad dt > x^{2c/3}$
$A_{\alpha,\beta}(x)$	the number of quadruples d,t,u,v of positive integers satisfying the conditions $t^2v - d^2u = 1, \quad d^2u \leq \alpha x + \beta, \quad x^{1/4} < dt \leq x^{2/3}$
$B_{\alpha,\beta}(x)$	the number of quadruples d,t,u,v of positive integers satisfying the conditions $t^2v = d^2u = 1, \quad d^2u \leq \alpha x + \beta, \quad dt > x^{2/3}$
$f(x) = O(g(x))$	$f(x)$ is big oh of $g(x)$.
$f(x) \ll g(x)$	$f(x)$ is big oh of $g(x)$.
$f(x) \sim g(x)$	$f(x)$ is asymptotic to $g(x)$ as $x \to \infty$.
$Q_r(x;\alpha,\beta)$	the number of r-free of Beatty sequence $\lfloor \alpha n + \beta \rfloor$, $1 \leq n \leq x$
$T_{\alpha,\beta}(x)$	the number of positive integers $n \leq x$ such that $\lfloor \alpha n+\beta \rfloor$ and $\lfloor \alpha n+\beta \rfloor+1$ are square-free

Chapter 1

Introduction

This chapter consists of five sections: research motivation, objectives of the study, scope of the study, benefits of the study and research methodology.

1.1 Research motivation

There are two different works in this dissertation, the first is about divided-differences characterization of polynomials over a finite field of characteristic two and the second is about r-free integers in Beatty sequences.

In the first part of this dissertation, let $\mathbb{F}$ be a field. Then the divided-differences [1] on distinct points $x_1, x_2, x_3, \ldots$ in $\mathbb{F}$ of a function $f : \mathbb{F} \to \mathbb{F}$ are defined by

$$f[x_1] = f(x_1), \qquad f[x_1, x_2] = \frac{f(x_1) - f(x_2)}{x_1 - x_2},$$

and inductively for $k > 2$ by

$$f[x_1, \ldots, x_k] = \frac{f[x_1, \ldots, x_{k-1}] - f[x_2, \ldots, x_k]}{x_1 - x_k};$$

keeping in mind that the divided differences are well-defined so long as there are enough distinct elements to do so. It is not difficult, using [2, Lemma 1], to see that if $f(x) := a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ is a polynomial of degree $n \in \mathbb{N}$, then

$$f[x_1, \ldots, x_n] = a_n(x_1 + \cdots + x_n) + a_{n-1}, \tag{1.1}$$

i.e., the divided-differences on n distinct points $x_1, \ldots, x_n$ of a polynomial of degree n can be expressed as function in $x_1 + \cdots + x_n$. There then arises the question whether the converse of this result is true, i.e., if there exists a function $h : \mathbb{F} \to \mathbb{F}$ satisfying

$$f[x_1, \ldots, x_n] = h(x_1 + \cdots + x_n) \tag{1.2}$$

for any n distinct points $x_1, \ldots, x_n$ in $\mathbb{F}$, is f necessarily a polynomial of degree at most n over $\mathbb{F}$? We refer to this question as the **DDCP (divided-differences characterization of polynomials problem)**. There are many authors have studied about this problem as describe below.

The case where $n = 2$ and $\mathbb{F}$ is a field of characteristic $\neq 2$ was solved by Aczél [3] in a more general form. Bailey [4] solved the DDCP in the case where f is a differentiable function, $\mathbb{F} = \mathbb{R},\ n = 3$. In 1994, Schwaiger [2] solved the DDCP when $n \geq 2$ with $\mathbb{F}$ any field of characteristic $\neq 2$ having cardinality $\geq 8(n-2)+2$; at the end of his paper, he mentioned that the bound can be reduced to $6(n-2)+2$. Andersen [5] solved the DDCP when $\mathbb{F} = \mathbb{R}$ and $n \geq 2$. Finally, Davies and Rousseau [6] resolved the

DDCP for $n \geq 2$ with $\mathbb{F}$ any field of characteristic $\neq 2$. In the appendix of their paper, Davies and Rousseau proved also that the DDCP holds for $\mathbb{F} = GF(2)$ and $GF(4)$, finite fields of order 2, respectively 4, but fails for fields of characteristic 2 with cardinality > 4. The case of $GF(2)$ is easily disposed of because every function is a linear polynomial. For the case $GF(4)$, since every function is a polynomial of degree ≤ 3, they show that no polynomial of degree 3 satisfies (1.2) for $n = 2$. As to the case where $\mathbb{F}$ is of characteristic 2 with cardinality > 4, they constructed a counter-example to the DDCP when $n = 2$. Thus our work in this part is to show that the result of Davies and Rousseau also true for the field of characteristic two with $n \geq 3$ that will make their work complete.

In the second part of this dissertation, we will study about r-free integer in Beatty sequences. In this part, let r be a fixed integer ≥ 2. A positive integer n is called r-free if in the canonical representation of n into prime powers each exponent is $< r$. By convention, a 2-free integer is called square-free. The problem for the existence of square -free numbers in the Beatty sequences arose in 2008. Güloğlu and Nevans [7] proved that

$$\sum_{\substack{n \leq x \\ \lfloor \alpha n \rfloor \text{ is square-free}}} 1 = \frac{x}{\zeta(2)} + O\Big(\frac{x \log\log x}{\log x}\Big),$$

where $\alpha > 1$ is irrational number of finite type. In 2009 Abercrombie and Banks [8] showed that

$$\sum_{\substack{n \leq x \\ \lfloor \alpha n \rfloor \text{ is square-free}}} 1 = \frac{x}{\zeta(2)} + O\Big(x^{2/3} \log N\Big),$$

for almost all $\alpha > 1$. Recently in 2013 Victorovich [9] showed that

$$\sum_{\substack{n \leq x \\ \lfloor \alpha n \rfloor \text{ is square-free}}} 1 = \frac{x}{\zeta(2)} + O\Big(Ax^{5/6} \log^5 N\Big), \tag{1.3}$$

where $\alpha > 1$ is irrational number with bounded partial quotient or irrational algebraic number. Here $A = \max\{\tau(m), 1 \leq m \leq x^2\}$.

The consecutive square-free numbers is an attractive problem. The distribution of the consecutive square-free is studied by many authors (see [10, 11, 12]). In particular, the existence of infinitely many consecutive square-free numbers of the form $\lfloor f(n) \rfloor,\ \lfloor f(n) \rfloor + 1$ is also studied. In 2018 Dimitrov [13] proved that for any fixed $1 < c < 7/6$, there exist infinitely many consecutive square-free integers of the form $\lfloor n^c \rfloor,\ \lfloor n^c \rfloor + 1$ by showing that

$$\sum_{\substack{x/2 < n \leq x \\ \lfloor n^c \rfloor,\, \lfloor n^c \rfloor + 1 \text{ are square-free}}} 1 = \frac{1}{2} \prod_p \Big(1 - \frac{2}{p^2}\Big) x + O\Big(x^{\frac{6c+1}{8} + \varepsilon}\Big), \qquad \text{for } 1 < c < \frac{7}{6}. \tag{1.4}$$

Very recently, Tangsupphathawat, Srichan and Laohakosol [14] improved the range of c and the error term in Dimitrov's work in (1.4) and showed that, for $1 < c < 3/2$, and sufficiently small $\varepsilon > 0$, we have

$$\sum_{\substack{n\le x\\ \lfloor n^c\rfloor,\, \lfloor n^c\rfloor+1 \text{ are square-free}}} 1 = \prod_p \Big(1-\frac{2}{p^2}\Big)x + O\Big(x^{\frac{2c+1}{4}+\varepsilon}\Big) \qquad (x\to\infty).$$

On the other hand in [15] Dimitrov used the method of Victorovich in [9] to showed that for $\alpha > 1$ be irrational number with bounded partial quotient or irrational algebraic number,

$$\sum_{\substack{n\le x\\ \lfloor \alpha n\rfloor,\, \lfloor \alpha n\rfloor+1 \text{ are square-free}}} 1 = \prod_p \Big(1-\frac{2}{p^2}\Big)x + O\Big(x^{\frac{5}{6}+\varepsilon}\Big). \tag{1.5}$$

Hence in this part, we will give other asymptotic formula for r-free numbers in Beatty sequence by using the result on the number of values of Beatty sequence $\lfloor \alpha n+\beta\rfloor$, in an arithmetic progression in [16] and then improve the formula (1.5) by using the similar idea as in [14].

1.2 Objectives of the study

1) To show that the counter-example of Davies-Rousseau is exceptional in the sense that for all $n \ge 3$, the DDCP holds for any finite field of characteristic 2 with cardinality $\ge \max(n, 2^2)$.

2) To prove an asymptotic formula for r-free numbers in a Beatty sequence by using results on the number of elements in Beatty sequence $\lfloor \alpha n+\beta\rfloor$, belonging to an arithmetic progression in [16].

3) To extend the formula of consecutive square-free numbers (1.5) from $\lfloor \alpha n\rfloor$, $\lfloor \alpha n\rfloor + 1$ to $\lfloor \alpha n+\beta\rfloor$, $\lfloor \alpha n+\beta\rfloor + 1$, by using ideas from [14].

1.3 Scope of the study

Our main objects are arithmetic properties of two structures where the domain of the first work is on the finite field of characteristic two and the domain of the second work is the set of real numbers and whose range is the set of natural numbers. Aspects of these structures to be investigated are

1) divided-differences on n distinct points of polynomial over field of characteristic two,

2) generalized Möbius function, divisor function and their basic properties,

3) r-free numbers, sqare-free numbers, Beatty sequence.

1.4 Benefits of the study

1) Characterization of divided differences of polynomial over finite field of characteristic two and making the result of Davies-Rousseau complete.

2) Asymptotical formula for r-free numbers and square-free numbers in Beatty sequence $\lfloor \alpha n + \beta \rfloor$ are obtained.

3) Counting formulae from the problems of consecutive sqare-free numbers in Beatty sequence $\lfloor \alpha n + \beta \rfloor, \lfloor \alpha n + \beta \rfloor + 1$ is obtained.

1.5 Research methodology

1) Study basic properties of the finite field, the properties of divided differences of polynomial over finite field [6], properties of Möbius function, Beatty sequences and their properties [16].

2) Study some advanced topics in algebra, abstract algebra, linear algebra, analytic number theory.

3) Characterize the result of Davies and Rousseau in a finite field of characteristic two.

4) Apply the methods of Dimitrove [13] and Tangsupphawat et al [14] to solve the problems of the r-free integer in Beatty sequences $\lfloor \alpha n + \beta \rfloor, \lfloor \alpha n + \beta \rfloor + 1$.

5) Summarize all the results so obtained and write a thesis.

Table 1.1: The research schedule

Activity	Time frame					
	2019	2020		2021		2022
	Aug.-Dec.	Jan.-Jun.	Jul.-Dec.	Jan.-Jun.	Jul.-Dec.	Jan.-Aug.
Step 1	→					
Step 2		→				
Step 3			→			
Step 4				→		
Step 5						→

Chapter 2

Preliminaries

In this chapter, we will recall some definitions, properties, theorems and examples that will be used throughout our study.

2.1 Background in algebra

Definition 2.1. [17] A **field** is a set $\mathbb{F}$ together with two binary operations $+, \times$ on $\mathbb{F}$ such that:

- $(\mathbb{F}, +)$ is an abelian group (called its identity 0)
- $(\mathbb{F} \setminus \{0\}, \times)$ is also an abelian group and
- the following distributive law hold:

$$a \times (b + c) = (a \times b) + (a \times c), \qquad \text{for all } a, b, c \in \mathbb{F}.$$

Definition 2.2. [18] Let $\mathbb{F}$ be any field. If the number of elements in $\mathbb{F}$ is infinite, $\mathbb{F}$ is called an **infinite field**. If the number of elements in $\mathbb{F}$ is finite, $\mathbb{F}$ is called a **finite field**.

Definition 2.3. [17] The **characteristic of a field** $\mathbb{F}$ is defined to the smallest positive integer p such that

$$p \cdot 1_{\mathbb{F}} = \underbrace{1_{\mathbb{F}} + \cdots + 1_{\mathbb{F}}}_{p \text{ times}} = 0,$$

where $1_{\mathbb{F}}$ is the identity of $\mathbb{F}$, if such a p exists and is defined to be 0 otherwise. Then the characteristic of F, ch($\mathbb{F}$), is either 0 or a prime p. If ch($\mathbb{F}$) $= p$ then for any $\alpha \in \mathbb{F}$,

$$p \cdot \alpha = \underbrace{\alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

Example 2.1.
1. The field $\mathbb{Q}$, $\mathbb{R}$ and the integral domain $\mathbb{Z}$ have characteristic 0: ch($\mathbb{Q}$) $=$ ch($\mathbb{R}$) $=$ ch($\mathbb{Z}$) $= 0$.
2. The (finite) field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p for any prime p.
3. The integral domain $\mathbb{F}_p[x]$ of polynomials in the variable x with coefficients in the field $\mathbb{F}_p$ has characteristic p.

Note. GF$(2) = \mathbb{F}_2 = \{0, 1\}$ is the Galois field of order 2 and GF$(4) = \mathbb{F}_{2^2}$ is the Galois field of order 4 which

$$\text{GF}(4) = \left\{ a_1\alpha + a_0 \middle| a_1, a_0 \in \text{GF}(2) \text{ and } \alpha \text{ is a root of an irreducible polynomial over GF}(2) \right\}.$$

Theorem 2.1. [18] Let $\mathbb{F}$ be a field of characteristic $p, p \neq 0$, and $a_1, a_2, \ldots, a_m$ be any m elements of $\mathbb{F}$, then

$$(a_1 + a_2 + \cdots + a_m)^p = a_1^p + a_1^p + \cdots + a_m^p.$$

Theorem 2.2. [18] Let $\mathbb{F}_q$ be a finite field with q elements. Then $a^{q-1} = 1$ for all $a \in \mathbb{F}_q^*$.

Corollary 2.3. [18] Let $\mathbb{F}_q$ be a finite field with q elements and E be a field which contains $\mathbb{F}_q$ as a subfield. Then $a^q = a$ for all $a \in \mathbb{F}_q$ and, moreover, for any $\alpha \in E$, $\alpha^q = \alpha$ implies $\alpha \in \mathbb{F}_q$.

Theorem 2.4. [18] The multiplicative group of any finite field is **cyclic**.

Definition 2.4. [18] Let $\mathbb{F}_q$ be a finite field with q elements. The generators of the cyclic group $\mathbb{F}_q^*$ are called **primitive elements** or **primitive roots** $\mathbb{F}_q$. The number of primitive elements of $\mathbb{F}_q$ is $\varphi(q-1)$.
More generally, if α is an element of order n in $\mathbb{F}_q^*$, then $n|(q-1)$ and α is called a **primitive n-th root of unity**.

Example 2.2. Consider the field $\mathbb{F}_{16}$, which is obtained from $\mathbb{F}_2[x]$ modulo the irreducible polymial $x^4 + x + 1$. That is,

$$\begin{aligned}\mathbb{F}_{16} &= \mathbb{F}[x]/(x^4 + x + 1) \\ &= \{a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0 \mid a_3, a_2, a_1, a_0 \in \mathbb{F}_2\},\end{aligned}$$

where $\alpha = \bar{x}$ is the residule class of x modulo $x^4 + x + 1$. We have $\alpha^4 = \alpha + 1, \alpha^5 = \alpha^2 + \alpha, \alpha^6 = \alpha^3 + \alpha^2$, and the multiplication rule in $\mathbb{F}_{16}$

$$\begin{aligned}&(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)(b_3\alpha^3 + b_2\alpha^2 + b_1\alpha + b_0) \\ &= (a_3b_3 + a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3)\alpha^3 \\ &+ (a_3b_3 + a_3b_2 + a_2b_3 + a_2b_0a_1b_1 + a_0b_2)\alpha^2 \\ &+ (a_3b_2 + a_2b_3 + a_3b_1 + a_2b_2 + a_1b_3 + a_1b_0 + a_0b_1)\alpha \\ &+ (a_3b_1 + a_2b_2 + a_1b_3 + a_0b_0).\end{aligned}$$

We use the 4-tuple $(a_4a_3a_2a_1)$ to represent the element $a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0$ of $\mathbb{F}_{16}$. It is easy to show that α is a primitive element.

Theorem 2.5. [18] Let $\mathbb{F}$ be a finite field of characteristic p. Then the number of elements of $\mathbb{F}$ must be a power of p.

Theorem 2.6. [18] Let $\mathbb{F}$ be a finite field which contains a subfield $\mathbb{F}_q$ with q elements. Then the number of elements of $\mathbb{F}$ must be a power of q.

Theorem 2.7. Let p be any prime number and n be any positive integer. Then there exists a finite field which contains exactly p^n elements.

2.2 Divided differences

Let $x_1, x_2, \ldots, x_n$ be n distinct points and form the n independent Newton polynomials

$$1, x - x_1, (x - x_1)(x - x_2), \ldots, (x - x_0)(x - x_1) \cdots (x - x_{n-1}).$$

For given values $w_1, w_2, \ldots, w_n$ there is a unique polynomial $f(x)$ for which

$$f(x_i) = w_i, \qquad i = 1, 2, \ldots, n.$$

Let us see if we can represent it in the form (Newton's form of $f(x)$)

$$f(x) = a_0 + a_1(x - x_1) + a_2(x - x_1)(x - x_2) + \cdots + a_n(x - x_1)(x - x_2) \cdots (x - x_n).$$

To determine the constants a_i, set $x = x_1, x = x_2, x = x_3, \ldots$, successively, and solve the resulting linear equation:

$$\begin{aligned}
a_0 &= w_1 = f(x_1) = f[x_1] \\
a_1 &= \frac{w_2 - w_1}{x_2 - x_1} = \frac{f(x_2) - f(x_1)}{x_2 - x_1} = f[x_1, x_2] \\
a_2 &= \frac{1}{x_3 - x_2}\left(\frac{w_3 - w_1}{x_3 - x_1} - \frac{w_2 - w_1}{x_2 - x_1}\right) = \frac{f[x_2, x_3] - f[x_1, x_2]}{x_3 - x_1} = f[x_1, x_2, x_3]. \\
&\vdots
\end{aligned}$$

Definition 2.5. For a field $\mathbb{F}$, the **divided-differences** [1] on distinct points $x_1, x_2, x_3, \ldots$ in $\mathbb{F}$ of a function $f : \mathbb{F} \to \mathbb{F}$ are defined by

$$f[x_1] = f(x_1), \qquad f[x_1, x_2] = \frac{f[x_1] - f[x_2]}{x_1 - x_2},$$

and inductively for $k > 2$ by

$$f[x_1, \ldots, x_k] = \frac{f[x_1, \ldots, x_{k-1}] - f[x_2, \ldots, x_k]}{x_1 - x_k} = \sum_{i=1}^{k} \frac{f(x_i)}{p_k'(x_i)};$$

where $p_k(x) = (x - x_1)(x - x_2) \cdots (x - x_k)$ and $p_k'(x) = \sum_{i=1}^{k} \prod_{\substack{j=1 \\ j \neq i}}^{k} (x - x_j)$.

Example 2.3. Let

$$\mathbb{F} = \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1\}$$

be a field of characteristic two where α is the root of the irreducible polynomial $x^3 + x + 1$ over $\{0, 1\}$.

Let g be a function over the field $\mathbb{F}$. From the definition above, we get:

$$g[\alpha] = g(\alpha);$$

$$g[1, \alpha^2 + \alpha] = \frac{g(1)}{1 - (\alpha^2 + \alpha)} + \frac{g(\alpha^2 + \alpha)}{(\alpha^2 + \alpha) - 1};$$

$$g[\alpha, \alpha+1, \alpha^2] = \frac{g(\alpha)}{\alpha-\alpha^2} + \frac{g(\alpha+1)}{\alpha+1-\alpha^2} + \frac{g(\alpha^2)}{(\alpha^2-\alpha)(\alpha^2-\alpha-1)};$$

$$g[0, 1, \alpha, \alpha^2] = \frac{g(0)}{\alpha\cdot\alpha^2} + \frac{g(1)}{(1-\alpha)(1-\alpha^2)} + \frac{g(\alpha)}{\alpha(\alpha+1)(\alpha-\alpha^2)} + \frac{g(\alpha^2)}{\alpha^2(\alpha^2+1)(\alpha^2+\alpha)}$$

and so on. In here, if we let $g(x) = \alpha x^2 + 1 \in \mathbb{F}[x]$. The we can calculate the value of divided differences of g and so from above we get:

$$g[\alpha] = \alpha\cdot\alpha^2 + 1 = \alpha;$$

$$g[1, \alpha^2+\alpha] = \frac{\alpha+1}{1-(\alpha^2+\alpha)} + \frac{\alpha(\alpha^2+\alpha)^2+1}{(\alpha^2+\alpha)-1} = \alpha^2+1;$$

$$g[\alpha, \alpha+1, \alpha^2] = \frac{\alpha\cdot\alpha^2+1}{\alpha-\alpha^2} + \frac{\alpha(\alpha+1)^2+1}{\alpha+1-\alpha^2} + \frac{\alpha(\alpha^2)^2+1}{(\alpha^2-\alpha)(\alpha^2-\alpha-1)} = 1;$$

$$g[0, 1, \alpha, \alpha^2] = \frac{1}{\alpha\cdot\alpha^2} + \frac{\alpha+1}{(1-\alpha)(1-\alpha^2)} + \frac{\alpha(\alpha)^2+1}{\alpha(\alpha+1)(\alpha-\alpha^2)} + \frac{\alpha(\alpha^2)^2+1}{\alpha^2(\alpha^2+1)(\alpha^2+\alpha)} = \alpha^2+1$$

and so on.

2.3 Lagrange interpolation polynomials

Let $\overline{a} = (a_1, a_2, \ldots, a_n) \in \mathbb{R}^n$ and $I = (i_1, i_2, \ldots, i_n) \in \mathbb{R}^n$ where $i_1 < i_2 < \cdots < i_n$. By [22], the Lagrange interpolation polynomial $L_{a,I}(x)$,

$$\begin{aligned} L_{a,I}(x) &= \sum_{j=1}^{n} a_j \prod_{m=1, m\neq j}^{n} \frac{x-i_m}{i_j-i_m} \\ &= a_1 \frac{(x-i_2)(x-i_3)(x-i_4)\cdots(x-i_n)}{(i_1-i_2)(i_1-i_3)(i_1-i_4)\cdots(i_1-i_n)} + a_2 \frac{(x-i_1)(x-i_3)(x-i_4)\cdots(x-i_n)}{(i_2-i_1)(i_2-i_3)(i_2-i_4)\cdots(i_-i_n)} \\ &\quad + \cdots + a_n \frac{(x-i_1)(x-i_2)(x-i_3)\cdots(x-i_{n-1})}{(i_n-i_1)(i_n-i_2)(i_n-i_3)\cdots(i_n-i_{n-1})}, \end{aligned}$$

is the polynomial of degree $\leq n-1$ that passes through n points (i_j, a_j) for $1 \leq j \leq n$. That is, $L_{a,I}(i_j) = a_j$ for all $1 \leq j \leq n$.

2.4 Identity connecting divided differences with Lagrange interpolation polynomials

Proposition 2.8. [6] It is easy to verify that

$$f[x_1, \ldots, x_n] = \frac{f(x_1)}{\prod_{\substack{i=1\\ i\neq 1}}^{n}(x_1+x_i)} + \frac{f(x_2)}{\prod_{\substack{i=1\\ i\neq 2}}^{n}(x_2+x_i)} + \cdots + \frac{f(x_n)}{\prod_{\substack{i=1\\ i\neq n}}^{n}(x_n+x_i)}, \tag{2.1}$$

for distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$.

Lemma 2.9. [2, Lemma 1] Let $\mathbb{F}_{2^\ell}$ be a finite field of characteristic 2 with $2^\ell \geq n$ and let $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ defined by function $f(x) = x^k \quad (k = 0, 1, \ldots, 2^\ell - 1)$. Then

$$f[x_1, x_2, \ldots, x_n] = \sum_{i=1}^{n} \frac{f(x_i)}{\prod_{\substack{j=1\\ j\neq i}}^{n}(x_i+x_j)} = \sum_{i=1}^{n} \frac{x_i^k}{\prod_{\substack{j=1\\ j\neq i}}^{n}(x_i+x_j)} \tag{2.2}$$

for all distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$.

In particular

$$\sum_{i=1}^{n} \frac{x_i^k}{\prod_{\substack{j=1 \\ j\neq i}}^{n}(x_i+x_j)} = \begin{cases} 0 & \text{if } k \leq n-2 \\ 1 & \text{if } k = n-1 \\ x_1 + x_2 + \cdots + x_n & \text{if } k = n \\ \displaystyle\sum_{i_1+\cdots+i_n=k+1-n} x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} & \text{if } k > n. \end{cases}$$

Example 2.4. Let $\mathbb{F}$ be a field of characteristic 2 and let $f(x) = x^k \in \mathbb{F}[x]$. For 3 distinct elements $x_1, x_2, x_3 \in \mathbb{F}$, we get the order 3 divided-differences of f as follow:

1. For $k = 1$, then

$$\begin{aligned} f[x_1, x_2, x_3] &= \frac{x_1}{(x_1+x_2)(x_1+x_3)} + \frac{x_2}{(x_2+x_1)(x_2+x_3)} + \frac{x_3}{(x_3+x_1)(x_3+x_2)} \\ &= \frac{x_1(x_2+x_3) + x_2(x_1+x_3) + x_3(x_1+x_2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} = 0. \end{aligned}$$

2. For $k = 2$, then

$$\begin{aligned} f[x_1, x_2, x_3] &= \frac{x_1^2}{(x_1+x_2)(x_1+x_3)} + \frac{x_2^2}{(x_2+x_1)(x_2+x_3)} + \frac{x_3^2}{(x_3+x_1)(x_3+x_2)} \\ &= \frac{x_1^2(x_2+x_3) + x_2^2(x_1+x_3) + x_3^2(x_1+x_2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1^2x_2 + x_1x_2^2 + x_1x_2x_3 + x_2^2x_3) + (x_1^2x_3 + x_1x_2x_3 + x_1x_3^2 + x_2x_3^2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1^2 + x_1x_2 + x_1x_3 + x_2x_3)(x_2+x_3)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1+x_2)(x_1+x_3)(x_2+x_3)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} = 1. \end{aligned}$$

3. For $k = 3$, then

$$\begin{aligned} f[x_1, x_2, x_3] &= \frac{x_1^3}{(x_1+x_2)(x_1+x_3)} + \frac{x_2^3}{(x_2+x_1)(x_2+x_3)} + \frac{x_3^3}{(x_3+x_1)(x_3+x_2)} \\ &= \frac{x_1^3(x_2+x_3) + x_2^3(x_1+x_3) + x_3^3(x_1+x_2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1^3x_2 + x_1^3x_3 + x_2^2x_1^2 + x_2^2x_1x_3 + x_3^2x_1^2 + x_3^2x - 2x_1)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &\quad + \frac{(x_1^2x_2^2 + x_1^2x_2x_3 + x_2^3x_1 + x_2^3x_3 + x_3^2x_1x_2 + x_3^2x_2^2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &\quad + \frac{(x_1^2x_2x_3 + x_1^2x_3^2 + x_2^2x_1x_3 + x_2^2x_3^2 + x_3^3x_1 + x_3^3x_2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2)(x_1+x_2+x_3)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1+x_2)(x_1+x_3)(x_2+x_3)(x_1+x_2+x_3)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= x_1 + x_2 + x_3. \end{aligned}$$

4. For $k = 4$, then

$$\begin{aligned} f[x_1, x_2, x_3] &= \frac{x_1^4}{(x_1+x_2)(x_1+x_3)} + \frac{x_2^4}{(x_2+x_1)(x_2+x_3)} + \frac{x_3^4}{(x_3+x_1)(x_3+x_2)} \\ &= \frac{x_1^4(x_2+x_3) + x_2^4(x_1+x_3) + x_3^4(x_1+x_2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{x_1^4x_2 + x_1^4x_3 + x_2^4x_1 + x_2^4x_3 + x_3^4x_1 + x_3^4x_2}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= \frac{(x_1+x_2)(x_1+x_3)(x_2+x_3)(x_1^2+x_2^2+x_3^2+x_1x_2+x_1x_3+x_2x_3)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)} \\ &= x_1^2+x_2^2+x_3^2+x_1x_2+x_1x_3+x_2x_3. \end{aligned}$$

From this example, we see that it is easier if we use Lemma 2.9 above.

2.5 Some basic results in Number Theory

In this section, we will say about definitions and theorems of arithmetic.

Definition 2.6. ([19]) A positive integer $n > 1$ with unique **prime factorization**

$$n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$$

where $p_1, \dots, p_s$ are distinct primes and $a_1, \dots, a_s \in \mathbb{N}$, is **r-free** whenever $a_i < r$ for all $i = 1, 2, ..., s$.
In case $r = 2$, we call n, a **square-free**.

Example 2.5.
1. Let $r = 3$. Then we see that $102 = 3 \cdot 5 \cdot 7$ and $60 = 2^2 \cdot 3 \cdot 5$ are 3-free integers but $200 = 2^3 \cdot 5^2$ and $162 = 3^4 \cdot 2$ are not.
2. Let $r = 2$. Then we see that $102 = 3 \cdot 5 \cdot 7$ and $165 = 3 \cdot 5 \cdot 11$ are square-free integers but $100 = 2^2 \cdot 5^2$ and $162 = 3^4 \cdot 2$ are not.

Definition 2.7. ([19]) Given $a, b, m \in \mathbb{Z}$ with $m > 0$. We say that a is **congruent to** b **modulo** m, if $m|(a-b)$ and write

$$a \equiv b \pmod{m}.$$

Definition 2.8. ([19]) A congruence of the form

$$ax \equiv b \pmod{m}$$

where x is an unknown integer is called a **linear congruence** in one variable.

Theorem 2.10. ([19], Theorem 5.12, 5.13, 5.14 on p.111-112) Given $a, b, m \in \mathbb{Z}$ with $m > 0$.

1) If $\gcd(a, m) = 1$, then the linear congruence $ax \equiv b \pmod{m}$ has exactly one solution modulo m.

2) If $\gcd(a, m) = d$, then the linear congruence $ax \equiv b \pmod{m}$ has solutions if and only if $d|b$.

3) Assume that $\gcd(a, m) = d$ and suppose that $d|b$. Then the linear congruence $ax \equiv b \pmod{m}$ has exactly d solutions modulo m. These are given by

$$t,\ t + \frac{m}{d},\ t + 2m/d,\ \ldots,\ t + (d-1)\frac{m}{d},$$

where t is the solution, unique modulo m/d, of the linear congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right).$$

2.6 Arithmetic functions

Definition 2.9. [19, 23] A complex - valued function defined on the positive integers is called an **arithmetic function**. Denote by $\mathcal{A}$ the **set of all arithmetic functions**.

Examples of arithmetic functions are:

1. The **greatest integer function** [20], denoted $[x]$, is defined on the reals and is the largest integer less than or equal to x. In the other words, it is that integer n such that

$$n \leq x < n + 1.$$

2. The **Möbius function**, $\mu(n)$, defined by, [19],

$$\mu(n) := \begin{cases} (-1)^s & \text{if } n = p_1 p_2 \cdots p_s \text{ for distinct primes } p_1, \ldots, p_s \\ 1 & \text{if } n = 1 \\ 0 & \text{otherwise.} \end{cases}$$

3. For $\alpha \in \mathbb{R}$, the **divisor function**, $\sigma_\alpha(n)$, is defined to be the sum of the αth power of divisors of n, [19],

$$\sigma_\alpha(n) := \sum_{d|n} d^\alpha;$$

when $\alpha = 0$, σ_0 is the number of divisors of n denoted by $d(n)$;
when $\alpha = 1$, σ_1 is the sum of divisors of n denoted by $\sigma(n)$.

4. The **Euler phi function**, $\varphi(n)$, is defined to be the number of positive integers not exceeding n that are relatively prime to n, i.e.,

$$\varphi(n) := \sum_{\substack{x \leq n \\ \gcd(x,n)=1}} 1.$$

The Euler phi function satisfies, [23],

$$\varphi(n) = \sum_{d|n} \mu(d) \left(\frac{n}{d}\right),$$

where the sum is extended over divisors d of n.

Theorem 2.11 (**Properties of Greatest Integer Function** [20])**.** Let x and y be reals. Then we have

1. $[x] \leq x < [x]+1,\ x-1 < [x] \leq x,\ 0 \leq x-[x] < 1$;
2. if n is an integer, then $[x+n] = [x]+n$;
3. if $x \geq 0$, then
$$[x] = \sum_{1 \leq n \leq x} 1;$$
4. $[x]+[y] \leq [x+y] \leq [x]+[y]+1$;
5. $[x]+[-x] = \begin{cases} 0 & \text{if } x \text{ is an integer} \\ -1 & \text{otherwise.} \end{cases}$.
6. if m and n are integers, with m positive, then
$$[\frac{n+x}{m}] = [\frac{n+[x]}{m}];$$
and
7. if $x \geq 0$ and a is a positive integer, then $[x/a]$ is the number of positive integers $\leq x$ that are divisible by a.

Definition 2.10. ([19]) An arithmetic function f is called **multiplicative** if f is not identically zero, $f(1) = 1$, and
$$f(mn) = f(m)f(n) \qquad (\gcd(m,n) = 1, m, n \in, \mathbb{N}).$$
Denote $\mathcal{M}$ be the **set of multiplicative functions**. Clearly, if $f \in \mathcal{A}$ with $f(1) = 1$ then $f \in \mathcal{M}$ if and only if
$$f(p_1^{a_1} \dots p_s^{a_s}) = f(p_1^{a_1}) \cdots f(p_s^{a_s})$$
for all prime p_i's and positive integer a_i's. Note that $\mu(n)$, $\sigma_\alpha(n)$, $U(n)$, $\varphi(n)$ and $\lambda(n)$ are multiplicative on n (see also [19, 23]).

2.7 Continued fractions

Definition 2.11. [20] Let u_0/u_1 be a rational number with $u_1 > 0$ and $(u_0, u_1) = 1$. If we apply the Euclidean algorithm we get a sequence of the following sort continued fractions

$$\begin{aligned} u_0 &= u_1 a_0 + u_2 && 0 < u_2 < u_1 \\ u_1 &= u_2 a_1 + u_3 && 0 < u_3 < u_2 \\ &\vdots \\ u_{j-1} &= u_j a_{j-1} + u_{j+1} && 0 < u_{j+1} < u_j \end{aligned}$$

$$u_j = u_{j+1}a_j.$$

If we write $\xi_i = u_i/u_{i+1},\ 0 \le i \le j$, then all the equations above states that

$$\begin{cases} \xi_i = a_i + 1/\xi_{i+1},\ 0 \le i \le j-1 \\ \xi_j = a_j \end{cases}.$$

Thus

$$\xi_0 = a_0 + \frac{1}{a_1 + 1/\xi_2} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + 1/\xi_3}}$$

and so on. Thus

$$\frac{u_0}{u_1} = \xi_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j}}}}$$

and it is called the **continued fraction expansion** of the rational number u_0/u_1. The integers a_i are called the **partial quotients** and the numbers ξ_i are called **complete quotients** of u_0/u_1. We usually write the continued fraction exspansion of u_0/u_1 in the more condensed form $[a_0; a_1, \ldots, a_j]$

$$u_0/u_1 = [a_0; a_1, \ldots, a_j].$$

Note that a_0 can be positive, negative or zero, but all further partial quotients must be strictly positive. Note also that if $j > 1$, then $a_j = [u_j/u_{j+1}]$ and so $0 < u_{j+1} < u_j$ imply that $a_j > 1$.

One may generalize the notation of the form $[a_0; a_1, \ldots, a_j]$. If $x_0, x_1, \ldots, x_j$ are any real numbers,with $x_1, \ldots, x_j$ all positive, then we define

$$[x_0; x_1, \ldots, x_j] = x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \ddots + \cfrac{1}{x_{j-1} + \cfrac{1}{x_j}}}}.$$

If the x_i are all integers, then the continued fraction is said to be **simple**. The following obvious formulas will be useful in what follows:

$$\begin{aligned} [x_0; x_1, \ldots, x_j] &= x_0 + \frac{1}{[x_1; x_2, \ldots, x_j]} \\ &= [x_0; x_1, \ldots, x_{j-2} + 1/x_j]. \end{aligned}$$

Example 2.6. Find the finite simple continued fraction expansions of the rational number $6/7, 15/11$ and $-31/17$.

Solution. We have

$$6 = 7 \cdot 0 + 6$$
$$7 = 6 \cdot 1 + 1$$
$$6 = 1 \cdot 6,$$

so that $6/7 = [0; 1, 6]$. We have

$$15 = 11 \cdot 1 + 4$$
$$11 = 4 \cdot 2 + 3$$
$$4 = 3 \cdot 1 + 1$$
$$3 = 1 \cdot 3$$

so that $15/11 = [1; 2, 1, 3]$. We have

$$-31 = 17(-2) + 3$$
$$17 = 3 \cdot 5 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2$$

so that $-31/17 = [-2; 5, 1, 2]$. □

2.8 The big oh notation and asymptotic equality

Definition 2.12. [19] If $g(x) > 0$ for all $x \geq a$, we write

$$f(x) = O(g(x)) \text{ or } f(x) \ll g(x) \qquad \text{(read: "} f(x) \text{ is big oh of } g(x)\text{")}$$

to mean that the quotient $f(x)/g(x)$ is bounded for $x \geq a$; that is there exist a constant $M > 0$ such that

$$| f(x) | \leq Mg(x) \qquad \text{for all } x \geq a.$$

An equation of the form

$$f(x) = h(x) + O(g(x))$$

means that $f(x) - h(x) = O(g(x))$. We note that $f(t) = O(g(t))$ for $t \geq a$ implies $\int_a^x f(t)dt = O(\int_a^x g(t)dt)$ for $x \geq a$.

Example 2.7.

1. Let $f(x) = x^2 + 2x - 1$. Then we can write $f(x) = x^2 + O(x)$. The symbol $O(x)$ represents an unspecified function of x which grows no faster than some constant time x^2.
2. Let $E(x) = (2C - 1)x + O(\sqrt{x})$ where $C = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$. Then we can write $E(x) = O(x)$.

Definition 2.13. [19] If

$$\lim_{x\to\infty}\frac{f(x)}{g(x)}=1$$

we say that $f(x)$ is asymptotic to $g(x)$ as $x\to\infty$, and we write

$$f(x)\sim g(x) \text{ as } x\to\infty.$$

Example 2.8. 1. $\sum_{n\le x} d(n)\sim x\log x$ as $x\to\infty$.

Since $\sum_{n\le x} d(n)=x\log x+(2C-1)x+O(\sqrt{x})$, we get

$$\lim_{x\to\infty}\left(\frac{\sum_{n\le x} d(n)}{x\log x}\right)=1+\lim_{x\to\infty}\left(\frac{(2C-1)x+O(\sqrt{x})}{x\log x}\right)=1.$$

2. From Example 2.7 (2.), we see that $E(x)\sim(2C-1)x$.

Since $E(x)=(2C-1)x+O(\sqrt{x})$, we get

$$\lim_{x\to\infty}\left(\frac{E(x)}{(2C-1)x}\right)=1+\lim_{x\to\infty}\left(\frac{O(\sqrt{x})}{(2C-1)x}\right)=1.$$

Definition 2.14. [19] The **Riemann zeta function** $\zeta(s)$ defined by

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s} \qquad \text{if } s>1,$$

and by

$$\zeta(s)=\lim_{x\to\infty}\left(\sum_{n\le x}\frac{1}{n^s}-\frac{x^{1-s}}{1-s}\right) \qquad \text{if } 0<s<1.$$

Theorem 2.12. [19] If $x\ge 1$ we have:

1. $\sum_{n\le x}\frac{1}{n}=\log x+C+O\left(\frac{1}{x}\right)$.
2. $\sum_{n\le x}\frac{1}{n^s}=\frac{x^{1-s}}{1-s}+\zeta(s)+O(x^{-s})$ if $s>0, s\neq 1$.
3. $\sum_{n>x}\frac{1}{n^s}=O(x^{1-s})$ if $s>1$.
4. $\sum_{n\le x} n^{\alpha}=\frac{x^{\alpha+1}}{\alpha+1}+O(x^{\alpha})$ if $\alpha\ge 0$.

2.9 Averages of arithmetic functions

Theorem 2.13. [19] For all $x\ge 1$ we have

$$\sum_{n\le x} d(n)=x\log x+(2C-1)x+O(\sqrt{x}),$$

where C is Euler's constant.

Theorem 2.14. [19] For all $x \geq 1$ we have

$$\Big|\sum_{n\leq x}\frac{\mu(n)}{n}\Big| \leq 1,$$

with equality holding only if $x < 2$.

Theorem 2.15. [19] Let f be a multiplicative arithmetical function such that the series $\sum f(n)$ is absolutely convergent. Then the sum of the series can be expressed as an absolutely convergent infinite product,

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\{1 + f(p) + f(p^2) + \cdots\}$$

extended over all primes. If f is completely multiplicative, the product simplifies and we have

$$\sum_{n=1}^{\infty} f(n) = \prod_{p}\frac{1}{1-f(p)}.$$

Note. In each case the product is called the **Euler product of the series**.

Theorem 2.16. [19] Assume $\sum f(n)n^{-s}$ converges absolutely for $\sigma > \sigma_a$. If f is multiplicative we have

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_{p}\{1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\} \qquad \text{if } \sigma > \sigma_a,$$

and if f is completely multiplicative we have

$$\sum_{n=1}^{\infty}\frac{f(n)}{n^s} = \prod_{p}\frac{1}{1-f(p)p^{-s}}, \qquad \text{if } \sigma > \sigma_a.$$

Lemma 2.17. [13] For $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0;\alpha)$ and positive integer $d \geq 2, 0 \leq a < d$, we have

$$\sum_{\substack{n\leq x\\ \lfloor \alpha n+\beta\rfloor \equiv a(\bmod d)}} 1 = \frac{x}{d} + O(d\log^3 x) \qquad \text{as } x \to \infty.$$

For growing difference d the result is non-trivial provided $d \ll \sqrt{x}\log^{-3/2-\varepsilon} x$, for $\varepsilon > 0$.

Example 2.9. Let $\alpha = \sqrt{2} \sim 1.4142$ and $\beta = 0.4142 \in [0, 1.4142)$. Then we have

$$\lfloor \alpha n+\beta\rfloor_{n\leq 21} := \{1,3,4,6,7,8,10,11,13,14,15,17,18,20,21,23,24,25,27,28,30\};$$

$$\lfloor \alpha n+\beta\rfloor_{n\leq 21} \equiv 1(\mod 3) := \{1,4,7,10,13,25,28\}.$$

So, we see that

$$\sum_{\substack{n\leq 21\\ \lfloor \alpha n+\beta\rfloor \equiv 1(\bmod 3)}} 1 = 7 \sim \frac{21}{3} + O(3\log^3 21).$$

2.10 Beatty sequences

Theorem 2.18 (Beatty Theorem)**.** [24] Let X be any positive irrational number and Y its reciprocal i.e., $Y = \frac{X}{X-1}$ or $\frac{1}{X} + \frac{1}{Y} = 1$. Then the two sequences

$$1 + X, 2(1 + X), 3(1 + X), \dots,$$
$$1 + Y, 2(1 + Y), 3(1 + Y), \dots$$

together contain exactly one number from each of the intervals $(n, n + 1)$ between consecutive positive integers $(n = 1, 2, 3, \dots)$.

Corollary 2.19. [24] The sequences $\lfloor n(1 + X) \rfloor, \lfloor n(1 + Y) \rfloor$, called ***Beatty Sequences*** corresponding to the irrational number X, together contain each natural number exactly once.

Example 2.10. Let $X = \sqrt{2} \approx 1.4142$ is irrational number. Then we get $Y = X/(X-1) = 3.4143$ and for $n = 1, 2, 3, \dots$, we get the sequences

$$n(1 + X) := \{2.4142, 4.8284, 7.2426, 9.6568, \dots\};$$
$$n(1 + Y) := \{4.4143, 8.8286, 13.2429, 17.6572, \dots\}.$$

Then we get the Beatty sequences

$$\lfloor n(1 + X) \rfloor_{n \geq 1} := \{2, 4, 7, 9, \dots\};$$
$$\lfloor n(1 + Y) \rfloor_{n \geq 1} := \{4, 8, 13, 17, \dots\}.$$

2.11 Chinese remainder theorem

Theorem 2.20 (**Chines remainder theorem, [19]**)**.** Assume $m_1, \dots, m_r$ are positive integers, relatively prime in pairs:

$$(m_i, m_k) = 1 \qquad \text{if } i \neq k.$$

Let $b_1, \dots, b_r$ be arbitrary integers. Then the system of congruences

$$x \equiv b_1 (\mod m_1)$$
$$\vdots$$
$$x \equiv b_r (\mod m_r)$$

has exactly one solution modulo the product $m_1 \cdots m_r$.

Theorem 2.21. [19] Assume $m_1, \dots, m_r$ are relatively prime in pairs. Let $b_1, \dots, b_r$ be arbitrary integer and let $a_1, \dots, a_r$ satisfy

$$(a_k, m_k) = 1 \qquad \text{if } k = 1, 2, \dots, r.$$

Then the linear system of system of congruences

$$a_1 x \equiv b_1 (\mod m_1)$$
$$\vdots$$
$$a_r x \equiv b_r (\mod m_r)$$

has exactly one solution modulo the product $m_1 \cdots m_r$.

Theorem 2.22. [19] Let f be a polynomial with integer coefficients, let $m_1, m_2, \ldots, m_r$ be positive integers relative prime in pairs, and let $m = m_1 m_2 \cdots m_r$. Then the congruence

$$f(x) \equiv 0 (\mod m)$$

has a solution if and only if each of congruences

$$f(x) \equiv 0 (\mod m_i) \qquad (i = 1, 2, \ldots, r)$$

has a solution. Moreover, if $v(m)$ and $v(m_i)$ denote the number of solutions of two equations above respectively, then

$$v(m) = v(m_1) v(m_2) \cdots v(m_r).$$

2.12 Literature reviews

In this section, we will review some preliminaries and results in [6], [14] and [15] that are strong basic for our work.

2.12.1 The work of Davies and Rousseau

In this work of Davies and Rousseau [6], they considered any field not of characteristic 2 and used some auxiliary results to prove the divided differences characterization of polynomials problem.

Lemma 2.23 (Interpolation Theorem). [25, Sect. 5.6, pp. 86-89] If $x_1, \ldots, x_{m+1}$ are distinct elements in a field (of any characteristic), then for any $c_1, \ldots, c_{m+1}$ in this field, there exists a unique polynomial f over the same field of degree at most m such that $f(x_j) = c_j$ for $j = 1, \ldots, m+1$.

Corollary 2.24. Let $\mathbb{F}$ be a finite field with order n. Then every function $f : \mathbb{F} \to \mathbb{F}$ is equal to a polynomial of degree at most $n - 1$.

Theorem 2.25 (Davies-Rousseau's main work). [6] Let n be an integer, $n \geq 2$, and let K be a field not of characteristic 2. Suppose that functions $f : K \to K$ and $h : K \to K$ satisfy (1.2) where $x_1, \ldots, x_n$ are distinct of K. Then f is equal to a polynomial of degree at most n over K:

$$f(x) \equiv a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0.$$

In their appendix, they shown that for the case ch$(K) \neq 2$ and $n = 2$, the result holds if $|K| \leq 4$, but it does not hold if $|K| > 4$ (where $|K|$ denote the cardinality of the field $K$and ch(K) denote the characteristic of a field K).

Example 2.11. Let $\mathbb{F}_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. Let $f, h := \mathbb{F}_7 \to \mathbb{F}_7$ such that

$$f[x_1, x_2, x_3] = h(x_1 + x_2 + x_3)$$

for any 3 distinct $x_1, x_2, x_3 \in \mathbb{F}_7$.
Now we will show that f is a polynomial of degree at most 3.
Choose 4 distinct elements of the form

$$S := \{\bar{0}, \bar{1}, \bar{6}, \bar{2}\}$$

from $\mathbb{F}_7$. Then there exist a unique polynomial $f_1(x)$ of degree at most 3 over $\mathbb{F}_7$ such that

$$f_1(u) = f(u) \qquad \forall u \in S.$$

Let $h_1(x) \in \mathbb{F}_7[x]$ such that $f_1[x_1, x_2, x_3] = h_1(x_1 + x_2 + x_3)$ for any 3 distinct elements $x_1, x_2, x_3 \in \mathbb{F}_7$. Set $F(x) = f(x) - f_1(x)$ and $H(x) = h(x) - h_1(x)$ such that

$$F(u) = 0 \qquad \forall u \in S$$

and

$$F[x_1, x_2, x_3] = H(x_1 + x_2 + x_3)$$

for any 3 distinct elements $x_1, x_2, x_3 \in \mathbb{F}_7$.

Substituting x_1, x_2, x_3 by

$$\bar{1}, \bar{6}, \bar{2}, \qquad \bar{0}, \bar{6}, \bar{2},$$
$$\bar{1}, \bar{0}, \bar{2}, \qquad \bar{1}, \bar{6}, \bar{0},$$

and applying the 3-rd order divided-differences of $F(x)$, we get

$$F[\bar{1}, \bar{6}, \bar{2}] = H(\bar{2}) = \bar{0}, \qquad F[\bar{0}, \bar{6}, \bar{2}] = H(\bar{1}) = \bar{0},$$
$$F[\bar{1}, \bar{0}, \bar{2}] = H(\bar{3}) = \bar{0}, \qquad F[\bar{1}, \bar{6}, \bar{0}] = H(\bar{0}) = \bar{0}.$$

Next, we will show that $F(x) = 0$ for all $x \in \mathbb{F}_7$.
Substituting x_1, x_2, x_3 by $\bar{0}, \bar{2}, \bar{5}$ and applying 3-rd order divided-differences of $F(x)$, we get

$$F[\bar{0}, \bar{2}, \bar{5}] = \frac{F(\bar{5})}{\bar{5} \cdot (\bar{5} - \bar{2})} = H(\bar{0}) = \bar{0}.$$

So, $F(\bar{5}) = 0$ and consequency $H(\bar{5}) = \bar{0}$.
Substituting x_1, x_2, x_3 by $\bar{0}, \bar{3}, \bar{4}$ and applying the 3-rd order divided-differences of $F(x)$, we get

$$F[\bar{0}, \bar{3}, \bar{4}] = \frac{F(\bar{3})}{\bar{3} \cdot (\bar{3} - \bar{4})} + \frac{F(\bar{4})}{\bar{4} \cdot (\bar{4} - \bar{3})} = H(\bar{0}) = \bar{0}.$$

So, we have

$$F(\bar{3}) + F(\bar{4}) = \bar{0}. \tag{2.3}$$

Substituting x_1, x_2, x_3 by $\bar{1}, \bar{3}, \bar{4}$ and applying the 3-rd order divided-differences of $F(x)$, we get

$$F[\bar{1}, \bar{3}, \bar{4}] = \frac{F(\bar{3})}{(\bar{3}-\bar{1})(\bar{3}-\bar{4})} + \frac{F(\bar{4})}{(\bar{4}-\bar{1})(\bar{4}-\bar{3})} = H(\bar{1}) = \bar{0}.$$

So, we have

$$\bar{3}F(\bar{3}) + \bar{5}F(\bar{4}) = \bar{0}. \tag{2.4}$$

Solving system equations (2.3) and (2.4), we get

$$F(\bar{3}) = F(\bar{4}) = \bar{0}.$$

Therefore, $F(x) = 0$ for all $x \in \mathbb{F}_7$ and so $f(x)$ is a polynomial of degree at most 3 over $\mathbb{F}_7$.

2.12.2 The work of Dimitrov

In paper [15], let N be a sufficient large positive integer. Let ε denote an arbitrary small positive number, not necessarily the same in different occurrences. Then, they denote by $\mu(n)$ the Möbius function and by $\tau(n)$ the number of positive divisors of n. Let $\|t\|$ be the distance from t to the nearest integer and let

$$\psi(t) = \{t\} - \frac{1}{2}$$

where $\{t\}$ is the fraction part of t. Let $\alpha > 1$ be irrational number with bounded partial quotient or irrational algebraic number. Denote

$$\sigma = \prod_p \left(1 - \frac{2}{p^2}\right).$$

They defined the characteristic function $\omega_\alpha(x)$ in the interval $(0, 1]$ as follows

$$\omega_\alpha(x) = \begin{cases} 1, & \text{if } i - \frac{1}{\alpha} < x < 1; \\ \frac{1}{2}, & \text{if } x = 1 - \frac{1}{\alpha} \text{ or } x = 1; \\ 0, & \text{otherwise.} \end{cases}$$

Then, they got some results as following.

Lemma 2.26. The formula

$$\omega_\alpha(x) = \frac{1}{\alpha} + \psi(x) - \psi\left(x + \frac{1}{\alpha}\right)$$

holds.

Lemma 2.27. For every $J \geq 2$, then

$$\psi(t) = \sum_{1 \leq |k| \leq J} a(k)e(kt) + O\left(\sum_{|k| \leq J} b(k)e(kt)\right), \qquad a(k) \ll 1/|k|, b(k) \ll 1/J.$$

Note: $a(k) \ll 1/J$ means that $a(k)$ is an big oh of $1/J$.

Lemma 2.28. If $X \geq 1$, then

$$|\sum_{n\leq X} e(\alpha n)| \leq \min\left(X, \frac{1}{2\parallel \alpha \parallel}\right).$$

Lemma 2.29. Suppose that $X, Y \geq 1, \lambda = \frac{a}{q} + \frac{\theta}{q^2}, q \geq 1, (a,q) = 1, |\theta| \leq 1$. Then

$$\sum_{n\leq X} \min\left(Y, \frac{1}{\parallel \lambda n \parallel}\right) \ll \frac{XY}{q} + (X+q)\log 2q.$$

Theorem 2.30 (Main Theorem)**.** Let $\alpha > 1$ be irrational number with bounded partial quotient or irrational algebraic number. Then

$$S(N,\alpha) = \sum_{n\leq N} \mu^2(\lfloor \alpha n \rfloor)\mu^2(\lfloor \alpha n \rfloor + 1) = \sigma N + O(N^{\frac{5}{6}+\varepsilon}).$$

Example 2.12. Let $N = 20, \alpha = \sqrt{2} \sim 1.4142, \epsilon = 0.0001$. Then for integers $n \leq N$ we have

$$\lfloor \alpha n \rfloor := \{1,2,4,5,7,8,9,11,12,14,15,16,18,19,21,22,24,25,26,28\},$$
$$\lfloor \alpha n \rfloor + 1 := \{2,3,5,6,8,9,10,12,13,15,16,17,19,20,22,23,25,26,27,29\}.$$

From here, we see that

$$\begin{aligned}
S(N,\alpha) &= \sum_{n\leq N} \mu^2(\lfloor \alpha n \rfloor)\mu^2(\lfloor \alpha n \rfloor + 1) \\
&= 1+1+0+1+0+0+0+0 = 0+1+0+0+0+0+1+1+0+0+0+0 \\
&= 6 \\
&\sim \sigma N + O(N^{\frac{5}{6}+\epsilon}) = \prod_p \left(1-\frac{2}{p^2}\right)\cdot 20 + O(20^{\frac{5}{6}+0.0001}) \\
&= 20(1-\frac{2}{2^2})(1-\frac{2}{3^2})(1-\frac{2}{5^2})(1-\frac{2}{7^2})(1-\frac{2}{11^2})(1-\frac{2}{13^2})(1-\frac{2}{17^2})(1-\frac{2}{19^2}) + O(20^{\frac{5}{6}+0.0001}) \\
&\sim 6.58731.
\end{aligned}$$

Lemma 2.31 (Main Lemma)**.** Let $\alpha > 1$ be irrational number with bounded partial quotient or irrational algebraic number. Then for the sum

$$\Sigma = \sum_{1\leq k\leq J} \frac{1}{k}\Big|\sum_{m\leq \alpha N} \mu^2(m)\mu^2(m+1)e(\lambda k m)\Big|.$$

where $\lambda = \frac{1}{\alpha}$, the estimation

$$\Sigma \ll N^{\frac{5}{6}+\varepsilon}$$

holds.

2.12.3 The work of Tangsupphathawat, Srichan, and Laohakosol

In the work of Tangsupphathawat et al [14], they used the similar method due to Rieger to prove that the Piateske-Shapiro sequence defined by

$$\mathbb{N}^c = \{\lfloor n^c \rfloor : n \in \mathbb{N}, c \in \mathbb{R}, c > 1\}$$

contains infinitely many consecutive square-free integers whenever $1 < c < 3/2$. To do this, they let ε be arbitrary small positive number, not necessarily the same in different occurrences and then they got some lemmas as following:

Lemma 2.32. For $1 < c < 2$, let x be a positive real number and let q and a be two integers such that $0 \leq a < q \leq x^c$. Then

$$\sum_{\substack{n \leq x \\ \lfloor n^c \rfloor \equiv a \pmod q}} 1 = \frac{x}{q} + \begin{cases} O\left(\frac{x^{(c+4)/7}}{q^{1/7}}\right) & \text{for } q < x^{c-5/4}, \\ O\left(\frac{x^{(c+1)/3}}{q^{1/3}}\right) & \text{for } x^{c-5/4} \leq q < x^{c-1/2}, \\ O\left(\frac{x^c}{q}\right) & \text{for } x^{c-1/2} \leq q < x^c. \end{cases}$$

Lemma 2.33. ([26, Exercise 9, p. 50]) For each $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ such that for all $n \geq 1$ we have

$$d(n) \leq C_\varepsilon n^\varepsilon.$$

Lemma 2.34. For a fixed real $y > 1$,

$$\sum_{\substack{d,t \\ \gcd(d,t)=1 \\ dt \leq y}} \frac{\mu(d)\mu(t)}{d^2 t^2} = \prod_{p \text{ prime}} \left(1 - \frac{2}{p^2}\right) + O\left(y^{-1+\varepsilon}\right).$$

Lemma 2.35. Let $1 < c < 2$ and let x be a positive real number.

(I) If $A_c^2(x)$ denotes the number of quadruples d, t, u, v of positive integers satisfying the conditions

$$t^2 v - d^2 u = 1, \qquad d^2 u \leq x^c, \qquad x^{c/2} < dt \leq x^{2c/3},$$

then

$$A_c^2(x) \ll x^{2c/3+\varepsilon}.$$

(II) If $A_c^3(x)$ denotes the number of quadruples d, t, u, v of positive integers satisfying the conditions

$$t^2 v - d^2 u = 1, \qquad d^2 u \leq x^c, \qquad dt > x^{2c/3},$$

then

$$A_c^3(x) \ll x^{2c/3+\varepsilon}.$$

Theorem 2.36 (Main Theorem)**.** For $1 < c < 3/2$ and sufficiently small $\varepsilon > 0$,

$$\sum_{\substack{n \leq x \\ \lfloor n^c \rfloor, \lfloor n^c \rfloor + 1 \text{ are square-free}}} 1 = \prod_p \left(1 - \frac{2}{p^2}\right) x + O\left(x^{(2c+1)/4+\varepsilon}\right) \quad \text{as } x \to \infty.$$

Example 2.13. Let $n \in \mathbb{N}, c = 1.4142, \epsilon = 0.0001$ and $x = 20$. Then we have

$$\lfloor n^c \rfloor = \{1, 2, 4, 7, 9, 12, 15, 18, 22, 25, 29, 33, 37, 41, 46, 50, 54, 59, 64, 69\};$$

$$\lfloor n^c \rfloor + 1 = \{2, 3, 5, 8, 10, 13, 16, 19, 21, 26, 30, 34, 38, 42, 47, 51, 55, 60, 65, 70\}.$$

So we get

$$\sum_{\substack{n \le x \\ \lfloor n^c \rfloor, \lfloor n^c \rfloor + 1 \text{ are square-free}}} 1 = 1+1+0+0+0+0+0+0+1+0+1+1+1+1+1+0+0+0+0+1$$

$$= 9$$

$$\sim 20(1-\frac{2}{2^2})(1-\frac{2}{3^2})(1-\frac{2}{5^2})(1-\frac{2}{7^2})(1-\frac{2}{11^2})(1-\frac{2}{13^2})(1-\frac{2}{17^2})(1-\frac{2}{19^2}) + O(20^{(2\cdot 1.4142+1)/4+0.0001})$$

$$= 6.58 + O(20^{(2\cdot 1.4142+1)/4+0.0001}) \sim 6.58 + 2.67.$$

Chapter 3

A divided-differences characterization of polynomials over a finite field of characteristic two

In this chapter, we will characterize the divided-defferences of polynomials over a finite field of characteristic two with $n \geq 3$.

3.1 Important properties

Throughout the rest of the paper, let $n \in \mathbb{N}$ with $n \geq 3$, and let $\mathbb{F}_{2^\ell}$ be a finite field of characteristic 2 with cardinality $|\mathbb{F}_{2^\ell}| = 2^\ell \geq n,\ \ell \in \mathbb{N},\ \ell \geq 2$. For definiteness, we represent the elements of $\mathbb{F}_{2^\ell}$ by

$$a_0 + a_1\alpha + \cdots + a_{\ell-1}\alpha^{\ell-1}, \qquad a_i \in \{0,1\} \qquad (0 \leq i \leq \ell - 1), \tag{3.1}$$

where α is a root of an irreducible polynomial of degree ℓ over $GF(2) = \{0,1\}$. The divided difference on n distinct points of a function $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ may be defined inductively as follows:

$$f[x_1] = f(x_1), \qquad f[x_1, x_2] = \frac{f(x_1) + f(x_2)}{x_1 + x_2},$$

and for $n > 2$

$$f[x_1, \ldots, x_n] = \frac{f[x_1, \ldots, x_{n-1}] + f[x_2, \ldots, x_n]}{x_1 + x_n},$$

for n distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$. To reach our main result, we could study some Lemma of the polynomials in a finite field and Properties of divided differences as follow.

Lemma 3.1. If $x_1, \ldots, x_{n+1}$ are distinct elements of a field $\mathbb{F}_{2^\ell}$ then for any $c_1, \ldots, c_{n+1}$ in $\mathbb{F}_{2^\ell}$ there exists a unique polynomial f over $\mathbb{F}_{2^\ell}$, of degree at most n, such that $f(x_j) = c_j$ for $j = 1, \ldots, n+1$.

Proof. Let $x_1, x_2, \ldots, x_{n+1}$ in $\mathbb{F}_{2^\ell}$ be distinct elements. Then for any $c_1, c_2, \ldots, c_{n+1} \in \mathbb{F}_{2^\ell}$ there exists the Lagrange's interpolation,

$$L(x) = \sum_{j=1}^{n+1} c_j \prod_{\substack{m=1 \\ m \neq j}}^{n+1} \frac{x + x_m}{x_j + x_m}$$

with degree at most n with coefficients in $\mathbb{F}_{2^\ell}$, pass through $n+1$ points such that

$$L(x_j) = c_j \qquad (1 \leq j \leq n+1).$$

Suppose that there exists another $r(x)$ of degree at most n over $\mathbb{F}_{2^\ell}$ such that

$$r(x_j) = c_j$$

for all $1 \leq j \leq n+1$.

Let $g(x) = L(x) + r(x)$. Since $L(x) = r(x)$ for $1 \leq j \leq n+1$, then

$$g(x_j) = L(x_j) + r(x_j) = 0.$$

Hence,

$$\prod_{j=0}^{n+1}(x + x_j) \mid g(x).$$

Since $g(x)$ is a polynomial of degree at most n, $g(x) = 0$.

Thus,

$$L(x) = r(x).$$

Therefore, $L(x)$ is the unique polynomial of degree less than $n+1$ over $\mathbb{F}_{2^\ell}$ such that

$$L(x_j) = c_j \text{ for all } 1 \leq j \leq n+1.$$

□

Corollary 3.2. Every function $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ is equal to a polynomial of degree at most $2^\ell - 1$.

Proof. Let $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ be a function such that $x_i \mapsto c_i$ for distinct $x_i \in \mathbb{F}_{2^\ell}$ $(i = 1, 2, 3, \ldots, 2^\ell)$ and $c_i \in \mathbb{F}_{2^\ell}$ $(i = 1, 2, 3, \ldots, 2^\ell)$ not necessary distinct. By Lemma 3.1, there exists $p(x)$ over $\mathbb{F}_{2^\ell}$ of degree at most $2^\ell - 1$ such that

$$p(x_i) = c_i \text{ for all } x_i \in \mathbb{F}_{2^\ell}.$$

Therefore,

$$p \equiv f.$$

□

Proposition 3.3. It is known that if f is a polynomial of degree $n \geq 1$ with coefficients in $\mathbb{F}_{2^\ell}$,

$$f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

then

$$f[x_1, \ldots, x_n] = a_n(x_1 + \cdots + x_n) + a_{n-1},$$

for distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$.

Proof. Let f be a polynomial of degree $n \geq 1$,

$$f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

where $a_i \in \mathbb{F}_{2^\ell}$ for all $i = 0, 1, \ldots, n$. Then for n distinct elements, $x_1, \ldots, x_n$ of $\mathbb{F}_{2^\ell}$, we have

$$f[x_1, \ldots, x_n] = \frac{a_n x_1^n + a_{n-1}x_1^{n-1} + \cdots + a_1 x_1 + a_0}{\prod_{\substack{i=1 \\ i \neq 1}}^{n}(x_1 + x_i)} + \frac{a_n x_2^n + a_{n-1}x_2^{n-1} + \cdots + a_1 x_2 + a_0}{\prod_{\substack{i=1 \\ i \neq 2}}^{n}(x_2 + x_i)} + \cdots$$

$$
\begin{aligned}
&+\frac{a_nx_{n-1}^n+a_{n-1}x_{n-1}^{n-1}+\cdots+a_1x_{n-1}+a_0}{\prod_{\substack{i=1\\i\neq n-1}}^{n}(x_{n-1}+x_i)}+\frac{a_nx_n^n+a_{n-1}x_n^{n-1}+\cdots+a_1x_n+a_0}{\prod_{\substack{i=1\\i\neq n}}^{n}(x_n+x_i)}\\
=&a_n\left(\frac{x_1^n}{\prod_{\substack{i=1\\i\neq 1}}^{n}(x_1+x_i)}+\frac{x_2^n}{\prod_{\substack{i=1\\i\neq 2}}^{n}(x_2+x_i)}+\cdots+\frac{x_n^n}{\prod_{\substack{i=1\\i\neq n}}^{n}(x_n+x_i)}\right)\\
&+a_{n-1}\left(\frac{x_1^{n-1}}{\prod_{\substack{i=1\\i\neq 1}}^{n}(x_1+x_i)}+\frac{x_2^{n-1}}{\prod_{\substack{i=1\\i\neq 2}}^{n}(x_2+x_i)}+\cdots+\frac{x_n^{n-1}}{\prod_{\substack{i=1\\i\neq n}}^{n}(x_n+x_i)}\right)+\cdots\\
&+a_1\left(\frac{x_1}{\prod_{\substack{i=1\\i\neq 1}}^{n}(x_1+x_i)}+\frac{x_2}{\prod_{\substack{i=1\\i\neq 2}}^{n}(x_2+x_i)}+\cdots+\frac{x_n}{\prod_{\substack{i=1\\i\neq n}}^{n}(x_n+x_i)}\right)\\
&+a_0\left(\frac{1}{\prod_{\substack{i=1\\i\neq 1}}^{n}(x_1+x_i)}+\frac{1}{\prod_{\substack{i=1\\i\neq 2}}^{n}(x_2+x_i)}+\cdots+\frac{1}{\prod_{\substack{i=1\\i\neq n}}^{n}(x_n+x_i)}\right).
\end{aligned}
$$

By Lemma 2.9, we get the form of coefficient of a_k for $k=0,1,\ldots,n$:

$$
\frac{x_1^k}{\prod_{\substack{i=1\\i\neq 1}}^{n}(x_1+x_i)}+\frac{x_2^k}{\prod_{\substack{i=1\\i\neq 2}}^{n}(x_2+x_i)}+\cdots+\frac{x_n^k}{\prod_{\substack{i=1\\i\neq n}}^{n}(x_n+x_i)}=\begin{cases}0 & \text{if } 0\leq k\leq n-2\\ 1 & \text{if } k=n-1\\ x_1+\cdots+x_n & \text{if } k=n.\end{cases}
$$

Thus, $f[x_1,\ldots,x_n]=a_n(x_1+\cdots+x_n)+a_{n-1}$ as required.

□

Lemma 3.4. If $g(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\in\mathbb{F}_{2^\ell}[x]$ is a polynomial of degree n with $1\leq n\leq 2^\ell-1$, then for any n distinct elements $x_1,\ldots,x_n$ in $\mathbb{F}_{2^\ell}$, the linear polynomial $h_g(x):=a_nx+a_{n-1}$ satisfies

$$
g[x_1,\ldots,x_n]=h_g(x_1+\cdots+x_n).
$$

(The polynomial h_g is henceforth referred as the n-th order divided-differences of g.)

Proof. The proof follows immediately form Proposition 3.3. □

Example 3.1. Let $\mathbb{F}_{2^4}:=\{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3\mid a_i\in\{0,1\}\}$ where α is the root of the irreducible polynomial x^4+x+1. Let $g(x)=x^3+1\in\mathbb{F}_{2^4}[x]$. By Lemma 3.4, there exists a polynomial $h_g(x)=x\in\mathbb{F}_{2^4}[x]$ such that for 3 distinct elements $x_1,x_2,x_3\in\mathbb{F}_{2^4}$,

$$
\begin{aligned}
g[x_1,x_2,x_3]&=\frac{g(x_1)}{(x_1+x_2)(x_1+x_3)}+\frac{g(x_2)}{(x_2+x_1)(x_2+x_3)}+\frac{g(x_3)}{(x_3+x_1)(x_3+x_2)}\\
&=\frac{(x_1^3+1)(x_2+x_3)+(x_2^3+1)(x_1+x_3)+(x_3^3+1)(x_1+x_2)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)}\\
&=\frac{x_1^3x_2+x_1x_2^3+x_1^3x_3+x_2^3x_3+x_1x_3^3+x_2x_3^3}{(x_1+x_2)(x_1+x_3)(x_2+x_3)}\\
&=\frac{(x_1+x_2+x_3)(x_1+x_2)(x_1+x_3)(x_2+x_3)}{(x_1+x_2)(x_1+x_3)(x_2+x_3)}\\
&=x_1+x_2+x_3\\
&=h_g(x_1+x_2+x_3).
\end{aligned}
$$

3.2 Main theorem

Now we will work on our main results in the case of a finite field of characteristic 2. Davies and Rousseau [6] have been shown for $n = 2$ the theorem holds if $\mathbb{F}_{2^\ell}$ has cardinality at most 4 and fails if its number of elements is greater than 4. Thus here we could begin with $n = 3$.

Theorem 3.5. Let $n, \ell \in \mathbb{N}$ with $n \geq 3, \ell \geq 2$ and let $\mathbb{F}_{2^\ell}$ be a finite field of characteristic 2 with cardinality $|\mathbb{F}_{2^\ell}| = 2^\ell \geq n$. Let f and h be functions over $\mathbb{F}_{2^\ell}$. Then for any n distinct elements $x_1, \ldots, x_n \in \mathbb{F}_{2^\ell}$, f and h satisfy

$$f[x_1, \ldots, x_n] = h(x_1 + \cdots + x_n), \tag{3.2}$$

if and only if f is equal to a polynomial of degree at most n over $\mathbb{F}_{2^\ell}$:

$$f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Proof. The inverse is sufficiancy part holds by Lemma 3.4.
So now we just prove the necessarily part. Here we could divide it in to two cases.

Case 1: n $\geq \ell$;
Write $n = \ell + r \leq 2^\ell$ with $0 \leq r \leq 2^\ell - \ell$. If $n = 2^\ell$, by Corollary 3.2 the result of Theorem 3.5 holds trivially without any restriction. Henceforth, we assume that $\ell \leq n < 2^\ell$. Referring to the shapes of the elements of $\mathbb{F}_{2^\ell}$ displayed in (2.2), we consider the following set of $n + 1$ distinct elements in $\mathbb{F}_{2^\ell}$ of the form

$$S_1 := \{0, 1, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r\}; \tag{3.3}$$

by choosing $b_1 \notin \{0, 1, \alpha, \ldots, \alpha^{\ell-1}\}, b_2 \notin \{0, 1, \alpha, \ldots, \alpha^{\ell-1}, b_1\}, b_3 \notin \{0, 1, \alpha, \ldots, \alpha^{\ell-1}, b_1, b_2\}$ and so on. Throughout as a convention if $n = \ell$, we simply the presence of the b_i's in the corresponding expressions. By Lemma 3.1 there exist a unique polynomial $f_1(x) \in \mathbb{F}_{2^\ell}[x]$ of degree at most n such that

$$f_1(u) = f(u) \quad \text{for all } u \in S_1. \tag{3.4}$$

Since $\deg f_1 \leq n$, by Lemma 3.4, for any n distinct elements $x_1, \ldots, x_n \in \mathbb{F}_{2^\ell}$, there is a (linear) polynomial h_1 such that

$$f_1[x_1, \ldots, x_n] = h_1(x_1 + \cdots + x_n); \tag{3.5}$$

we note in passing that if $\deg f_1 = n - 1$, the polynomial h_1 is a constant, while if $\deg f_1 < n - 1$, the polynomial h_1 vanishes identically. Let

$$F_1(x) = f(x) - f_1(x), \qquad H_1(x) = h(x) - h_1(x). \tag{3.6}$$

Observe from Lemma 2.8 that the divided difference of a function over n distinct points depend only on the points and the functional values at these points. Using the hypothesis (3.2), (3.4) and (3.5), we get

$$F_1[x_1, \ldots, x_n] = H_1(x_1 + \cdots + x_n) \tag{3.7}$$

and

$$F_1(u) = 0 \qquad \text{for all } u \in S_1. \tag{3.8}$$

We substitute the n points $x_1, \ldots, x_n$ in (3.7) by the following sets of points

- $1, \alpha, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r$,
- $0, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r$,
- $1, \alpha, \ldots, \alpha^{i-1}, 0, \alpha^{i+1}, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r$ for $1 \le i \le \ell - 2$,
- $1, \alpha, \ldots, \alpha^{\ell-2}, 0, b_1, \ldots, b_r$,
- $1, \alpha, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_r$ for $i = 1, \ldots, r$,

by using Lemma 2.8 and (3.8), we get

$$0 = F_1[1, \alpha, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r] = H_1(1 + \alpha + \cdots + \alpha^{\ell-1} + b_1 + \cdots + b_r), \tag{3.9}$$

$$0 = F_1[0, \alpha, \alpha^2, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r] = H_1\left(\sum_{j=0,\, j\neq 1}^{\ell-1} \alpha^j + \sum_{j=1}^{r} b_j\right), \tag{3.10}$$

$$0 = F_1[1, \alpha, \ldots, \alpha^{i-1}, 0, \alpha^{i+1}, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r] = H_1\left(\sum_{j=0,\, j\neq i}^{\ell-1} \alpha^j + \sum_{j=1}^{r} b_j\right) = 0, \tag{3.11}$$

$$0 = F_1[1, \alpha, \ldots, \alpha^{\ell-2}, 0, b_1, \ldots, b_r] = H_1\left(\sum_{j=0,\, j\neq \ell-1}^{\ell-1} \alpha^j + \sum_{j=1}^{r} b_j\right), \tag{3.12}$$

$$0 = F_1[1, \alpha, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_{i-1}, 0, b_{i+1}, \ldots, b_r] = H_1\left(\sum_{j=0}^{\ell-1} \alpha^j + \sum_{j=1,\, j\neq i}^{r} b_j\right). \tag{3.13}$$

To prove the desired result, we aim to show that $f \equiv f_1$, i.e., $F \equiv 0$. From (3.1), each element in $\mathbb{F}_{2^\ell}$ can be uniquely written as $x(0; i) = 0$, or for $m \in \{1, 2. \ldots, \ell\}$

$$x(m; i_1 : i_m) := \alpha^{i_1} + \alpha^{i_2} + \cdots + \alpha^{i_m}, \qquad 0 \le i_1 < i_2 < \cdots < i_m \le \ell - 1.$$

We proceed to show by induction on m that $F(x(m; i_1 : i_m)) = 0$ for all $x(m; i_1 : i_m)$.

Using (3.4), this clearly holds when $m = 0$ and 1. We work out the next two values of m to explicitly illustrate the lines of proof.

When $m = 2$, the field elements are of the form

$$x(2; i_1 : i_2) = \alpha^{i_1} + \alpha^{i_2}, \qquad 0 \le i_1 < i_2 \le \ell - 1,$$

and because of (3.8) we need only consider these elements for which $x(2;i_1:i_2) \neq b_s \quad (s=1,2,\ldots,r)$. We substitute for the n points $x_1,\ldots,x_n$ in (3.7) by

$$1,\alpha,\ldots,\alpha^{i_1-1},x(2;i_1:i_2),\alpha^{i_1+1},\ldots,\alpha^{\ell-1},b_1,\ldots,b_r,$$

and by using (3.10) or (3.11) or (3.12), with $i=i_2$, we get

$$F_1[1,\alpha,\ldots,\alpha^{i_1-1},x(2;i_1:i_2),\alpha^{i_1+1},\ldots,\alpha^{\ell-1},b_1,\ldots,b_r]=H_1\left(\sum_{j=0,\ j\neq i_2}^{\ell-1}\alpha^j+\sum_{j=1}^{r}b_j\right)=0.$$

Expanding the left-hand expression by Lemma 2.8 and using (3.8), we get

$$\frac{F_1(x(2;i_1:i_2))}{D(x)}=0,$$

where

$$D(x):=(x(2;i_1:i_2)+1)\cdots(x(2;i_1:i_2)+\alpha^{i_1-1})(x(2;i_1:i_2)+\alpha^{i_1+1})\times\cdots$$
$$\times(x(2;i_1:i_2)+\alpha^{\ell-1})(x(2;i_1:i_2)+b_1)\cdots(x(2;i_1:i_2)+b_r)\neq 0,$$

which clearly implies that $F_1(x(2;i_1:i_2))=0$.

When $m=3$, the field elements are of the form

$$x(3;i_1:i_3)=\alpha^{i_1}+\alpha^{i_2}+\alpha^{i_3},\qquad 0\leq i_1<i_2<i_3\leq \ell-1,$$

and because of (3.8) we need consider only those $x(3;i_1:i_3)\neq b_s \quad (s=1,\ldots,r)$. We need to analyze two possibilities depending on whether any sum of two elements in $x(3;i_1:i_3)$ coincides with one of the elements $b_s \quad (s=1,\ldots,r)$.

Possibility 1: none of the elements $\sum_{j=1,\ j\neq t}^{3}\alpha^{i_j}$ $(t=1,2,3)$ is equal to some $b_s \quad (s=1,2,\ldots,r)$. Substituting $x_1,\ldots,x_n$ in (3.7) by

$$1,\alpha,\ldots,\alpha^{i_1-1},x(3;i_1:i_3),\alpha^{i_1+1},\ldots,\alpha^{i_2-1},x(2;i_2:i_3),\alpha^{i_2+1},\ldots,\alpha^{\ell-1},b_1,\ldots,b_r,$$

where $x(2;i_2:i_3)=\alpha^{i_2}+\alpha^{i_3}$ satisfies, from the case $m=2$, $F(x(2;i_2:i_3))=0$, and using (3.11) with $i=i_2$ for the vanishing of the right-hand expression, we get

$$F_1[1,\alpha,\ldots,\alpha^{i_1-1},x(3;i_1:i_3),\alpha^{i_1+1},\ldots,\alpha^{i_2-1},x(2;i_2:i_3),\alpha^{i_2+1},\ldots,\alpha^{\ell-1},b_1,\ldots,b_r]$$
$$=H_1\left(\sum_{j=0,\ j\neq i_2}^{\ell-1}\alpha^j+\sum_{j=1}^{r}b_j\right)=0.$$

Expanding the left-hand expression by Lemma 2.8, using (3.8) and the case $m=2$, we deduce that $F_1(x(3;i_1:i_3))=0$.

Possibility 2: there exists $t\in\{1,2,3\}$ such that $\sum_{j=1,\ j\neq t}^{3}\alpha^{i_j}=b_s$ for some $s\in\{1,2,\ldots,r\}$, which implies $x(3;i_1:i_3)=\alpha^{i_t}+b_s$. Substituting $x_1,\ldots,x_n$ in (3.7) by

$$1,\alpha,\ldots,\alpha^{i_t-1},x(3;i_1:i_3),\alpha^{i_t+1},\ldots,\alpha^{\ell-1},b_1,\ldots,b_r,$$

and using (3.13) with $i = s$, we get

$$F_1[1, \alpha, \ldots, \alpha^{i_t-1}, x(3; i_1 : i_3), \alpha^{i_t+1}, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r] = H_1\left(\sum_{j=0}^{\ell-1}\alpha^j + \sum_{j=1,\, j\neq s}^{r} b_j\right) = 0,$$

and as before, we deduce that $F(x(3; i_1 : i_3)) = 0$.

Proceeding with the induction, assume this is true up to $m = k-1$, i.e., $F_1(x(k-1; i_1 : i_{k-1})) = 0$, where

$$x(k-1; i_1 : i_{k-1}) = \alpha^{i_1} + \cdots + \alpha^{i_{k-1}}, \qquad 0 \le i_1 < \cdots < i_{k-1} \le \ell - 1,$$

with $x(k-1; i_1 : i_{k-1}) \neq b_s \quad (s = 1, \ldots, r)$. As in the case $m = 3$, two possibilities depending on whether any sum of $k-1$ elements in $x(k; i_1 : i_k)$ coincides with one of the b_s need to be analyzed.

Possibility 1: none of the elements $\sum_{j=1,\, j\neq t}^{k} \alpha^{i_j} \quad (t = 1, \ldots, k)$ is equal to some b_s. Substituting $x_1, \ldots, x_n$ in (3.7) by

$$1, \alpha, \ldots, \alpha^{i_1-1}, x(k; i_1 : i_k), \alpha^{i_1+1}, \ldots, \alpha^{i_2-1}, x(k-1; i_2 : i_k), \alpha^{i_2+1} \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r,$$

where $x(k-1; i_2 : i_k) = \alpha^{i_2} + \cdots + \alpha^{i_k}$ satisfies, by induction hypothesis, $F_1(x(k-1; i_2 : i_k)) = 0$, and using (3.10) or (3.11) or (3.12) for the vanishing of the right-hand expression, we get

$$F_1[x_1, \ldots, x_n] = H_1\left(\sum_{j=0,\, j\neq i_2}^{\ell-1} \alpha^j + \sum_{j=1}^{r} b_j\right) = 0.$$

Expanding the left-hand expression by Lemma 2.8, using (3.8) and the induction hypothesis, we get $F_1(x(k; i_1 : i_k)) = 0$.

Possibility 2: there exists $t \in \{1, \ldots, k\}$ such that $\sum_{j=1,\, j\neq t}^{k} \alpha^{i_j} = b_s$ for some $s \in \{1, 2, \ldots, r\}$, so that $x(k; i_1 : i_k) = \alpha^{i_t} + b_s$. Substituting $x_1, \ldots, x_n$ in(3.7) by

$$1, \alpha, \ldots, \alpha^{i_t-1}, x(k; i_1 : i_k), \alpha^{i_t+1}, \ldots, \alpha^{\ell-1}, b_1, \ldots, b_r,$$

and using (3.13) with $i = s$ for the vanishing of the right-hand expression, we get

$$F_1[1, \alpha, \ldots, \alpha^{i_t-1}, x(k; i_1 : i_k), \alpha^{i_t+1}, \ldots, \alpha^{l-1}, b_1, \ldots, b_r] = H_1\left(\sum_{j=0}^{\ell-1}\alpha^j + \sum_{j=1,\, j\neq s}^{r} b_j\right) = 0.$$

As before, expanding the left-hand expression by Lemma 2.8, using (3.8), we deduce that $F_1(x(k; i_1 : i_k)) = 0$, which completes the induction, and the theorem is proved in this case.

Case 2: $3 \le n \le \ell - 1$;

Though the steps of proof are much the same as in case 1, the analysis is somewhat more involved, so we give most of the details. We consider the set of $n+1$ distinct elements in $\mathbb{F}_{2^\ell}$ of the form

$$S_2 := \{0, 1, \alpha, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}\}. \tag{3.14}$$

Note: *The sum of non-zero n distinct elements in S are zero. So, this choice of distinct elements are possible only when $n \geq 3$, which explains why the counter-example of Davies-Rousseau only works for $n = 2$.*

By Lemma 3.1, there is a unique polynomial $f_2(x) \in \mathbb{F}_{2^\ell}[x]$, $\deg f_2 \leq n$, such that

$$f_2(u) = f(u) \quad \text{for all } u \in S_2.$$

By Lemma 3.4, for any n distinct elements $x_1, \ldots, x_n \in \mathbb{F}_{2^\ell}$, there is a (linear) polynomial $h_2(x) \in \mathbb{F}_{2^\ell}[x]$ such that

$$f_2[x_1, \ldots, x_n] = h_2(x_1 + \cdots + x_n). \tag{3.15}$$

Let

$$F_2(x) = f(x) - f_2(x), \qquad H_(x) = h(x) - h_2(x). \tag{3.16}$$

Since the divided difference on n points depends only on the points (Lemma 2.8), using the main hypothesis (3.2), (3.15) and (3.16), for distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$, we have

$$F_2[x_1, \ldots, x_n] = H_2(x_1 + \cdots + x_n) \tag{3.17}$$

and

$$F_2(u) = 0 \quad \text{for all } u \in S_2. \tag{3.18}$$

Substituting the n distinct points $x_1, \ldots, x_n$ in (3.17) by the following sets of points

- $1, \alpha, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}$,
- $0, \alpha, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}$,
- $1, \alpha, \ldots, \alpha^{i-1}, 0, \alpha^{i+1}, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}$ for $i = 1, 2, \ldots, n-3$,
- $1, \alpha, \ldots, \alpha^{n-3}, 0, 1 + \alpha + \cdots + \alpha^{n-2}$,
- $1, \alpha, \ldots, \alpha^{n-2}, 0$,

using Lemma 2.8 and (3.18) for the vanishing of the left-hand side, we get

$$0 = F_2[1, \alpha, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}] = H_2(0), \tag{3.19}$$

$$0 = F_2[0, \alpha, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}] = H_2(1), \tag{3.20}$$

$$0 = F_2[1, \alpha, \ldots, \alpha^{i-1}, 0, \alpha^{i+1}, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}] = H_2(\alpha^i) \quad (1 \leq i \leq n-3), \tag{3.21}$$

$$0 = F_2[1, \alpha, \ldots, \alpha^{n-3}, 0, 1 + \alpha + \cdots + \alpha^{n-2}] = H_2(\alpha^{n-2}), \tag{3.22}$$

$$0 = F_2[1, \alpha, \ldots, \alpha^{n-2}, 0] = H_2(1 + \alpha + \cdots + \alpha^{n-2}). \tag{3.23}$$

As in case 1, our objective is to prove that $f \equiv f_2$ by showing the polynomial $F_2 := f - f_2$ vanishes at every point in $\mathbb{F}_{2^\ell}$. To do so, we subdivide our analysis into three steps

depending on the shapes of the field elements.

Step 1. We show that $F_2(z) = 0$ at the points

$$z(m; i_1 : i_m) := \alpha^{i_1}+\alpha^{i_2}+\cdots+\alpha^{i_m}, \qquad 0 \le i_1 < i_2 < \cdots < i_m \le n-2, \qquad m \in \{1, 2, \ldots, n-1\},$$

where we may assume, without loss of generality, that these numbers are not in S_2. This assertion clearly holds when $m = 1$ by (3.18). For the remaining values of m, we proceed by induction on m (≥ 2). Starting with $m = 2$, substituting $x_1, \ldots, x_n$ in (3.17) by

$$1, \alpha, \ldots, \alpha^{i_1-1}, z(2; i_1 : i_2), \alpha^{i_1+1}, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2},$$

and using (3.21) or (3.22) for the vanishing of the right-hand expression, we get

$$F_2[1, \alpha, \ldots, \alpha^{i_1-1}, z(2; i_1 : i_2), \alpha^{i_1+1}, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}] = H_2(\alpha^{i_2}) = 0.$$

Expanding the left expression by Lemma 2.8, using (3.18), we deduce that $F_2(z(2; i_1 : i_2)) = 0$. Assume now that the assertion holds for $m = 2, 3, \ldots, k-1$. Substituting $x_1, \ldots, x_n$ in (3.17) by

$$1, \alpha, \ldots, \alpha^{i_1-1}, z(k; i_1 : i_k), \alpha^{i_1+1}, \ldots, \alpha^{i_2-1}, z(k-1; i_2 : i_k), \alpha^{i_2+1}, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}$$

where

$$z(k; i_1 : i_k) = \alpha^{i_1} + \alpha^{i_2} + \alpha^{i_3} + \cdots + \alpha^{i_k} \notin S_2, \qquad z(k-1; i_2 : i_k) = \alpha^{i_2} + \alpha^{i_3} + \cdots + \alpha^{i_k} \notin S_2$$
$$(0 \le i_1 < i_2 < \cdots < i_k \le n-2),$$

and using (3.21) or (3.22) for the vanishing of the right-hand expression, we get

$$F_2[x_1, \ldots, x_n] = H_2(\alpha^{i_2}) = 0.$$

Expanding the left-hand expression by Lemma 2.8, using (3.18) and $F_2(z(k-1; i_2 : i_k) = 0$ from the induction hypothesis, we deduce that

$$0 = \frac{F_2(z(k; i_1 : i_k)}{D_2}$$

where

$$D_2 := (z(k; i_1 : i_k)+z(k-1; i_2 : i_k))(z(k; i_1 : i_k)+1+\alpha+\cdots+\alpha^{n-2}) \prod_{j=0,\, j\neq i_1, i_2}^{n-2} (z(k; i_1 : i_k)+\alpha^j) \neq 0,$$

yielding $F_2(z(k; i_1 : i_k)) = 0$, and the induction is complete.

Remark. As an immediate consequence, substituting $x_1, \ldots, x_n$ in (3.17) by

$$z(m; i_1 : i_k), 1 + \alpha, \alpha^2, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2},$$

using the results in Lemma 2.8 and Step 1, we have

$$0 = F_2[z(m; i_1 : i_m), 1 + \alpha, \alpha^2, \ldots, \alpha^{n-2}, 1 + \alpha + \cdots + \alpha^{n-2}] = H_2(z(m; i_1 : i_m)).$$

Step 2. We will show that $F(\alpha^j) = 0$ for $j \in \{n-1, n, \ldots, \ell-1\}$.
When $n = 3$, we take $S_2 := \{1, \alpha, \alpha+1\}$. We substitute x_1, x_2, x_3 in (3.17) by

$$\alpha^j, \alpha^j + \alpha + 1, 0;$$

now $H_2(\alpha+1) = 0$ and $F_2(0) = 0$, so as before

$$0 = H_2(\alpha+1) = F_2[\alpha^j, \alpha^j+1, 0] = \frac{F_2(\alpha^j)}{\alpha^j(\alpha+1)} + \frac{F_2(\alpha^j+\alpha+1)}{(\alpha^j+\alpha+1)(\alpha+1)}. \tag{3.24}$$

Then we substitute x_1, x_2, x_3 by

$$\alpha^j, \alpha^j + \alpha + 1, \alpha + 1,$$

so again

$$0 = H_2(0) = F_2[\alpha^j, \alpha^j+\alpha+1, \alpha+1] = \frac{F_2(\alpha^j)}{(\alpha+1)(\alpha^j+\alpha+1)} + \frac{F_2(\alpha^j+\alpha+1)}{\alpha^j(\alpha+1)}. \tag{3.25}$$

From (3.24) and (3.25), we get the system

$$(\alpha^j+\alpha+1)F_2(\alpha^j) + \alpha^j F_2(\alpha^j+\alpha+1) = 0$$
$$\alpha^j F_2(\alpha^j) + (\alpha^j+\alpha+1)F_2(\alpha^j+\alpha+1) = 0.$$

From above system, we have $F_2(\alpha^j) = F_2(\alpha^i+\alpha+1) = 0$.
When $n \geq 4$, we substitute $x_1, \ldots, x_n$ in (3.17) by

$$\alpha^j, \alpha^j + 1 + \alpha, 0, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2},$$

using (3.2), Lemma 2.8, the results from Step 1 and (3.21), we get

$$\begin{aligned} 0 = H_2(\alpha^2) &= F[\alpha^j, \alpha^j+1+\alpha, 0, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2}] \\ &= \frac{F_2(\alpha^j)}{\alpha^j(1+\alpha)(\alpha^j+\alpha^3)\cdots(\alpha^j+\alpha^{n-2})(\alpha^j+1+\cdots+\alpha^{n-2})} \\ &+ \frac{F_2(\alpha^j+1+\alpha)}{(\alpha^j+1+\alpha)(1+\alpha)(\alpha^j+1+\alpha+\alpha^3)\cdots(\alpha^j+1+\alpha+\alpha^{n-2})(\alpha^j+\alpha^2+\cdots+\alpha^{n-2})}. \end{aligned}$$

Simplifying, we get

$$(\alpha^j+1+\alpha)B \cdot F_2(\alpha^j) + \alpha^j A \cdot F_2(\alpha^j+1+\alpha) = 0 \tag{3.26}$$

where $A = (1+\alpha)(\alpha^j+\alpha^3)\cdots(\alpha^j+\alpha^{n-2})(\alpha^j+1+\cdots+\alpha^{n-2}) \neq 0,$

$$B = (1+\alpha)(\alpha^j+1+\alpha+\alpha^3)\cdots(\alpha^j+1+\alpha+\alpha^{n-2})(\alpha^j+\alpha^2+\cdots+\alpha^{n-2}) \neq 0.$$

Substituting $x_1, \ldots, x_n$ in (3.17) by

$$\alpha^j, \alpha^j+1+\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2},$$

using (3.19), the results from Step 1 and Lemma 2.8, we get

$$0 = H_2(0) = F_2[\alpha^j, \alpha^j+1+\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2}]$$

$$= \frac{F_2(\alpha^j)}{(\alpha^j+\alpha^2)(1+\alpha)(\alpha^j+\alpha^3)\cdots(\alpha^j+\alpha^{n-2})(\alpha^j+1+\cdots+\alpha^{n-2})}$$
$$+ \frac{F_2(\alpha^j+1+\alpha)}{(\alpha^j+1+\alpha+\alpha^2)(1+\alpha)(\alpha^j+1+\alpha+\alpha^3)\cdots(\alpha^j+1+\alpha+\alpha^{n-2})(\alpha^j+\alpha^2+\cdots+\alpha^{n-2})}.$$

Simplifying, we get

$$(\alpha^j+1+\alpha+\alpha^2)B\cdot F_2(\alpha^j)+(\alpha^j+\alpha^2)A\cdot F_2(\alpha^j+1+\alpha)=0. \tag{3.27}$$

Solving (3.26) and (3.27), we obtain

$$0=F_2(\alpha^j)=F_2(\alpha^j+1+\alpha)=0 \quad \text{for all } j\in\{n-1,n,\ldots,\ell-1\}, \tag{3.28}$$

which completes the proof of Step 2.

Remark. Substituting $x_1,\ldots,x_n$ in (3.17) by

$$\alpha^j, 1+\alpha, \alpha^2,\ldots,\alpha^{n-2}, 1+\cdots+\alpha^{n-2} \qquad (j=n-1,n-2,\ldots,\ell-1),$$

using the results in Lemma 2.8, Steps 1 and 2, we have

$$0=F_2[\alpha^j,1+\alpha,\alpha^2,\ldots,\alpha^{n-2},1+\cdots+\alpha^{n-2}]=H_2(\alpha^j) \quad \text{for all } j\in\{n-1,n,\ldots,\ell-1\}.$$

Step 3. We show by induction on j that $F_2(y_j)=0$ for all $j\in\{n-1,n,\ldots,\ell-1\}$, where

$$y_j=\alpha^j+a_{j-1}\alpha^{j-1}+a_{j-2}\alpha^{j-2}+\cdots+a_0\in\mathbb{F}_2[\alpha], \qquad y_j\neq\alpha^j.$$

For $j=n-1$, since

$$y_{n-1}=\alpha^{n-1}+a_{n-2}\alpha^{n-2}+\cdots+a_0\in\mathbb{F}_2[\alpha], \qquad y_{n-1}\neq\alpha^{n-1},$$

we need to consider two subcases depending on the shape of $T_{n-1}:=a_{n-2}\alpha^{n-2}+\cdots+a_0$.

Subcase 1: $T_{n-1}\notin S_2$.

Substituting $x_1,\ldots,x_n$ in (3.17) by

$$y_{n-1},\alpha^{n-1},1+\alpha+\alpha^2,\alpha^3,\ldots,\alpha^{n-2},1+\alpha+\alpha^2+\cdots+\alpha^{n-2},$$

using the result in Step 1 and its remark for the vanishing of the H-value, Lemma 2.8, the result in Step 2 and (3.18), we obtain

$$0=H_2(T_{n-1})=F_2[y_{n-1},\alpha^{n-1},1+\alpha+\alpha^2,\alpha^3,\ldots,\alpha^{n-2},1+\alpha+\alpha^2+\cdots+\alpha^{n-2}]$$
$$=\frac{F_2(y_{n-1})}{(y_{n-1}+\alpha^{n-1})(y_{n-1}+1+\alpha+\alpha^2)(y_{n-1}+\alpha^3)\cdots(y_{n-1}+\alpha^{n-2})(y_{n-1}+1+\alpha+\cdots+\alpha^{n-2})},$$

which yields $F_2(y_{n-1})=0$.

Subcase 2: $T_{n-1}\in S_2$.

Substituting $x_1,\ldots,x_n$ in (3.17) by

$$y_{n-1},\alpha^{n-1},1+\alpha+\alpha^2,\alpha^3,\ldots,\alpha^{n-2},1+\alpha+\alpha^2+\cdots+\alpha^{n-2},$$

we see that the divided difference $F_2[y_{n-1}, \alpha^{n-1}, 1+\alpha+\alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2}]$ is equal to $H(0)$, or $H(\alpha^i)$ for some $i \in \{0, 1, \ldots, n-2\}$, or $H(1+\alpha+\cdots+\alpha^{n-2})\}$; all three of these last H-values are 0 because of (3.19), or (3.20), or (3.21), or (3.22), or (3.23). Expanding the divided difference via Lemma 2.8, using the results in Steps 1-2 and (3.18), we obtain $F_2(y_{n-1}) = 0$.

Remark. Substituting $x_1, \ldots, x_n$ in (3.17) by

$$y_{n-1}, 1+\alpha, \alpha^2, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2},$$

using (3.18), the results in Steps 1-2, the last Subcase 2 and Lemma 2.8 for the vanishing of the left-hand divided difference, we get

$$0 = F_2[y_{n-1}, 1+\alpha, \alpha^2, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2}] = H_2(y_{n-1}).$$

Returning to the induction process, from the case $j = n-1$ above and the last remark, we slightly modify our pending induction hypothesis to be that both $F_2(y_j)$ and $H_2(y_j)$ vanish for $j = n-1, n, \ldots, k-1$, and proceed now to verify that it holds when $j = k$. Recall that

$$y_k = \alpha^k + a_{k-1}\alpha^{k-1} + a_{k-2}\alpha^{k-2} + \cdots + a_0 \in \mathbb{F}_2[\alpha],\ y_k \neq \alpha^k.$$

As before, we need to consider two subcases depending on the shape of $T_k := a_{k-1}\alpha^{k-1} + a_{k-2}\alpha^{k-2} + \cdots + a_0$.

Subcase 2.1*:* $T_k \notin S_2$.

When $n \geq 4$, substituting $x_1, \ldots, x_n$ in (3.17) by

$$y_k, \alpha^k, 1+\alpha+\alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2},$$

and using the induction hypothesis for the vanishing H-value, we get

$$F_2[y_k, \alpha^k, 1+\alpha+\alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2}] = H_2(a_{k-1}\alpha^{k-1} + \cdots + a_0) = 0.$$

Expanding the divided difference using Lemma 2.8, using the results in Steps 1-2 and (3.18), we get $F_2(y_k) = 0$.

When $n = 3$, substituting x_1, x_2, x_3 by $y_k, \alpha^k, 0$ again

$$0 = H_2(T_k) = F_2[y_k, \alpha^k, 0] = \frac{F_2(y_k)}{y_k\alpha^k}.$$

Subcase 2.2*:* $T_k \in S_2$.

Substituting $x_1, \ldots, x_n$ in (3.17) by

$$y_k, \alpha^k, 1+\alpha+\alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2},$$

we see that the divided differences $F_2[y_k, \alpha^k, 1+\alpha+\alpha^2, \alpha^3, \ldots, \alpha^{n-2}, 1+\alpha+\cdots+\alpha^{n-2}]$ is equal to $H_2(0)$, or $H_2(\alpha^i)$ for some $i \in \{0, 1, \ldots, n-2\}$, or $H_2(1+\cdots+\alpha^{n-2})$, and these H-values vanish because of (3.19), or (3.20), or (3.21), or (3.22), or (3.23). Expanding

the divided difference using Lemma 2.8, using the results in Steps 1-2 and (3.18), we deduce that $F_2(y_k) = 0$, which completes the induction.

The results of Steps 1-3 show that $F(x) = 0$ for all $x \in \mathbb{F}_{2^\ell}$, and Theorem 3.5 is proved.

□

Remark 3.6. In here, we will discuss on the problem when $n = 2$.

1. For $\mathbb{F}_2 = \{0, 1\}$, the theorem holds by Lemma 3.2.
2. For $\mathbb{F}_{2^2} = \{0, 1, \alpha, \alpha + 1\}$ where α is a root of irreducible polynomial of degree 2, $x^2 + x + 1$, our theorem holds and we can prove it by using the same method of the Case $n \geq \ell$ in the proof of Theorem 3.5 or using the method in appendex of Davies-Rousseau [6].
3. For $| \mathbb{F}_{2^\ell} | > 4$ (The counter-example of Davies-Rousseau [6].), the theorem does not hold. By our method, it is in the Case of $n \leq \ell - 1$ and we cannot choose any two distinct elements $x_1, x_2 \in \mathbb{F}_{2^\ell} \setminus \{0\}$ such that

$$x_1 + x_2 = 0.$$

Example 3.2. For $n \geq \ell$, we set $n = 3$ and $\ell = 3$. Let β be the root of irreducible polynomial of degree 3, $x^3 + x + 1 \in \mathbb{F}_2[x]$. Then we get

$$\mathbb{F}_{2^3} := \{0, 1, \beta, \beta + 1, \beta^2, \beta^2 + 1, \beta^2 + \beta, \beta^2 + \beta + 1\}$$

and $| \mathbb{F}_{2^3} | = 2^3 = 8$. Suppose $f, h : \mathbb{F}_{2^3} \to \mathbb{F}_{2^3}$ satisfy

$$f[x_1, x_2, x_3] = h(x_1 + x_2 + x_3)$$

for any 3 distinct points $x_1, x_2, x_3 \in \mathbb{F}_{2^3}$. Now we will use the same method as in the case $n \geq \ell$ of Theorem 3.5's proof to show that f is a polynomial of degree at most 3 over $\mathbb{F}_{2^3}[x]$ as following.

We shoose 4 distincts elements in $S := \{0, 1, \beta, \beta^2\} \subseteq \mathbb{F}_{2^3}$. By Lemma 3.1, there exists a polynomial $f_1(x)$ of degree at most 3 such that $f(u) = f_1(u) \quad \forall u \in S$ and by Lemma 3.4, there exist a polynomial $h_1(x)$ such that $f_1[x_1, x_2, x_3] = h_1(x_1 + x_2 + x_3)$ for any 3 distinct points $x_1, x_2, x_3 \in \mathbb{F}_{2^3}$. We set $F(x) = f(x) - f_1(x)$ and $H(x) = h(x) - h_1(x)$. Then

$$F[x_1, x_2, x_3] = H(x_1 + x_2 + x_3)$$

for distinct elements $x_1, x_2, x_3 \in \mathbb{F}_{2^3}$ and $F(u) = 0$ for all $u \in S$.

Substituting x_1, x_2, x_3 by

$$1, \beta, \beta^2,$$

$$0, \beta, \beta^2,$$

$$1, 0, \beta^2,$$
$$1, \beta, 0,$$

and applying 3-rd order divided-differences of F, we get

$$F[1, \beta, \beta^2] = H(1 + \beta + \beta^2) = 0,$$
$$F[0, \beta, \beta^2] = H(\beta + \beta^2) = 0,$$
$$F[1, 0, \beta^2] = H(1 + \beta^2) = 0,$$
$$F[1, \beta, 0] = H(1 + \beta) = 0.$$

Next we will show that $F(x) = 0$ for all $x \in \mathbb{F}_{2^3}$. Substituting x_1, x_2, x_3 by

$$1, \beta + 1, \beta^2,$$
$$1, \beta, \beta^2 + \beta,$$
$$1, \beta + \beta^2, \beta^2,$$

and applying 3-rd order divided-differences of F, we get

$$F[1, \beta + 1, \beta^2] = \frac{\beta + 1}{\beta(\beta^2 + \beta + 1)} = H(\beta^2 + \beta) = 0,$$
$$F[1, \beta, \beta^2 + \beta] = \frac{\beta^2 + \beta}{(\beta^2 + \beta + 1)\beta^2} = H(\beta^2 + 1) = 0,$$
$$F[1, \beta + \beta^2, \beta^2] = \frac{\beta^2 + \beta}{\beta(\beta^2 + \beta + 1)} = H(\beta + 1) = 0.$$

So we get $F(\beta + 1) = F(\beta^2 + 1) = F(\beta^2 + \beta) = 0$.
Substituting x_1, x_2, x_3 by $1, \beta + 1, \beta^2 + \beta + 1$ and applying 3-rd order divided-differences of F, we get

$$F[1, \beta + 1, \beta^2 + \beta + 1] = \frac{F(\beta^2 + \beta + 1)}{(\beta^2 + \beta)\beta^2} = H(\beta^2 + 1) = 0.$$

Hence, $F(\beta^2 + \beta + 1) = 0$. Therefore, $F(x) = 0$ for all $x \in \mathbb{F}_{2^3}$.

Example 3.3. For $n \leq \ell - 1$, we set $n = 3$ and $\ell = 4$. Let α be the root of an irreducible polynomial of degree 4, $x^4 + x + 1 \in \mathbb{F}_2[x]$. Then we get

$$\mathbb{F}_{2^4} := \{0, 1, \alpha, \alpha + 1, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha, \alpha^2 + \alpha + 1, \alpha^3, \alpha^3 + 1, \alpha^3 + \alpha, \alpha^3 + \alpha + 1,$$
$$\alpha^3 + \alpha^2, \alpha^3 + \alpha^2 + 1, \alpha^3 + \alpha^2 + \alpha, \alpha^3 + \alpha^2 + \alpha + 1\}$$

and $| \mathbb{F}_{2^4} | = 2^4 = 16$. Now let $f, h : \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ satisfy

$$f[x_1, x_2, x_3] = h(x_1 + x_2 + x_3)$$

for any distinct x_1, x_2, x_3 in $\mathbb{F}_{2^4}$. We will use the same method as in the case $3 \leq n \leq \ell - 1$ of the proof of Theorem 3.5 to show that f is a polynomial of degree at most 3 over $\mathbb{F}_{2^4}$ as following.

We choose 4 distinct elements in the form $S := \{0, 1, \alpha, \alpha + 1\} \subseteq \mathbb{F}_{2^3}$. By Lemma 2.9, there exists a polynomial $f_1(x)$ of degree at most 3 such that $f(u) = f_1(u) \quad \forall u \in S$ and by Lemma 3.4, there exists a polynomial $h_1(x)$ such that $f_1[x_1, x_2, x_3] = h_1(x_1 + x_2 + x_3)$ for any 3 distinct $x_1, x_2, x_3 \in \mathbb{F}_{2^4}$.

We set $F(x) = f(x) - f_1(x)$ and $H(x) = h(x) - h_1(x)$. Then

$$F[x_1, x_2, x_3] = H(x_1 + x_2 + x_3)$$

for distinct elements $x_1, x_2, x_3 \in \mathbb{F}_{2^4}$ and $F(u) = 0$ for all $u \in S$.

Substituting 3 distinct points x_1, x_2, x_3 by

$$1, \alpha, \alpha + 1,$$

$$0, \alpha, \alpha + 1,$$

$$1, 0, \alpha + 1,$$

$$1, \alpha, 0,$$

and applying 3-rd order divided-differences of F, we get

$$F[1, \alpha, \alpha + 1] = H(1 + \alpha + \alpha + 1) = H(0) = 0,$$

$$F[0, \alpha, \alpha + 1] = H(0 + \alpha + \alpha + 1) = H(1) = 0,$$

$$F[1, 0, \alpha + 1] = H(1 + 0 + \alpha + 1) = H(\alpha) = 0,$$

$$F[1, \alpha, 0] = H(1 + \alpha + 0) = H(\alpha + 1) = 0.$$

Next we will show that $F(x) = 0$ for all $x \in \mathbb{F}_{2^3}$. Substituting x_1, x_2, x_3 by $\alpha^2 + 1, 1, \alpha^2$ and applying 3-rd order divided-diferences of F, we get

$$F[\alpha^2 + 1, 1, \alpha^2] = \frac{F(\alpha^2 + 1)}{\alpha^2} + \frac{F(\alpha^2)}{\alpha^2 + 1} = H(0) = 0. \tag{3.29}$$

Substituting x_1, x_2, x_3 by $\alpha^2 + 1, 0, \alpha^2$ and applying 3-rd order divided-differences of F, we get

$$F[\alpha^2 + 1, 0, \alpha^2] = \frac{F(\alpha^1 + 1)}{\alpha^2 + 1} + \frac{F(\alpha^2)}{\alpha^2} = H(1) = 0. \tag{3.30}$$

Solving the system equations (3.29) and (3.30), we get

$$F(\alpha^2) = F(\alpha^2 + 1) = 0$$

and consequencely we get

$$H(\alpha^2) = H(\alpha^2 + 1) = 0$$

when we substitute x_1, x_2, x_3 by $0, 1, \alpha^2 + 1$ and $0, 1, \alpha^2$ respectively.

Similarly for $F(\alpha^3) = F(\alpha^3 + 1) = 0$ and $H(\alpha^3) = H(\alpha^3 + 1) = 0$.

Substituting x_1, x_2, x_3 by

$$\alpha, \alpha^2 + \alpha, \alpha^2,$$

$$\alpha^2, \alpha^2+\alpha^3, \alpha^3,$$
$$\alpha, \alpha^3+\alpha, \alpha^3,$$

and applying 3-rd order divided-differences of F, we get

$$F[\alpha, \alpha^2+\alpha, \alpha^2] = \frac{F(\alpha^2+\alpha)}{\alpha \cdot \alpha^2} = H(0) = 0,$$
$$F[\alpha^2, \alpha^2+\alpha^3, \alpha^3] = \frac{F(\alpha^3+\alpha^2)}{\alpha^3 \cdot \alpha^2} = H(0) = 0,$$
$$F[\alpha, \alpha^3+\alpha, \alpha^3] = \frac{F(\alpha^3+\alpha)}{\alpha^3 \cdot \alpha} = H(0) = 0.$$

So $F(\alpha^2+\alpha) = F(\alpha^3+\alpha) = F(\alpha^3+\alpha^2) = 0$ and consequencely $H(\alpha^2+\alpha) = H(\alpha^3+\alpha) = H(\alpha^3+\alpha^2) = 0$.

Next substituting x_1, x_2, x_3 by

$$\alpha^2+\alpha+1, \alpha+1, \alpha^2,$$
$$\alpha^3+\alpha+1, \alpha+1, \alpha^3,$$
$$\alpha^3+\alpha^2+1, \alpha^2+1, \alpha^3,$$
$$\alpha^3+\alpha^2+\alpha, \alpha^2+\alpha, \alpha^3,$$

and applying 3-rd order divided-differences of F, we get

$$F[\alpha^2+\alpha+1, \alpha+1, \alpha^2] = \frac{F(\alpha^2+\alpha+1)}{\alpha^2(\alpha+1)} = H(0) = 0,$$
$$F[\alpha^3+\alpha+1, \alpha+1, \alpha^3] = \frac{F(\alpha^3+\alpha+1)}{\alpha^3(\alpha+1)} = H(0) = 0,$$
$$F[\alpha^3+\alpha^2+1, \alpha^2+1, \alpha^3] = \frac{F(\alpha^3+\alpha^2+1)}{\alpha^3(\alpha^2+1)} = H(0) = 0,$$
$$F[\alpha^3+\alpha^2+\alpha, \alpha^2+\alpha, \alpha^3] = \frac{F(\alpha^3+\alpha^2+\alpha)}{\alpha^3(\alpha^2+\alpha)} = H(0) = 0.$$

So we get $F(\alpha^2+\alpha+1) = F(\alpha^3+\alpha+1) = F(\alpha^3+\alpha^2+1) = F(\alpha^3+\alpha^2+\alpha) = 0$.

Last, substituting x_1, x_2, x_3 by $\alpha^3+\alpha^2+\alpha+1, \alpha^2+\alpha+1, \alpha^3$ and applying 3-rd order divided-differences of F, we get

$$F[\alpha^3+\alpha^2+\alpha+1, \alpha^2+\alpha+1, \alpha^3] = \frac{F(\alpha^3+\alpha^2+\alpha+1)}{\alpha^3(\alpha^2+\alpha+1)} = H(0) = 0.$$

So $F(\alpha^3+\alpha^2+\alpha+1) = 0$ and therefore $F(x) = 0$ for all $x \in \mathbb{F}_{2^4}$.

Hence, f is a polynomial of degree at most 3 over $\mathbb{F}_{2^4}$.

From the examples, we see that it is so easy if we use Theorem 3.5 with the problem of divided-differences characterization polynomials.

Chapter 4

On r-free integers in Beatty sequences

In this chapter, we prove an asymptotic formula for the existence of r-free numbers by using the result on the number of values in the Beatty sequences $\lfloor \alpha n + \beta \rfloor, \lfloor \alpha n + \beta \rfloor + 1$, in an arithmetic progression in [16]. On such values of Beatty sequences, we improve the equation (1.5) by using the ideas as in [14].

4.1 Auxilary lemmas

We need some lemmas here to prove our Theorems.

Lemma 4.1. For a fixed real $y > 1$, we have

$$\sum_{\substack{d,\,t \\ \gcd(d,t)=1 \\ dt \le y}} \frac{\mu(d)\mu(t)}{d^2t^2} = \prod_{p \text{ prime}} \Big(1 - \frac{2}{p^2}\Big) + O(y^{-1+\varepsilon}).$$

Proof. We have

$$A = \sum_{\substack{d,\,t \\ \gcd(d,t)=1 \\ dt \le y}} \frac{\mu(d)\mu(t)}{d^2t^2} = \sum_{\substack{d,\,t \\ \gcd(d,t)=1}} \frac{\mu(d)\mu(t)}{d^2t^2} - \sum_{\substack{dt > y \\ \gcd(d,t)=1}} \frac{\mu(d)\mu(t)}{d^2t^2}.$$

Let $m = dt$ for $\gcd(d,t) = 1$. By the properties of Möbius function in [19, p. 61], we have

$$-\sum_{\substack{dt > y \\ \gcd(d,t)=1}} \frac{\mu(d)\mu(t)}{d^2t^2} = -\sum_{m>y} \frac{\mu(m)d(m)}{m^2} = O\Big(\Big|\sum_{m>y} \frac{d(m)}{m^2}\Big|\Big).$$

So, we get

$$A = \sum_{m=1}^{\infty} \frac{\mu(m)d(m)}{m^2} + O\Big(\Big|\sum_{m>y} \frac{d(m)}{m^2}\Big|\Big).$$

In view of Lemma 2.33, for $\varepsilon > 0$, there exist a constant $c_\varepsilon = 1 > 0$ such that

$$d(m) \le c_\varepsilon m^\varepsilon = m^\varepsilon.$$

Thus,

$$\sum_{m>y} \frac{d(m)}{m^2} \le \sum_{m>y} m^{-2+\varepsilon}.$$

Since

$$\Big|\sum_{m>y} m^{-2+\varepsilon}\Big| = \Big|\int_y^\infty t^{-2+\varepsilon}\,\mathrm{dt}\Big| \ll t^{-1+\varepsilon}\Big|_y^\infty = y^{-1+\varepsilon},$$

the error term of A can be replaced by

$$O\Big(\Big|\sum_{m>y} m^{-2+\varepsilon}\Big|\Big) = O\Big(y^{-1+\varepsilon}\Big),$$

and so, using also [19, Theorem 11.7, p. 231], we get

$$\begin{aligned}
A &= \sum_{m=1}^{\infty} \frac{\mu(m)d(m)}{m^2} + O\Big(y^{-1+\varepsilon}\Big) \\
&= \prod_{p} \Big\{1 + \frac{\mu(p)d(p)}{p^2} + \frac{\mu(p^2)d(p^2)}{p^4} + \frac{\mu(p^3)d(p^3)}{p^6} + \cdots + \frac{\mu(p^n)d(p^n)}{p^{2n}} + \cdots \Big\} + O\Big(y^{-1+\varepsilon}\Big) \\
&= \prod_{p} \Big\{1 + \frac{(-1)\cdot 2}{p^2} + \frac{0\cdot 3}{p^4} + \frac{0\cdot 4}{p^6} + \cdots + \frac{0\cdot (n+1)}{p^{2n}} + \cdots \Big\} + O\Big(y^{-1+\varepsilon}\Big) \\
&= \prod_{p} \Big(1 - \frac{2}{p^2}\Big) + O\Big(y^{-1+\varepsilon}\Big).
\end{aligned}$$

□

Lemma 4.2. Let $\alpha > 1$ be an irrational and with bounded partial quotients, $\beta \in [0, \alpha)$, let x be a positive real number.

(I) If $A_{\alpha,\beta}(x)$ denotes the number of quadruples d, t, u, v of positive integers satisfying the conditions

$$t^2v - d^2u = 1, \qquad d^2u \le \alpha x + \beta, \qquad x^{1/4} < dt \le x^{2/3}, \tag{4.1}$$

then

$$A_{\alpha,\beta}(x) \ll \alpha x^{3/4+\varepsilon}.$$

(II) If $B_{\alpha,\beta}(x)$ denotes the number of quadruples d, t, u, v satisfying the conditions

$$t^2v - d^2u = 1, \qquad d^2u \le \alpha x + \beta, \qquad dt > x^{2/3}, \tag{4.2}$$

then

$$B_{\alpha,\beta}(x) \ll \alpha^2 x^{2/3+\varepsilon}.$$

Proof. (I) For any fixed choice of positive integers d and t satisfying (4.1), the condition $d^2u \equiv -1 (\mathrm{mod}\ t^2)$ fixes the value of u modulo t^2. Thus, by conditions in (4.1), the total number of possibilities for u is $O(1 + (\alpha x + \beta)/d^2t^2)$. By (4.1), the value of v is fixed, for any given d, t, u. Then

$$\begin{aligned}
A_{\alpha,\beta}(x) &\ll \sum_{x^{1/4} < dt \le x^{2/3}} (1 + (\alpha x + \beta)/d^2t^2) \\
&= \sum_{x^{\frac{1}{4}} < dt \le \alpha x + \beta} 1 + \sum_{x^{\frac{1}{4}} < dt \le \alpha x + \beta} (\alpha x + \beta)/d^2t^2 \\
&= \Big(\sum_{x^{\frac{1}{4}} < dt \le x^{\frac{2}{3}}} + \sum_{x^{\frac{2}{3}} < dt \le x^{\frac{3}{4}}} + \sum_{x^{\frac{3}{4}} < dt \le \alpha x + \beta} \Big) 1 \\
&+ \Big(\sum_{x^{\frac{1}{4}} < dt \le x^{\frac{2}{3}}} + \sum_{x^{\frac{2}{3}} < dt \le x^{\frac{3}{4}}} + \sum_{x^{\frac{3}{4}} < dt \le \alpha x + \beta} \Big) \frac{\alpha x + \beta}{d^2t^2} \\
&= \Big(\sum_{dt \le x^{\frac{2}{3}}} - \sum_{dt \le x^{\frac{1}{4}}} + \sum_{dt \le x^{\frac{3}{4}}} - \sum_{dt \le x^{\frac{2}{3}}} + \sum_{dt \le \alpha x + \beta} - \sum_{dt \le x^{\frac{3}{4}}} \Big) 1
\end{aligned}$$

$$+\Big(\sum_{dt\le x^{\frac{2}{3}}}-\sum_{dt\le x^{\frac{1}{4}}}+\sum_{dt\le x^{\frac{3}{4}}}-\sum_{dt\le x^{\frac{2}{3}}}+\sum_{dt\le \alpha x+\beta}-\sum_{dt\le x^{\frac{3}{4}}}\Big)\frac{\alpha x+\beta}{d^2t^2}.$$

In view of properties in [19],

- $\sum_{n\le x}T(n)=\sum_{n\le x}\sum_{d|n}1=\sum_{n\le x}1\ll x\log x$;
- $\sum_{n\le x}\frac{d(n)}{n^2}\ll\frac{1}{x^2}\sum_{n\le x}d(n)\ll(x\log x)/x^2\ll x^{-1}\log x$;

we have

$$\begin{aligned}
A_{\alpha,\beta}(x)&\ll\Big(\frac{3}{4}x^{\frac{3}{4}}\log x+\frac{1}{4}x^{\frac{1}{4}}\log x+\frac{2}{3}x^{\frac{2}{3}}\log x+\frac{3}{4}x^{\frac{3}{4}}\log x+(\alpha x+\beta)\log(\alpha x+\beta)\\
&\quad+\frac{2}{3}x^{\frac{2}{3}}\log x\Big)+\Big(\frac{(\alpha x+\beta)\log x}{x^{3/4}}+\frac{(\alpha x+\beta)\log x}{x^{1/4}}+\frac{(\alpha x+\beta)\log x}{x^{2/3}}\\
&\quad+\frac{\log(\alpha x+\beta)}{x^{3/4}}+\frac{(\alpha x+\beta)\log(\alpha x+\beta)}{\alpha x+\beta}+\frac{(\alpha x+\beta)\log x}{x^{2/3}}\Big)\\
&\ll\Big(x^{2/3}\log x\Big)+\Big(\alpha x^{1/4}\log x+\alpha x^{3/4}\log x+\alpha x^{1/3}\log x+\log x\Big)\\
&\ll\Big(x^{2/3}\log x\Big)+\Big(\alpha x^{3/4}\log x\Big)\\
&\ll x^{2/3+\varepsilon}+\alpha x^{3/4+\varepsilon};\qquad\text{(Taking } x^{\varepsilon}\ge\log x.\text{)}\\
&\ll\alpha x^{3/4+\varepsilon}.
\end{aligned}$$

(II) From (4.2), we have

$$\begin{aligned}
uvd^2t^2&\le(\alpha x+\beta)+(d^2u)^2\\
&\le(\alpha x+\beta)+(\alpha x+\beta)^2\\
&=(\alpha x+\beta)(\alpha x+\beta+1),
\end{aligned}$$

whence

$$\begin{aligned}
uv&\le(\alpha x+\beta)(\alpha x+\beta+1)/d^2t^2\\
&\le(\alpha x+\beta)(\alpha x+\beta+1)x^{-4/3}\\
&=\Big(\alpha^2x^2+(2\alpha\beta+\alpha)x+\beta^2+\beta\Big)x^{-4/3}\\
&=\alpha^2x^{2/3}+(2\alpha\beta+\alpha)x^{-1/3}+(\beta^2+\beta)x^{-4/3}\\
&\ll\alpha^2x^{2/3},
\end{aligned}$$

for any quadruple counted by $B_{\alpha,\beta}(x)$. Therefore, the total number of choices for u,v is

$$\#\Big\{(u,v)\Big|uv<\alpha^2x^{\frac{2}{3}}\Big\}=\sum_{n\le\alpha^2x^{\frac{2}{3}}}T(n)=\alpha^2x^{\frac{2}{3}}\log(\alpha^2x^{\frac{2}{3}})\ll\alpha^2x^{\frac{2}{3}+\varepsilon}.$$

For any such choice of u,v, the number of solutions in d,t of the equation $t^2v-d^2u=1$ is $O(x^{\varepsilon})$, see e.g. [27].

□

4.2 Main results

Theorem 4.3. Let $\alpha > 1$ be an irrational number and with bounded partial quotients, $\beta \in [0, \alpha)$. As $x \to \infty$, we have

$$Q_r(x;\alpha,\beta) = \frac{x}{\zeta(r)} + O(x^{(r+1)/2r}\log^3 x).$$

Proof. Let $x > 1$, we write

$$Q_r(x;\alpha,\beta) = \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \text{is } r\text{-free}}} 1 = \sum_{n\le x} \mu^r\Big(\lfloor \alpha n+\beta\rfloor\Big).$$

Since, [26, p. 290], $\mu^r(n) = \sum_{d^r|n}\mu(d)$, we get

$$\begin{aligned} Q_r(x;\alpha,\beta) &= \sum_{n\le x}\sum_{d^r|\lfloor \alpha n+\beta\rfloor} \mu(d) \\ &= \sum_{d\le(\alpha x+\beta)^{1/r}} \mu(d) \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0 (\bmod d^r)}} 1 \\ &= \sum_{d\le x^{1/(2r)}} \mu(d) \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0 (\bmod d^r)}} 1 + \sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}} \mu(d) \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0 (\bmod d^r)}} 1. \end{aligned}$$

In view of Lemma 2.17, we have

$$\begin{aligned} \sum_{d\le x^{1/(2r)}} \mu(d) \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0 (\bmod d^r)}} 1 &= \sum_{d\le x^{1/(2r)}} \mu(d)\Big(\frac{x}{d^r} + O(d^r\log^3 x)\Big) \\ &= \sum_{d\le x^{1/(2r)}} \frac{x\mu(d)}{d^r} + O\Big(\log^3 x \sum_{d\le x^{1/(2r)}} d^r\mu(d)\Big) \\ &= x\sum_{d\le x^{1/(2r)}} \frac{\mu(d)}{d^r} + O\Big(\log^3 x\Big|\sum_{d\le x^{1/(2r)}} d^r\Big|\Big) \\ &= \frac{x}{\zeta(r)} + O(x^{(r+1)/2r}\log x) + O(x^{(r+1)/2r}\log^3 x). \end{aligned}$$

We note that

$$\begin{aligned} \sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}} \mu(d) \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0 (\bmod d^r)}} 1 &\ll \sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}} \mu(d)\Big(\frac{x\log x}{d^r}\Big) \\ &\ll \log x\Big|\sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}} \frac{x}{d^r}\Big| \\ &\ll x(x^{\frac{1}{2r}})^{\frac{1}{r}-1}\log x \\ &\ll x^{(r+1)/2r}\log x. \end{aligned}$$

This proves Theorem 4.3. □

Example 4.1. Let $x = 20, \alpha = 1.4142, \beta = 0.4142$ and $r = 3$. Then we have

$$\lfloor \alpha n+\beta\rfloor = \{\mathbf{1}, \mathbf{3}, \mathbf{4}, \mathbf{6}, \mathbf{7}, 8, \mathbf{10}, \mathbf{11}, \mathbf{13}, \mathbf{14}, \mathbf{15}, \mathbf{17}, \mathbf{18}, \mathbf{20}, \mathbf{21}, \mathbf{23}, 24, \mathbf{25}, 27, \mathbf{28}\}.$$

So the number of 3-free integers in values of Beatty sequence $\lfloor \alpha n+\beta\rfloor_{n\le 20}$ is

$$Q_3(20;\alpha,\beta) = 17 \approx \frac{20}{\zeta(3)} = 16.6381.$$

In the case of $r = 2$, we obtain the improvement of (1.3) in following corollary.

Corollary 4.4. Let $\alpha > 1$ be an irrational number and with bounded partial quotients, $\beta \in [0, \alpha)$. As $x \to \infty$, we have

$$Q_2(x; \alpha, \beta) = \frac{x}{\zeta(2)} + O(x^{3/4} \log^3 x).$$

Example 4.2. Let $x = 20, \alpha = 1.4142, \beta = 0.4142$ and $r = 3$. Then we have

$$\lfloor \alpha n + \beta \rfloor_{n \le 20} = \{\mathbf{1}, \mathbf{3}, 4, \mathbf{6}, \mathbf{7}, 8, \mathbf{10}, \mathbf{11}, \mathbf{13}, \mathbf{14}, \mathbf{15}, \mathbf{17}, 18, 20, \mathbf{21}, \mathbf{23}, 24, 25, 27, 28\}.$$

So the number of square-free integers in values of Beatty sequence $\lfloor \alpha n + \beta \rfloor_{n \le 20}$ is

$$Q_2(20; \alpha, \beta) = 12 \approx \frac{20}{\zeta(2)} = 12.1585.$$

Theorem 4.5. For $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0, \alpha)$ and sufficiently small $\varepsilon > 0$, as $x \to \infty$ we have

$$\sum_{\substack{n \le x \\ \lfloor \alpha n + \beta \rfloor,\ \lfloor \alpha n + \beta \rfloor + 1 \text{ are square-free}}} 1 = \prod_p \Big(1 - \frac{2}{p^2}\Big) x + O\Big(\alpha x^{\frac{3}{4}+\varepsilon} \log^3 x\Big).$$

Proof. For $x \ge 1$, let

$$T_{\alpha,\beta}(x) := \sum_{\substack{n \le x \\ \lfloor \alpha n + \beta \rfloor,\ \lfloor \alpha n + \beta \rfloor + 1 \text{ are square-free}}} 1.$$

Since, [26, p. 290],

$$\sum_{d^2 \mid n} \mu(d) = \mu^2(n) = \begin{cases} 1 & \text{if } n \text{ is square-free} \\ 0 & \text{otherwise} \end{cases}$$

is the characteristic function of the set of square-free numbers. We get

$$\begin{aligned} T_{\alpha,\beta}(x) &= \sum_{n \le x} \sum_{d^2 \mid \lfloor \alpha n + \beta \rfloor} \mu(d) \sum_{t^2 \mid \lfloor \alpha n + \beta \rfloor + 1} \mu(t) \\ &= \sum_{\substack{d,\, t \le \sqrt{\alpha x + \beta} \\ \gcd(d,t) = 1}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor \alpha n + \beta \rfloor \equiv 0 \pmod{d^2} \\ \lfloor \alpha n + \beta \rfloor + 1 \equiv 0 \pmod{t^2}}} 1 \\ &= \Big(\sum_{\substack{d,\, t \le \sqrt{\alpha x + \beta} \\ \gcd(d,t) = 1 \\ dt \le x^{1/4}}} + \sum_{\substack{d,\, t \le \sqrt{\alpha x + \beta} \\ \gcd(d,t) = 1 \\ x^{1/4} < dt \le x^{2/3}}} + \sum_{\substack{d,\, t \le \sqrt{\alpha x + \beta} \\ \gcd(d,t) = 1 \\ dt > x^{2/3}}} \Big) \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor \alpha n + \beta \rfloor \equiv 0 \pmod{d^2} \\ \lfloor \alpha n + \beta \rfloor + 1 \equiv 0 \pmod{t^2}}} 1. \end{aligned}$$

In view of Lemma 4.2, we have

$$T_{\alpha,\beta}(x) = \sum_{\substack{d,\, t \le \sqrt{\alpha x + \beta} \\ \gcd(d,t) = 1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor n^c \rfloor \equiv 0 \pmod{d^2} \\ \lfloor n^c \rfloor + 1 \equiv 0 \pmod{t^2}}} 1 + O(\alpha x^{3/4+\varepsilon}) + O(\alpha^2 x^{2/3+\varepsilon}). \qquad (4.3)$$

By the Chinese remainder theorem, there is a positive integer λ, unique modulo d^2t^2, satisfying the congruence system $\lambda \equiv 0 \pmod{d^2}$ and $\lambda + 1 \equiv 0 \pmod{t^2}$. Thus,

$$\sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor n^c \rfloor \equiv 0 \pmod{d^2} \\ \lfloor n^c \rfloor + 1 \equiv 0 \pmod{t^2}}} 1 = \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor n^c \rfloor \equiv \alpha \pmod{d^2t^2}}} 1. \tag{4.4}$$

Next we use Lemma 2.17, so that the right-hand side of (4.4) becomes

$$\sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t)\Big(\frac{x}{d^2t^2} + O(d^2t^2 \log^3 x)\Big). \tag{4.5}$$

In view of Lemma 4.1, we have

$$x \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t)\frac{1}{d^2t^2} = \prod_p \Big(1 - \frac{2}{p^2}\Big)x + O\Big(\alpha x^{\frac{3}{4}+\varepsilon}\Big). \tag{4.6}$$

Using Lemma 2.33 to bound the error term in (4.5), we have

$$\Big| \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) d^2t^2 \log^3 x \Big| \ll \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} d^2t^2 \log^3 x \tag{4.7}$$

$$\ll \log^3 x \sum_{m \le x^{1/4}} m^2 d(m) \tag{4.8}$$

$$\ll x^{\frac{3}{4}+\varepsilon} \log^3 x. \tag{4.9}$$

Theorem 4.5 follows from (4.4)-(4.9). □

Example 4.3. Let $x = 20, \alpha = 1.4142, \beta = 0.4142$ and $r = 3$. Then we have

$$\lfloor \alpha n + \beta \rfloor_{n \le 20} = \{1, 3, 4, 6, 7, 8, 10, 11, 13, 14, 15, 17, 18, 20, 21, 23, 24, 25, 27, 28\};$$
$$\lfloor \alpha n + \beta \rfloor_{n \le 20} + 1 = \{2, 4, 5, 7, 8, 9, 11, 12, 14, 15, 16, 18, 19, 21, 22, 24, 25, 26, 28, 29\}.$$

In here, we see that the number of n for which the values of Beatty sequences $\lfloor \alpha n + \beta \rfloor_{n \le 20}$ and $\lfloor \alpha n + \beta \rfloor_{n \le 20} + 1$ are square-free integers, is

$$6 \approx \prod_p (1 - \frac{2}{p^2}) \cdot 20 = 6.58731.$$

Chapter 5

Conclusion

In this chapter, we will summary the results in this dissertation that consists of two parts, the first part is about the characterization of divided-differences polynomial over finite fields of characteristic two and the second one is about r-free integer on Beatty sequences.

In the first part, let $n \in \mathbb{N}$ with $n \geq 3$, and let $\mathbb{F}_{2^\ell}$ be a finite field of characteristic 2 with cardinality $2^\ell \geq n,\ \ell \in \mathbb{N},\ \ell \geq 2$. For definiteness, we represent the elements of $\mathbb{F}_{2^\ell}$ by

$$a_0 + a_1\alpha + \cdots + a_{\ell-1}\alpha^{\ell-1}, \qquad a_i \in \{0,1\} \qquad (0 \leq i \leq \ell-1),$$

where α is a root of an irreducible polynomial of degree ℓ over $GF(2) = \{0,1\}$. The divided difference on n distinct points of a function $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ may be defined inductively as follows:

$$f[x_1] = f(x_1), \qquad f[x_1, x_2] = \frac{f(x_1) + f(x_2)}{x_1 + x_2},$$

and for $n > 2$

$$f[x_1, \ldots, x_n] = \frac{f[x_1, \ldots, x_{n-1}] + f[x_2, \ldots, x_n]}{x_1 + x_n},$$

for n distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$. Then we get:

1. If $x_1, \ldots, x_{n+1}$ are distinct elements of a field $\mathbb{F}_{2^\ell}$ then for any $c_1, \ldots, c_{n+1}$ in $\mathbb{F}_{2^\ell}$ there exists a unique polynomial f over $\mathbb{F}_{2^\ell}$, of degree at most n, such that $f(x_j) = c_j$ for $j = 1, \ldots, n+1$.

2. Every function $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ is equal to a polynomial of degree at most $2^\ell - 1$.

3. It is easy to verify that

$$f[x_1, \ldots, x_n] = \frac{f(x_1)}{\prod_{\substack{i=1 \\ i\neq 1}}^{n}(x_1 + x_i)} + \frac{f(x_2)}{\prod_{\substack{i=1 \\ i\neq 2}}^{n}(x_2 + x_i)} + \cdots + \frac{f(x_n)}{\prod_{\substack{i=1 \\ i\neq n}}^{n}(x_n + x_i)},$$

   for distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$.

4. Let $\mathbb{F}_{2^\ell}$ be a finite field of characteristic 2 with $2^\ell \geq n$ and let $f : \mathbb{F}_{2^\ell} \to \mathbb{F}_{2^\ell}$ defined by function $f(x) = x^k \qquad (k = 0, 1, \ldots, 2^\ell - 1)$. Then

$$f[x_1, x_2, \ldots, x_n] = \sum_{i=1}^{n} \frac{f(x_i)}{\prod_{\substack{j=1 \\ j\neq i}}^{n}(x_i + x_j)} = \sum_{i=1}^{n} \frac{x_i^k}{\prod_{\substack{j=1 \\ j\neq i}}^{n}(x_i + x_j)}$$

for all distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$.

In particular

$$\sum_{i=1}^{n} \frac{x_i^k}{\prod_{\substack{j=1 \\ j\neq i}}^{n}(x_i + x_j)} = \begin{cases} 0 & \text{if } k \leq n-2 \\ 1 & \text{if } k = n-1 \\ x_1 + x_2 + \cdots + x_n & \text{if } k = n \\ \displaystyle\sum_{i_1+\cdots+i_n=k+1-n} x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} & \text{if } k > n. \end{cases}$$

5. It is known that if f is a polynomial of degree $n \geq 1$ with coefficients in $\mathbb{F}_{2^\ell}$,

$$f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$

then

$$f[x_1, \ldots, x_n] = a_n(x_1 + \cdots + x_n) + a_{n-1},$$

for distinct $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$.

6. If $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{F}_{2^\ell}[x]$ is a polynomial of degree n with $1 \leq n \leq 2^\ell - 1$, then for any n distinct elements $x_1, \ldots, x_n$ in $\mathbb{F}_{2^\ell}$, there is a linear polynomial $h_g(x) := a_n x + a_{n-1}$ such that

$$g[x_1, \ldots, x_n] = h_g(x_1 + \cdots + x_n).$$

7. **(Main result.)** Let n be an integer, $n \geq 3$, and let $\mathbb{F}_{2^\ell}$ be a finite field of characteristic 2 with $|\mathbb{F}_{2^\ell}| \geq n$. Let f and h be functions over $\mathbb{F}_{2^\ell}$. Then f and h satisfy

$$f[x_1, \ldots, x_n] = h(x_1 + \cdots + x_n) \tag{5.1}$$

whenever $x_1, \ldots, x_n$ are distinct elements of $\mathbb{F}_{2^\ell}$ if and only if f is equal to a polynomial of degree at most n over $\mathbb{F}_{2^\ell}$:

$$f(x) \equiv a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

So we have fulfilled our first objective that make the whole picture of the divided-differences characterization of polynomials problem complete.

In the second part, let r be a fixed integer ≥ 2. A positive integer n is called r-free if in the canonical representation of n into prime powers each exponent is $< r$. By convention, a 2-free integer is called square-free. Let $Q_r(x; \alpha, \beta)$ be the number of r-free integers of Beatty sequence $\lfloor \alpha n + \beta \rfloor, 1 \leq n \leq x$, for $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0, \alpha)$. Then we have:

1. For $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0, \alpha)$, and positive integer $d \geq 2, 0 \leq a < d$, we have

$$\sum_{\substack{n \leq x \\ \lfloor \alpha n + \beta \rfloor \equiv a \pmod d}} 1 = \frac{x}{d} + O(d \log^3 x) \quad \text{as } x \to \infty.$$

For growing difference d the result is non-trivial provided $d \ll \sqrt{x}\log^{-3/2-\varepsilon} x$, for $\varepsilon > 0$.

2. For each $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ such that for all $n \geq 1$ we have

$$d(n) \leq C_\varepsilon n^\varepsilon.$$

3. For a fixed real $y > 1$, we have

$$\sum_{\substack{d,\,t\\ \gcd(d,t)=1\\ dt\leq y}} \frac{\mu(d)\mu(t)}{d^2t^2} = \prod_{p \text{ prime}} \Big(1 - \frac{2}{p^2}\Big) + O(y^{-1+\varepsilon}).$$

4. Let $\alpha > 1$ be an irrational and with bounded partial quotients, $\beta \in [0, \alpha)$, let x be a positive real number.

   - If $A_{\alpha,\beta}(x)$ denotes the number of quadruples d, t, u, v of positive integers satisfying the conditions

$$t^2v - d^2u = 1, \qquad d^2u \leq \alpha x + \beta, \qquad x^{1/4} < dt \leq x^{2/3},$$

   then

$$A_{\alpha,\beta}(x) \ll \alpha x^{3/4+\varepsilon}.$$

   - If $B_{\alpha,\beta}(x)$ denotes the number of quadruples d, t, u, v satisfying the conditions

$$t^2v - d^2u = 1, \qquad d^2u \leq \alpha x + \beta, \qquad dt > x^{2/3},$$

   then

$$B_{\alpha,\beta}(x) \ll \alpha^2 x^{2/3+\varepsilon}.$$

5. Let $\alpha > 1$ be an irrational number and with bounded partial quotients, $\beta \in [0, \alpha)$. As $x \to \infty$, we have

$$Q_r(x; \alpha, \beta) = \frac{x}{\zeta(r)} + O(x^{(r+1)/2r}\log^3 x).$$

6. Let $\alpha > 1$ be an irrational number and with bounded partial quotients, $\beta \in [0, \alpha)$. As $x \to \infty$, we have

$$Q_2(x; \alpha, \beta) = \frac{x}{\zeta(2)} + O(x^{3/4}\log^3 x).$$

7. For $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0, \alpha)$ and sufficiently small $\varepsilon > 0$, as $x \to \infty$ we have

$$\sum_{\substack{n\leq x\\ \lfloor \alpha n+\beta\rfloor,\, \lfloor \alpha n+\beta\rfloor+1 \text{ are square-free}}} 1 = \prod_p \Big(1 - \frac{2}{p^2}\Big)x + O\Big(\alpha x^{\frac{3}{4}+\varepsilon}\log^3 x\Big).$$

References

[1] Milne-Thomson, L. M. 1981. **The Calculus of Finite Differences**. Chelsea, New York.

[2] Schwaiger, J. 1994. "On a characterization of polynomials by divided differences."*Aequationes Math*. 48: 317–323.

[3] Aczél, J. 1985. "A mean value property of the derivative of quadratic polynomials–without mean values and derivatives." *Math. Mag.* 58 (1): 42–45.

[4] Bailey, D. F. 1992. "A mean-valued property of cubic polynomials–without mean values." *Math. Mag.* 65: 123–124.

[5] Andersen, K. M. 1996. "A characterization of polynomials." *Math. Mag.* 69 (2): 137–142.

[6] Davies, R. O. and Rousseau, G. 1998. "A divided-difference characterization of polynomials over a general field." *Aequationes Math.* 55: 73–78.

[7] Güloğlu, A. M. and Nevans, C. W. 2008. "Sums of multiplicative functions over a Beatty sequence." *Bull. Austral. Math. Soc.* 78: 327 – 334.

[8] Abercrombie, A. G. Banks, W. D. and Shparlinski, I. E. 2009. "Arithmetic functions on Beatty sequences." *Acta Arith.* 136: 81 – 89.

[9] Goryashin, D. V. 2013. "Squarefree numbers in the sequence $\lfloor \alpha n \rfloor$." *Chebyshevskii Sb.* 14(3): 42–48.

[10] Carlitz, L. 1932. "On a problem in additive arithmetic II." *Q. J. Math., Oxf.* 3: 273–290.

[11] Heath-Brown, D. R. 1984. "The square sieve and consecutive square-free numbers." *Math. Ann.* 266: 251–259.

[12] Reuss, T. 2014. "Pairs of k-free numbers, consecutive square-full numbers." Available at https://arxiv.org/abs/1212.3150v2, 28 pages.

[13] Dimitrov, S. I. 2018. "Consecutive square-free numbers of a special form." arXiv: 1702.03983v3 [math.NT].

[14] Tangsupphathawat, P. Srichan, T. and Laohakosol, V. 2021. "Consecutive square–free numbers in Piatetski–Shapiro sequences."*Bull. Aust. Math. Soc.* 1-6. doi: 10.1017/S0004972721000666.

[15] Dimitrov, S. I. 2019. "On the distribution of consecutive square-free numbers of the form $\lfloor \alpha n \rfloor, \lfloor \alpha n \rfloor + 1$." *Proc. Jangjeon Math. Soc.* 22: 463-470.

[16] Begunts, A. V. and Goryashin D. V. 2020. “On the values of Beatty sequence in an arithmetic progression.” *Chebyshevskii Sb.* 21(1): 343–346.

[17] Dummit, D.S. and Foote, R.M. 1991. **Abstract algebra.** Englewood Cliffs, NJ: Prentice Hall, Vol. 1999.

[18] Wan, Z.X. 2003. **Lectures on finite fields and Galois rings**. World Scientific Publishing Company.

[19] Apostol, T. M. 1976. **Introduction to Analytic Number Theory**. Springer, New York.

[20] Redmond, D. 2020. **Number Theory: an introduction**. CRC Press.

[21] Friedberg, S.H. Insel, A.J. and Spen, L.E. 2003. **Linear algebra.** Pearson Education, 4^{th} edition.

[22] Carl De Boor, 1978. **A practical guide to splines**. Etats-Unis Mathematicien, Springer-Verlag, New York, volume 27.

[23] Sivaramakrishnan, A. 1998. **Classical Theory of Arithmetic Functions**. Marcel Dekker, New York and Basel.

[24] Honsberger, R. McAsey, M.J. Lange, L.H. Saul, M.E. Guy, R.K. Straffin, P.D. and Honsberger, R.A. 1970. **Ingenuity in mathematics.** Washington, DC: Mathematical Association of America, Vol. 23.

[25] Vander Waerden, B. L. 1973. **Algebra**. Ungar, New York, Volume 1.

[26] Shapiro, H. N. 1983. **Introduction to the Theory of Numbers**. Wiley, New York.

[27] Estermann, T. 1931. On the representation of a number as the sum of two numbers not divisible by k th powers.” *J. London Math. Soc.* 6: 37–40.

[28] Schramm, W. 2008. “The Fourier transform of functions of the greatest common divisor”. *Integers*. 8: #A50.

Appendix

Aequat. Math.

https://doi.org/10.1007/s00010-021-00860-4

Aequationes Mathematicae

A divided-difference characterization of polynomials over finite fields of characteristic two

Veasna Kim, Vichian Laohakosol, and Sukrawan Mavecha

Abstract. For a finite field $\mathbb{F}$ of characteristic 2, an integer $n \geq 3$, and for a function $f : \mathbb{F} \to \mathbb{F}$, if there is a function $h : \mathbb{F} \to \mathbb{F}$ such that the divided difference $f[x_1, \ldots, x_n]$ on any n distinct elements of $\mathbb{F}$ satisfies $f[x_1, \ldots, x_n] = h(x_1 + \cdots + x_n)$, then f is a polynomial of degree at most n over $\mathbb{F}$. This makes earlier work of Davies and Rousseau complete.

Mathematics Subject Classification. Primary 39B52, Secondary 11T06.

Keywords. Divided-difference, Finite field, Characteristic 2, Polynomial.

1. Introduction

For a field $\mathbb{F}$, the divided differences [5] on distinct points $x_1, x_2, x_3, \ldots$ in $\mathbb{F}$ of a function $f : \mathbb{F} \to \mathbb{F}$ are defined by

$$f[x_1] = f(x_1), \quad f[x_1, x_2] = \frac{f(x_1) - f(x_2)}{x_1 - x_2},$$

and inductively for $k > 2$ by

$$f[x_1, \ldots, x_k] = \frac{f[x_1, \ldots, x_{k-1}] - f[x_2, \ldots, x_k]}{x_1 - x_k},$$

keeping in mind that the divided differences are well-defined so long as there are enough distinct elements to do so. It is not difficult, using [6, Lemma 1], to see that if $f(x) := a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$ is a polynomial of degree $n \in \mathbb{N}$, then

$$f[x_1, \ldots, x_n] = a_n(x_1 + \cdots + x_n) + a_{n-1}, \tag{1.1}$$

i.e., the divided difference on n distinct points $x_1, \ldots, x_n$ of a polynomial of degree n can be expressed as a function in $x_1 + \cdots + x_n$. Then there arises

Published online: 09 January 2022

the question whether the converse of this result is true, i.e., if there exists a function $h : \mathbb{F} \to \mathbb{F}$ satisfying

$$f[x_1, \ldots, x_n] = h(x_1 + \cdots + x_n) \qquad \text{(f-h)}$$

for any n distinct points $x_1, \ldots, x_n$ in $\mathbb{F}$, is f necessarily a polynomial of degree at most n over $\mathbb{F}$? We refer to this question as the DDCP (divided-difference characterization of polynomials problem).

The case where $n = 2$ and $\mathbb{F}$ is a field of characteristic $\neq 2$ was solved by Acźel [1] in a more general form. Bailey [3] solved the DDCP in the case where f is a differentiable function, $\mathbb{F} = \mathbb{R}$, $n = 3$. In 1994, Schwaiger [6] solved the DDCP when $n \geq 2$, $\mathbb{F}$ is any field of characteristic $\neq 2$ with cardinality $\geq 8(n-2)+2$; at the end of his paper, he mentioned that the bound can be reduced to $6(n-2)+2$. Andersen [2] solved the DDCP when $\mathbb{F} = \mathbb{R}$ and $n \geq 2$. Finally, Davies and Rousseau [4] resolved the DDCP for $n \geq 2$ with $\mathbb{F}$ any field of characteristic $\neq 2$. In the appendix of their paper, Davies and Rousseau also proved that the DDCP holds for $\mathbb{F} = GF(2)$ and $GF(4)$, finite fields of order 2 and 4, respectively, but fails for fields of characteristic 2 with cardinality > 4. The case of $GF(2)$ is easily disposed of because every function is a linear polynomial (see e.g. Corollary 2.2 below). For the case $GF(4)$, since every function is a polynomial of degree ≤ 3, they show that no polynomial of degree 3 satisfies (f-h) for $n = 2$. As to the case where $\mathbb{F}$ is of characteristic 2 with cardinality > 4, they constructed a counter-example to the DDCP when $n = 2$.

The objective here is to show that the counter-example of Davies-Rousseau is exceptional in the sense that for all $n \geq 3$, the DDCP holds for any finite field of characteristic 2 with cardinality $\geq \max(n, 2^2)$. This makes the whole picture of the DDCP complete.

Our main result is:

Theorem 1.1. *Let $n, \ell \in \mathbb{N}$ with $n \geq 3$ and $\ell \geq 2$, and let $\mathbb{F}$ be a finite field of characteristic 2 with cardinality $2^\ell \geq n$. Suppose that functions $f, h : \mathbb{F} \to \mathbb{F}$ satisfy (f-h) for any distinct points $x_1, \ldots, x_n$ in $\mathbb{F}$. Then f is equal to a polynomial of degree at most n over $\mathbb{F}$.*

2. Lemmas

Throughout the rest of the paper, let $n \in \mathbb{N}$ with $n \geq 3$, and let $\mathbb{F}$ be a finite field of characteristic 2 with cardinality $2^\ell \geq n$, $\ell \in \mathbb{N}$, $\ell \geq 2$. For definiteness, we represent the elements of $\mathbb{F}$ by

$$a_0 + a_1\alpha + \cdots + a_{\ell-1}\alpha^{\ell-1}, \qquad a_i \in \{0, 1\} \quad (0 \leq i \leq \ell - 1), \qquad (2.1)$$

where α is a root of an irreducible polynomial of degree ℓ over $GF(2) = \{0, 1\}$.

We collect now some auxiliary results, the first of which is the well-known interpolation theorem.

Lemma 2.1. [7, Section 5.3, pp. 86-89] *If $x_1, \ldots, x_{m+1}$ are distinct elements in a field, then for any $c_1, \ldots, c_{m+1}$ in this field, there exists a unique polynomial f over the same field of degree at most m such that $f(x_j) = c_j$ for $j = 1, \ldots, m+1$.*

Lemma 2.1 immediately yields:

Corollary 2.2. *Every function $f : \mathbb{F} \to \mathbb{F}$ is equal to a polynomial of degree at most $2^\ell - 1$.*

The next lemma is a well-known identity connecting divided differences with Lagrange interpolation polynomials.

Lemma 2.3. [6, Lemma 1] *Let $x_1, \ldots, x_n$ be distinct elements in $\mathbb{F}$, and let $f : \mathbb{F} \to \mathbb{F}$. Then*

$$f[x_1, \ldots, x_n] = \sum_{j=1}^{n} \frac{f(x_j)}{\prod_{k \neq j}(x_j - x_k)}, \qquad (id)$$

where the product $\prod_{k \neq j}$ is taken over $k \in \{1, \ldots, n\}$ with $k \neq j$.

In particular, taking $f(X) = X^t \quad (t = 0, 1, \ldots, 2^\ell - 1)$, we have

$$X^t[x_1, x_2, \ldots, x_n] = \begin{cases} 0 & \text{if } t \leq n-2, \\ 1 & \text{if } t = n-1, \\ x_1 + x_2 + \cdots + x_n & \text{if } t = n. \end{cases}$$

Our last lemma is a formal statement of the remark following (1.1).

Lemma 2.4. *If $g(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{F}[x]$ is a polynomial of degree n with $1 \leq n \leq 2^\ell - 1$, then for any n distinct elements $x_1, \ldots, x_n$ in $\mathbb{F}$, the linear polynomial $h_g(x) := a_n x + a_{n-1}$ satifies*

$$g[x_1, \ldots, x_n] = h_g(x_1 + \cdots + x_n).$$

(The polynomial h_g is henceforth referred to as the n-th order divided-difference of g.)

3. Proof of Theorem 1.1

We fix n and ℓ and the field $\mathbb{F}$. The candidate polynomial is constructed explicitly by Lagrange interpolation using data at $n+1$ specific points, the data points including 0 and the first ℓ generators α^i when $n \geq \ell$, supplemented as necessary, and otherwise using 0 and the first $n-1$ generators when $3 \leq n \leq \ell - 1$ (the harder case) with a single supplement. The role of generators

is unsurprising, but the choice of the sum of the generators $1+\alpha+\cdots+\alpha^{n-2}$ as the supplementary point in the harder case is key to allowing certain sums to vanish thanks to the characteristic being 2.

For notational convenience, we write

$$\sum S = \sum_{s\in S} s \text{ for } S \subseteq \mathbb{F}$$

and denote by $[\mathbb{F}]^{=n}$ the set of all the distinct n-tuples in $\mathbb{F}$.

3.1. First case: n $\geq \ell$

Let $n = \ell + r$ $(\leq 2^\ell)$ with $0 \leq r \leq 2^\ell - \ell$. Choose $b_1, \ldots, b_r$ distinct from 0 and from the powers α^i for $i = 0, 1, \ldots, \ell-1$, omitting this step if $r = 0$. Put $B := \{b_1, \ldots, b_r\}$ (unless $r = 0$ in which case $B = \emptyset$), $G := \{\alpha^i : i = 0, 1, \ldots, \ell-1\}$ and $S = G \cup B$, which has n members. Define a polynomial f_1 of degree n by setting

$$f_1(s) = f(s) \text{ for } s \in S, \qquad f_1(0) = f(0),$$

whose existence is guaranteed by Lemma 2.1.

Let h_1 be the n-th order divided difference of f_1. Take

$$F_1 := f - f_1 \text{ and } H_1 := h - h_1.$$

Then

$$F_1[X] = H_1(x_1 + \cdots + x_n) = H_1\left(\sum X\right) \qquad (X := \{x_1, \ldots, x_n\} \in [\mathbb{F}]^{=n}),$$
$$F_1(s) = 0 \qquad (s \in S \cup \{0\}). \tag{3.1}$$

We show that this last equation extends to the span of G and hence to all of $\mathbb{F}$ in this case.

Proposition 3.1. *Suppose $\ell \leq n \leq 2^\ell$. Then for all $1 \leq k \leq \ell - 1$ and $0 \leq i_1 < \cdots < i_k \leq \ell - 1$, we have*

$$F_1(\alpha^{i_1} + \cdots + \alpha^{i_k}) = 0,$$

and so $f = f_1$.

Proof By induction. The case $k = 1$ is immediate from (3.1). Suppose the result is true for $k-1$ summands. Consider the sum $\alpha^{i_1}+\cdots+\alpha^{i_k}$. As $F_1(b) = 0$ for $b \in B$, without loss of generality, we may assume that $\alpha^{i_1} + \cdots + \alpha^{i_k} \notin B$. Suppose first that $\alpha^{i_2} + \cdots + \alpha^{i_k} \notin B$. Then

$$X := S \setminus \{\alpha^{i_1}, \alpha^{i_2}\} \cup \{\alpha^{i_1} + \cdots + \alpha^{i_k}, \alpha^{i_2} + \cdots + \alpha^{i_k}\}$$

has cardinality n. Since the characteristic is 2, we have

$$(\alpha^{i_1} + \cdots + \alpha^{i_k}) + (\alpha^{i_2} + \cdots + \alpha^{i_k}) = \alpha^{i_1},$$

from which it follows that

$$F_1[X] = H_1\left(\sum X\right) = H_1\left(0 + \sum S \setminus \{\alpha^{i_2}\}\right)$$
$$= F_1[\{0\} \cup S \setminus \{\alpha^{i_2}\}] = 0,$$

by the interpolation formula (id), since $F_1(s) = 0$ for $s \in S \cup \{0\}$. But by Lagrange's interpolation Lemma 2.3, for some non-zero λ, μ, λ_s, we have

$$F_1[X] = \lambda F_1(\alpha^{i_1} + \cdots + \alpha^{i_k}) + \mu F_1(\alpha^{i_2} + \cdots + \alpha^{i_k}) + \sum_{S\setminus\{\alpha^{i_1},\alpha^{i_2}\}} \lambda_s F_1(s)$$
$$= \lambda F_1(\alpha^{i_1} + \cdots + \alpha^{i_k}), \tag{3.2}$$

since $F_1(s) = 0$ for $s \in S$ and by the inductive hypothesis $F_1(\alpha^{i_2} + \cdots + \alpha^{i_k}) = 0$. So by (3.2), $F_1(\alpha^{i_1} + \cdots + \alpha^{i_k}) = 0$, in this case.

Now suppose that $b := \alpha^{i_2} + \cdots + \alpha^{i_k} \in B$. Then

$$\alpha^{i_1} + \cdots + \alpha^{i_k} = \alpha^{i_1} + b.$$

Take

$$X := S \setminus \{\alpha^{i_1}\} \cup \{\alpha^{i_1} + \cdots + \alpha^{i_k}\} = S \setminus \{\alpha^{i_1}\} \cup \{\alpha^{i_1} + b\}.$$

Then X has cardinality n, since $\alpha^{i_1} + \cdots + \alpha^{i_k} \notin B$. Then again since the characteristic is 2, we have

$$\sum X = \sum S \setminus \{b\},$$

and so

$$F_1[X] = H_1\left(\sum X\right) = H_1\left(0 + \sum S \setminus \{b\}\right) = F_1[\{0\} \cup S \setminus \{b\}] = 0,$$

again by the interpolation formula of Lemma 2.3, since $F_1(s) = 0$ for $s \in S \cup \{0\}$. This completes the induction. □

3.2. Second case: $3 \le n \le \ell - 1$

An argument similar to that of Proposition 3.1 can be repeated by taking $G := \{\alpha^i : i = 0, 1, \ldots, n-2\}$ and $S = G \cup B$ with $B := \{b\}$ where $b := 1 + \alpha + \cdots + \alpha^{n-2}$, so that S has n members. With these choices, define a polynomial f_2 of degree n by setting

$$f_2(s) = f(s) \text{ for } s \in S, \qquad f_2(0) = f(0).$$

Let h_2 be the n-th order divided-difference of the polynomial f_2. As before take

$$F_2 := f - f_2 \text{ and } H_2 := h - h_2.$$

Then again

$$F_2[X] = H_2\left(\sum X\right) \qquad (X \in [\mathbb{F}]^{=n}),$$
$$F_2(s) = 0 \qquad (s \in S \cup \{0\}).$$

This only yields $F_2 = 0$ on the the span of G. Note that $\sum S = 0$.

Proposition 3.2. *Suppose* $3 \leq n \leq \ell - 1$. *Then for all* $1 \leq k \leq n-2$ *and* $0 \leq i_1 < \cdots < i_k \leq n-2$, *we have*

$$F_2(\alpha^{i_1} + \cdots + \alpha^{i_k}) = 0.$$

Proof By induction. As before, the case $k = 1$ is clear. Consider $\alpha^{i_1} + \cdots + \alpha^{i_k}$ with $k \geq 2$. The set

$$X := S \setminus \{\alpha^{i_1}, \alpha^{i_2}\} \cup \{\alpha^{i_1} + \cdots + \alpha^{i_k}, \alpha^{i_2} + \cdots + \alpha^{i_k}\}$$

has cardinality n. As before

$$(\alpha^{i_1} + \cdots + \alpha^{i_k}) + (\alpha^{i_2} + \cdots + \alpha^{i_k}) = \alpha^{i_1},$$

but now $\sum S = 0$ and so

$$\sum X = \sum S \setminus \{\alpha^{i_2}\} = \alpha^{i_2},$$

from which it follows that

$$F_2[X] = H_2(\alpha^{i_2}) = 0,$$

provided $i_2 \leq n-2$. Again for non-zero coefficients λ, μ, λ_s by Lagrange's interpolation Lemma 2.3, we have

$$F_2[X] = \lambda F_2(\alpha^{i_1} + \cdots + \alpha^{i_k}) + \mu F_2(\alpha^{i_2} + \cdots + \alpha^{i_k}) + \sum_{s \in S \setminus \{\alpha^{i_1}, \alpha^{i_2}\}} \lambda_s F_2(s),$$

and so again by induction $F_2(\alpha^{i_1} + \cdots + \alpha^{i_k}) = 0$. □

As a first step in extending Proposition 3.2 to all of $\mathbb{F}$ we show the following:

Proposition 3.3. *We have* $F_2(\alpha^j) = 0$ *for* $n - 1 \leq j \leq \ell - 1$.

Proof. For $n \geq 4$, $H_2(\alpha^2) = 0$, by Proposition 3.2. In this case take

$$X := \{\alpha^j, \alpha^j + 1 + \alpha, 0\} \cup S \setminus \{1, \alpha, \alpha^2\},$$

which has cardinality n, and so

$$0 = H_2(\alpha^2) = F_2[X] = \lambda F_2[\alpha^j] + \mu F_2[\alpha^j + 1 + \alpha].$$

Here, by the formula (id), $\lambda = 1/(\alpha^j A), \mu = 1/((\alpha^i + 1 + \alpha)B)$ with

$$A = (1+\alpha)(\alpha^j + \alpha^3)\cdots(\alpha^j + \alpha^{n-2})(\alpha^j + b) \neq 0,$$
$$B = (1+\alpha)(\alpha^j + 1 + \alpha + \alpha^3)\cdots(\alpha^j + 1 + \alpha + \alpha^{n-2})(\alpha^j + 1 + \alpha + b) \neq 0,$$

the other terms vanishing as before. The set

$$X' := \{\alpha^j, \alpha^j + 1 + \alpha\} \cup S \setminus \{1, \alpha\}$$

has cardinality n, so a second equation connects $F_2[\alpha^j]$ and $F_2[\alpha^j + 1 + \alpha]$:

$$0 = H_2(0) = F_2[X'] = \lambda' F_2[\alpha^j] + \mu F_2[\alpha^j + 1 + \alpha]$$

where $\lambda' = 1/((\alpha^j + \alpha^2)A), \mu' = 1/((\alpha^j + 1 + \alpha + \alpha^2)B)$. It is readily verified that $\lambda\mu' - \lambda'\mu \neq 0$, since $\alpha^2 + \alpha^3 \neq 0$, and so $F_2[\alpha^j] = F_2[\alpha^j + 1 + \alpha] = 0$.

When $n = 3$, $S = \{1, \alpha, b\}$ and $b = 1 + \alpha$. Take

$$X := \{\alpha^j, \alpha^j + b, 0\};$$

now $H_2(b) = 0$ and $F_2(0) = 0$, so as before

$$0 = H_2(b) = F_2[X] = \lambda F_2[\alpha^j] + \mu F_2[\alpha^j + b],$$

where $\lambda = 1/(\alpha^j b), \mu = 1/((\alpha^j + b)b)$. Take

$$X' = \{\alpha^j, \alpha^j + b, b\},$$

so again

$$0 = H_2(0) = F_2[X'] = \lambda' F_2[\alpha^j] + \mu' F_2[\alpha^j + b]$$

where $\lambda' = 1/(b(\alpha^j + b)), \mu' = 1/(\alpha^j b)$. It is easily verified that $\lambda\mu' - \lambda'\mu \neq 0$ and so $F_2[\alpha^j] = F_2[\alpha^j + b] = 0$. □

Proposition 3.4. *For $n - 2 \leq j \leq \ell - 1$ and any $a_i \in \{0, 1\}$ for $0 \leq i \leq j - 1$, we have*

$$F_2(\alpha^j + a_{j-1}\alpha^{j-1} + \cdots + a_0) = 0.$$

Proof By induction. Write $y_j := \alpha^j + a_{j-1}\alpha^{j-1} + \cdots + a_0$. The result holds for $j = n - 2$ by Proposition 3.2. We make the strong inductive hypothesis that for $n - 2 \leq j \leq k - 1$, we have $F_2(y_j) = H_2(y_j) = 0$. We put $T_j := a_{j-1}\alpha^{j-1} + \cdots + a_0$.

We are to show that $F_2(y_k) = H_2(y_k) = 0$. As $a_k \in \{0, 1\}$, the strong inductive hypothesis gives $H_2(T_k) = 0$. Assume that $n > 3$ and suppose first that $T_k \notin S \cup \{0\}$. Here take

$$X := S \setminus \{1, \alpha, \alpha^2\} \cup \{y_k, \alpha^k, 1 + \alpha + \alpha^2\},$$

which has cardinality n. Since $y_k + \alpha^k = T_k$, we have

$$0 = H_2(T_k) = F_2[X] = \lambda F_2(y_k),$$

the latter since $F_2(\alpha^k) = 0$ (Proposition 3.3) and since $F_2(s) = 0$ for $s \in S$, whereas $F_2(1 + \alpha + \alpha^2) = 0$, by construction.

Now suppose that $T_k \in S \cup \{0\}$. Then as $F_2(s) = H_2(s) = 0$ for $s \in S \cup \{0\}$, again $F_2[X] = 0$, and so by the interpolation Lemma 2.3, $F_2(y_k) = 0$, since $F_2(y_{k-1}) = 0$.

If $n = 3$, take $X := \{y_k, \alpha^k, 0\}$, and again

$$0 = H_2(T_k) = F_2[X] = \lambda F_2(y_k).$$

Finally, since

$$X' := S \setminus \{1, \alpha, \alpha^2\} \cup \{y_k, 0, 1 + \alpha + \alpha^2\}$$

has cardinality n and $F_2[X'] = 0$, by the interpolation Lemma 2.3, we have

$$0 = F_2[X'] = H_2\left(\sum X'\right) = H_2(y_k).$$

This completes the induction up to $j = \ell - 1$. □

Taking Propositions 3.2 and 3.4 together, it follows that $F_2(x) = 0$ for all $x \in \mathbb{F}$.

Final remark. The proof given above also works when $n = 2$ and $\mathbb{F}$ has cardinality ≤ 4 (considering the case $n \geq \ell$) which offers another proof of a Davies-Rousseau type result.

Acknowledgements

The first author is supported by a scholarship from King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand. The authors thank the first referee for his careful reading and suggestions which substantially improve the proof in Section 3, and thank the second referee for language corrections.

References

[1] Aczél, J.: A mean value property of the derivative of quadratic polynomials-without mean values and derivatives. Math. Mag. **58**(1), 42–45 (1985)
[2] Andersen, K.M.: A characterization of polynomials. Math. Mag. **69**(2), 137–142 (1996)
[3] Bailey, D.F.: A mean-valued property of cubic polynomials-without mean values. Math. Mag. **65**, 123–124 (1992)
[4] Davies, R.O., Rousseau, G.: A divided-difference characterization of polynomials over a general field. Aequationes Math. **55**, 73–78 (1998)
[5] Milne-Thomson, L.M.: The calculus of finite differences. Chelsea, New York (1981)
[6] Schwaiger, J.: On a characterization of polynomials by divided differences. Aequationes Math. **48**, 317–323 (1994)
[7] van der Waerden, B.L.: Algebra, vol. 1. Ungar, New York (1973)

Veasna Kim and Sukrawan Mavecha
Department of Mathematics, Faculty of Science
King Mongkut's Institute of Technology Ladkrabang
Bangkok 10520
Thailand
e-mail: kim.veasna909@gmail.com

A divided-difference characterization of polynomials

Sukrawan Mavecha
e-mail: sukrawan.ta@kmitl.ac.th

Vichian Laohakosol
Department of Mathematics, Faculty of Science
Kasetsart University
Bangkok 10900
Thailand
e-mail: fscivil@ku.ac.th

Received: November 2, 2020
Revised: November 14, 2021
Accepted: November 18, 2021

Bol. Soc. Mat. Mex. (2022)28:28
https://doi.org/10.1007/s40590-022-00422-x

Sociedad Matemática Mexicana

ORIGINAL ARTICLE

On *r*-free integers in Beatty sequences

Veasna Kim[1] · **Teerapat Srichan**[2] · **Sukrawan Mavecha**[1]

Received: 16 October 2021 / Accepted: 14 February 2022

Abstract
Let $r \geq 2$ be a fixed integer. A positive integer n is called r-free if in the canonical representation of n into prime powers each exponent is $< r$. The integer 1 is considered to be r-free. In this paper, we consider $Q_r(x; \alpha, \beta)$, which is the number of r-free integers of Beatty sequence $\lfloor \alpha n + \beta \rfloor$, $1 \leq n \leq x$, for $\alpha > 1$ irrational and with bounded partial quotients, $\beta \in [0, \alpha)$. We prove that, as $x \to \infty$

$$Q_r(x; \alpha, \beta) = \frac{x}{\zeta(r)} + O(x^{(r+1)/2r} \log^3 x),$$

which improves Victorovich's result in the case of square-free integers. Moreover, we also prove there exist infinitely many consecutive square-free numbers of the forms $\lfloor \alpha n + \beta \rfloor$, $\lfloor \alpha n + \beta \rfloor + 1$, which improves Dimitrov's result in 2019.

Keywords Beatty sequence · r-free number · Square-free number

Mathematics Subject Classification 11N37 · 11N64

This work was financially supported by Office of the Permanent Secretary, Ministry of Higher Education, Science, Research and Innovation, Grant no. RGNS 63-40. The first author is supported by KMITL Doctoral Scholarship.

✉ Teerapat Srichan
fscitrp@ku.ac.th

Veasna Kim
62605009@kmitl.ac.th

Sukrawan Mavecha
sukrawan.ta@kmitl.ac.th

[1] Department of Mathematics, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand

[2] Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand

Published online: 15 March 2022

Birkhäuser

1 Introduction and results

Let r be a fixed integer ≥ 2. A positive integer n is called r-free if in the canonical representation of n into prime powers each exponent is $<r$. By convention, a 2-free integer is called square-free. The problem for the existence of square-free numbers in the Beatty sequences arose in 2008. Gűloğlu and Nevans [8] proved that

$$\sum_{\substack{n\leq x\\ \lfloor \alpha n\rfloor \text{is square}-\text{free}}} 1=\frac{x}{\zeta(2)}+O\Big(\frac{x\log\log x}{\log x}\Big),$$

where $\alpha>1$ is irrational number of finite type. In 2009 Abercrombie and Banks [1] showed that

$$\sum_{\substack{n\leq x\\ \lfloor \alpha n\rfloor \text{is square}-\text{free}}} 1=\frac{x}{\zeta(2)}+O\Big(x^{2/3}\log N\Big),$$

for almost all $\alpha>1$. Recently in 2013 Victorovich [9] showed that

$$\sum_{\substack{n\leq x\\ \lfloor \alpha n\rfloor \text{is square}-\text{free}}} 1=\frac{x}{\zeta(2)}+O\Big(Ax^{5/6}\log^5 N\Big), \tag{1}$$

where $\alpha>1$ is irrational number with bounded partial quotient or irrational algebraic number. Here $A=\max\{\tau(m),1\leq m\leq x^2\}$.

In this paper, we give other asymptotic formula for this problem by using the result on the number of values of Beatty sequence $\lfloor \alpha n+\beta\rfloor$, in an arithmetic progression in [3]. We obtain the following results.

Theorem 1 *Let $\alpha>1$ be an irrational number and with bounded partial quotients, $\beta\in[0;\alpha)$. As $x\to\infty$, we have*

$$Q_r(x;\alpha,\beta)=\frac{x}{\zeta(r)}+O(x^{(r+1)/2r}\log^3 x).$$

In the case of $r=2$, we obtain the improvement of (1) in following corollary.

Corollary 1 *Let $\alpha>1$ be an irrational number and with bounded partial quotients, $\beta\in[0;\alpha)$. As $x\to\infty$, we have*

$$Q_2(x;\alpha,\beta)=\frac{x}{\zeta(2)}+O(x^{3/4}\log^3 x).$$

The consecutive square-free numbers is an attractive problem. The distribution of the consecutive square-free is studied by many authors (see [4, 10, 11]). In particular, the existence of infinitely many consecutive square-free numbers of the form $\lfloor f(n)\rfloor$, $\lfloor f(n)\rfloor+1$ is also studied. In 2018 Dimitrov [5] proved that for any fixed $1<c<7/6$, there exist infinitely many consecutive square-free integers of the form $\lfloor n^c\rfloor$, $\lfloor n^c\rfloor+1$ by showing that

$$\sum_{\substack{x/2<n\le x\\ \lfloor n^c\rfloor,\ \lfloor n^c\rfloor+1\ \text{are square-free}}} 1=\frac{1}{2}\prod_p\Big(1-\frac{2}{p^2}\Big)x+O\Big(x^{\frac{6c+1}{8}+\varepsilon}\Big),\qquad \text{for } 1<c<\frac{7}{6}. \tag{2}$$

Very recently, Tangsupphathawat, Srichan and Laohakosol [13] improved the range of c and the error term in Dimitrov's work in (2) and showed that, for $1<c<3/2$, and sufficiently small $\varepsilon>0$, we have

$$\sum_{\substack{n\le x\\ \lfloor n^c\rfloor,\ \lfloor n^c\rfloor+1\ \text{are square-free}}} 1=\prod_p\Big(1-\frac{2}{p^2}\Big)x+O\Big(x^{\frac{2c+1}{4}+\varepsilon}\Big)\qquad (x\to\infty).$$

On the other hand in [6] Dimitrov used the method of Victorovich [9] to showed that for $\alpha>1$ be irrational number with bounded partial quotient or irrational algebraic number,

$$\sum_{\substack{n\le x\\ \lfloor \alpha n\rfloor,\ \lfloor \alpha n\rfloor+1\ \text{are square-free}}} 1=\prod_p\Big(1-\frac{2}{p^2}\Big)x+O\Big(x^{\frac{5}{6}+\varepsilon}\Big). \tag{3}$$

To improve (3), we use the similar idea as in [13] and we obtain the following theorem.

Theorem 2 *For $\alpha>1$ irrational and with bounded partial quotients, $\beta\in[0;\alpha)$ and sufficiently small $\varepsilon>0$, as $x\to\infty$ we have*

$$\sum_{\substack{n\le x\\ \lfloor \alpha n+\beta\rfloor,\ \lfloor \alpha n+\beta\rfloor+1\ \text{are square-free}}} 1=\prod_p\Big(1-\frac{2}{p^2}\Big)x+O\Big(\alpha x^{\frac{3}{4}+\varepsilon}\log^3 x\Big).$$

2 Lemmas

The following lemma is the result of Vladimirovich and Victorovich [3], which is the main ingradient of our proof.

Lemma 1 *For $\alpha>1$ irrational and with bounded partial quotients, $\beta\in[0;\alpha)$, and positive integer $d\ge 2, 0\le a<d$, we have*

$$\sum_{\substack{n \le x \\ \lfloor \alpha n + \beta \rfloor \equiv a (\mathrm{mod}\, d)}} 1 = \frac{x}{d} + O(d \log^3 x) \quad \text{as } x \to \infty.$$

For growing difference d the result is non-trivial provided $d \ll \sqrt{x} \log^{-3/2-\varepsilon} x$, for $\varepsilon > 0$.

We will use the following upper bound.

Lemma 2 ([12, *Exercise* 9, *p.* 50]) *For each* $\varepsilon > 0$, *there exists a constant* $C_\varepsilon > 0$ *such that for all* $n \ge 1$ *we have*

$$d(n) \le C_\varepsilon n^\varepsilon.$$

Lemma 3 *For a fixed real* $y > 1$, *we have*

$$\sum_{\substack{d,\, t \\ \gcd(d,t) = 1 \\ dt \le y}} \frac{\mu(d)\mu(t)}{d^2 t^2} = \prod_{p \text{ prime}} \left(1 - \frac{2}{p^2}\right) + O(y^{-1+\varepsilon}).$$

Proof We have

$$\sum_{\substack{d,\, t \\ \gcd(d,t) = 1 \\ dt \le y}} \frac{\mu(d)\mu(t)}{d^2 t^2} = \sum_{\substack{d,\, t \\ \gcd(d,t) = 1}} \frac{\mu(d)\mu(t)}{d^2 t^2} - \sum_{\substack{dt > y \\ \gcd(d,t) = 1}} \frac{\mu(d)\mu(t)}{d^2 t^2}$$

$$= \sum_{\substack{d,\, t \\ \gcd(d,t) = 1}} \frac{\mu(d)\mu(t)}{d^2 t^2} + O\left(\left| \sum_{m > y} \frac{d(m)}{m^2} \right| \right).$$

In view of Lemma 2, the error term can be replaced by

$$O\left(\left| \sum_{m > y} m^{-2+\varepsilon} \right| \right) = O\left(y^{-1+\varepsilon} \right),$$

and so, using also [2, Theorem 11.7, p. 231], we get

$$\sum_{\substack{d,\,t\\ \gcd(d,t)=1\\ dt\le y}} \frac{\mu(d)\mu(t)}{d^2t^2} = \sum_{m=1}^{\infty}\frac{\mu(m)d(m)}{m^2} + O\Big(y^{-1+\varepsilon}\Big) = \prod_p\Big(1-\frac{2}{p^2}\Big) + O\Big(y^{-1+\varepsilon}\Big).$$

□

Lemma 4 *Let $\alpha > 1$ be an irrational and with bounded partial quotients, $\beta \in [0;\alpha)$, let x be a positive real number.*

(I) If $A_{\alpha,\beta}(x)$ denotes the number of quadruples d, t, u, v of positive integers satisfying the conditions

$$t^2v - d^2u = 1, \qquad d^2u \le \alpha x + \beta, \qquad x^{1/4} < dt \le x^{2/3}, \tag{4}$$

then

$$A_{\alpha,\beta}(x) \ll \alpha x^{3/4+\varepsilon}.$$

(II) If $B_{\alpha,\beta}(x)$ denotes the number of quadruples d, t, u, v satisfying the conditions

$$t^2v - d^2u = 1, \qquad d^2u \le \alpha x + \beta, \qquad dt > x^{2/3}, \tag{5}$$

then

$$B_{\alpha,\beta}(x) \ll \alpha^2 x^{2/3+\varepsilon}.$$

Proof (I) For any fixed choice of positive integers d and t satisfying (4), the condition $d^2u \equiv -1 \pmod{t^2}$ fixes the value of u modulo t^2. Thus, by conditions in (4), the total number of possibilities for u is $O(1 + (\alpha x + \beta)/d^2t^2)$. By (4), the value of v is fixed, for any given d, t, u. Then

$$A_{\alpha,\beta}(x) \ll \sum_{x^{1/4} < dt \le x^{2/3}} (1 + (\alpha x + \beta)/d^2t^2) \ll x^{2/3+\varepsilon} + \alpha x^{3/4+\varepsilon} \ll \alpha x^{3/4+\varepsilon}.$$

(II) From (5), we have $uvd^2t^2 \le (\alpha x + \beta)(\alpha x + \beta + 1)$, whence $uv \le (\alpha x + \beta)(\alpha x + \beta + 1)x^{-4/3}$ for any quadruple counted by $B_{\alpha,\beta}(x)$. The total number of choices for u, v is therefore bounded by $O(\alpha^2x^{2/3+\varepsilon})$, by a divisor argument. For any such choice of u, v, the number of solutions in d, t of the equation $t^2v - d^2u = 1$ is $O(x^{\varepsilon})$, see e.g. [7]. □

3 Proofs

Proof of Theorem 1 Let $x > 1$, we write

$$Q_r(x;\alpha,\beta) = \sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \text{is r}-\text{free}}} 1 = \sum_{n\le x} \mu^r\Big(\lfloor \alpha n+\beta\rfloor\Big).$$

Since, [12, p. 290], $\mu^r(n) = \sum_{d^r|n}\mu(d)$, we get

$$Q_r(x;\alpha,\beta) = \sum_{n\le x}\sum_{d^r|\lfloor \alpha n+\beta\rfloor}\mu(d)$$

$$= \sum_{d\le(\alpha x+\beta)^{1/r}}\mu(d)\sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0(\bmod d^r)}} 1$$

$$= \sum_{d\le x^{1/(2r)}}\mu(d)\sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0(\bmod d^r)}} 1$$

$$+ \sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}}\mu(d)\sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0(\bmod d^r)}} 1.$$

In view of Lemma 1, we have

$$\sum_{d\le x^{1/(2r)}}\mu(d)\sum_{\substack{n\le x \\ \lfloor \alpha n+\beta\rfloor \equiv 0(\bmod d^r)}} 1 = \sum_{d\le x^{1/(2r)}}\mu(d)\Big(\frac{x}{d^r}+O(d^r\log^3 x)\Big)$$

$$= x\sum_{d\le x^{1/(2r)}}\frac{\mu(d)}{d^r}+O\Big(\log^3 x\Big|\sum_{d\le x^{1/(2r)}} d^r\Big|\Big)$$

$$= \frac{x}{\zeta(r)}+O(x^{(r+1)/2r}\log x)+O(x^{(r+1)/2r}\log^3 x).$$

We note that

$$\sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}}\mu(d)\sum_{\substack{n\le x\\ \lfloor\alpha n+\beta\rfloor\equiv 0(\bmod d^r)}}1 \ll \log x\left|\sum_{x^{1/(2r)}<d\le(\alpha x+\beta)^{1/r}}\frac{x}{d^r}\right| \ll x^{(r+1)/2r}\log x.$$

This proves Theorem 1. □

Proof of Theorem 2 For $x\ge 1$, let

$$T_{\alpha,\beta}(x) := \sum_{\substack{n\le x\\ \lfloor\alpha n+\beta\rfloor,\ \lfloor\alpha n+\beta\rfloor+1\ \text{are square-free}}}1.$$

Since, [12, p. 290],

$$\sum_{d^2|n}\mu(d)=\mu^2(n)=\begin{cases}1 & \text{if } n \text{ is square-ree}\\ 0 & \text{otherwise}\end{cases}$$

is the characteristic function of the set of square-free numbers, we get

$$T_{\alpha,\beta}(x)=\sum_{n\le x}\sum_{d^2|\lfloor\alpha n+\beta\rfloor}\mu(d)\sum_{t^2|\lfloor\alpha n+\beta\rfloor+1}\mu(t)$$

$$=\sum_{\substack{d,\,t\le\sqrt{\alpha x+\beta}\\ \gcd(d,t)=1}}\mu(d)\mu(t)\sum_{\substack{n\le x\\ \lfloor\alpha n+\beta\rfloor\equiv 0(\bmod d^2)\\ \lfloor\alpha n+\beta\rfloor+1\equiv 0(\bmod t^2)}}1$$

$$=\Bigg(\sum_{\substack{d,\,t\le\sqrt{\alpha x+\beta}\\ \gcd(d,t)=1\\ dt\le x^{1/4}}}+\sum_{\substack{d,\,t\le\sqrt{\alpha x+\beta}\\ \gcd(d,t)=1\\ x^{1/4}<dt\le x^{2/3}}}\Bigg)\mu(d)\mu(t)\sum_{\substack{n\le x\\ \lfloor\alpha n+\beta\rfloor\equiv 0(\bmod d^2)\\ \lfloor\alpha n+\beta\rfloor+1\equiv 0(\bmod t^2)}}1.$$

$$+\sum_{\substack{d,\,t\le\sqrt{\alpha x+\beta}\\ \gcd(d,t)=1\\ dt>x^{2/3}}}\mu(d)\mu(t)\sum_{\substack{n\le x\\ \lfloor\alpha n+\beta\rfloor\equiv 0(\bmod d^2)\\ \lfloor\alpha n+\beta\rfloor+1\equiv 0(\bmod t^2)}}1.$$

In view of Lemma 4, we have

$$T_{\alpha,\beta}(x) = \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor n^c \rfloor \equiv 0 (\mathrm{mod}\ d^2) \\ \lfloor n^c \rfloor + 1 \equiv 0 (\mathrm{mod}\ t^2)}} 1 + O(\alpha x^{3/4+\varepsilon}) + O(\alpha^2 x^{2/3+\varepsilon}). \tag{6}$$

By the Chinese remainder theorem, there is a positive integer λ, unique modulo d^2t^2, satisfying the congruence system $\lambda \equiv 0 (\mathrm{mod}\ d^2)$ and $\lambda + 1 \equiv 0 (\mathrm{mod}\ t^2)$. Thus,

$$\begin{aligned} &\sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor n^c \rfloor \equiv 0 (\mathrm{mod}\ d^2) \\ \lfloor n^c \rfloor + 1 \equiv 0 (\mathrm{mod}\ t^2)}} 1 \\ &= \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t) \sum_{\substack{n \le x \\ \lfloor n^c \rfloor \equiv \alpha (\mathrm{mod}\, d^2t^2)}} 1. \end{aligned} \tag{7}$$

Next we use Lemma 1, so that the right-hand side of (7) becomes

$$\sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t)\left(\frac{x}{d^2t^2} + O(d^2t^2 \log^3 x)\right). \tag{8}$$

In view of Lemma 3, we have

$$x \sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} \mu(d)\mu(t)\frac{1}{d^2t^2} = \prod_p \left(1 - \frac{2}{p^2}\right)x + O\left(\alpha x^{\frac{3}{4}+\varepsilon}\right). \tag{9}$$

Using Lemma 2 to bound the error term in (8), we have

$$\sum_{\substack{d,\, t \le \sqrt{\alpha x+\beta} \\ \gcd(d,t)=1 \\ dt \le x^{1/4}}} d^2t^2 \log^3 x \ll \sum_{m \le x^{1/4}} m^2 \log^3 x \ll x^{\frac{3}{4}+\varepsilon} \log^3 x. \tag{10}$$

Theorem 2 follows from (7)–(10). □

4 Final remarks

Following the referee's report, since Dimitrov [5] proved in 2020 that there exist infinitely many consecutive square-free numbers of the form $\lfloor \alpha p \rfloor$, $\lfloor \alpha p \rfloor + 1$, where p is a prime and $\alpha > 0$ is an irrational algebraic number, the referee asks, following the spirit of the above work, whether there exist infinitely many consecutive square-free numbers of the form $\lfloor \alpha p + \beta \rfloor$, $\lfloor \alpha p + \beta \rfloor + 1$, where p is a prime, $\alpha > 0$ is an irrational algebraic number and $\beta \in [0, \alpha)$. In a preliminary attempt, the authors proceed with the same approach as above by considering the sum

$$\sum_{p \le x} \mu^2(\lfloor \alpha p + \beta \rfloor)\mu^2(\lfloor \alpha p + \beta \rfloor + 1) = \sum_{p \le x} \sum_{d^2 \mid \lfloor \alpha p + \beta \rfloor} \mu(d) \sum_{t^2 \mid \lfloor \alpha p + \beta \rfloor + 1} \mu(t)$$

$$= \sum_{\substack{d, t \le \alpha x + \beta \\ (d,t) = 1}} \mu(d)\mu(t) \sum_{\substack{p \le x \\ \lfloor \alpha p + \beta \rfloor \equiv 0 (\mathrm{mod}\ d^2) \\ \lfloor \alpha p + \beta \rfloor + 1 \equiv 0 (\mathrm{mod}\ t^2)}} 1.$$

Using the Chinese remainder theorem, the last sum reduces to

$$\sum_{\substack{p \le x \\ \lfloor \alpha p + \beta \rfloor \equiv \alpha (\mathrm{mod}\ d^2 t^2)}} 1.$$

It is this sum that the authors have not yet been able to obtain an asymptotic formula which will allow us to make a suitable sub-division of the range of dt so that Lemma 4 is applicable. However, this attempt positively suggests the following:

Conjecture *there exist infinitely many consecutive square-free numbers of the form* $\lfloor \alpha p + \beta \rfloor$, $\lfloor \alpha p + \beta \rfloor + 1$, *where* p *is a prime,* $\alpha > 0$ *is an irrational algebraic number and* $\beta \in [0, \alpha)$.

We wish to thank the referee for his/her careful reading of the original manuscript, his suggestion and advice.

References

1. Abercrombie, A.G., Banks, W.D., Shparlinski, I.E.: Arithmetic functions on Beatty sequences. Acta Arith. **136**, 81–89 (2009)
2. Apostol, T.M.: Introduction to Analytic Number Theory. Springer, New York (1976)
3. Begunts, A.V., Goryashin, D.V.: On the values of Beatty sequence in an arithmetic progression. Chebyshevskii Sb. **21**(1), 343–346 (2020)
4. Carlitz, L.: On a problem in additive arithmetic. II. Q. J. Math. Oxf. **3**, 273–290 (1932)
5. Dimitrov, S.I.: Consecutive square-free numbers of a special form (2018). arXiv:1702.03983v3 [math.NT]
6. Dimitrov, S.I.: On the distribution of consecutive square-free numbers of the form $\lfloor \alpha n \rfloor, \lfloor \alpha n \rfloor + 1$, Proc. Jangjeon Math. Soc. **22**, 463–470 (2019)

7. Estermann, T.: On the representation of a number as the sum of two numbers not divisible by k th powers. J. Lond. Math. Soc. **6**, 37–40 (1931)
8. Gűloğlu, A.M., Nevans, C.W.: Sums of multiplicative functions over a Beatty sequence. Bull. Austral. Math. Soc. **78**, 327–334 (2008)
9. Goryashin, D.V.: Squarefree numbers in the sequence $\lfloor \alpha n \rfloor$. Chebyshevskii Sb. **14**(3), 42–48 (2013)
10. Heath-Brown, D.R.: The square sieve and consecutive square-free numbers. Math. Ann. **266**, 251–259 (1984)
11. Reuss, T.: Pairs of k-free numbers, consecutive square-full numbers. arXiv:1212.3150v2 (2014)
12. Shapiro, H.N.: Introduction to the Theory of Numbers. Wiley, New York (1983)
13. Tangsupphathawat, P., Srichan, T., Laohakosol, V.: Consecutive square-free numbers in Piatetski-Shapiro sequences. Bull. Aust. Math. Soc. **1–6** (2021). https://doi.org/10.1017/S0004972721000666

Author Biography

Name	Mr. Veasna Kim
Date of Birth	10^{th} April 1990
Address	No. 30I, St. 60DIE, Khva Village, Dangkor Sub-district, Dangkor District, Phnom Penh, Cambodia
Education	(2015) Bachelor of Science in Mathematics GPA 3.00 (First Class Honor) Angkor Khemara University, Takeo, Cambodia
	(2019) Master of Science in Mathematics GPA 3.16 Prince of Songkla University, Hat Yai, Thailand
	(2022) Doctor of Philosophy in Applied Mathematics King Mongkut's Institute of Technology Ladkrabang Bangkok, Thailand
Scholarship	1. Royal Scholarship under Her Royal Highness Princess Maha Chakri Sirindhorn Education Project to The Kingdom of Cambodia, The Commission on Higher Education, Thailand, 2017-2019
	2. KMITL Doctoral Scholarships, Thailand, 2019-2022

Academic Publications

1. Kim, V. Laohakosol, V. and Mavecha, S. April 2022. "A divided-difference characterization of polynomials over finite fields of characteristic two ". *Aequationes Mathematicae*, 96(2): 339-347.
2. Kim, V. Srichan, T. and Mavecha, S. July 2022. "On r-free integers in Beatty sequences". *Boletin de la Sociedad Mathemática Mixicana,* 28 (2): 1-10.