Some problems related to the additive representation functions

outline of PhD Thesis

Eszter Rozgonyi

Supervisor: Dr. Csaba Sándor

2015
Introduction

In the PhD thesis we prove some results which are related to the additive representation functions and its properties. Let \( \mathbb{N} \) denote the set of non-negative integers, and let \( h \geq 2 \) be a fixed integer. Let \( A = \{a_1, a_2, \ldots\} \), \( (0 \leq a_1 < a_2 < \ldots) \) be an infinite sequence of nonnegative integers. Then for \( n = 0, 1, 2, \ldots \) the representation functions \( R_{h,A}^{(1)}(n) \), \( R_{h,A}^{(2)}(n) \) and \( R_{h,A}^{(3)}(n) \) denote the number of solutions of the equations:

\[
\begin{align*}
a_{i_1} + \cdots + a_{i_h} &= n, a_{i_1}, \ldots, a_{i_h} \in A, \\
a_{i_1} + \cdots + a_{i_h} &= n, a_{i_1}, \ldots, a_{i_h} \in A, a_{i_1} \leq \cdots \leq a_{i_h}, \\
a_{i_1} + \cdots + a_{i_h} &= n, a_{i_1}, \ldots, a_{i_h} \in A, a_{i_1} < \cdots < a_{i_h}
\end{align*}
\]

respectively. (In the first case the order of the summands counts, and they could be equal. In the second case the order of the elements does not count and they could be equal. In the last case the order of the elements does not count and they could not be equal.) We note that there is connection between these three functions. For example \( (h = 2) \):

\[
R_{2,A}^{(2)}(n) = \begin{cases} 
R_{2,A}^{(3)}(n) + 1 & \text{if } n \text{ is even and } \frac{n}{2} \in A \\
R_{2,A}^{(3)}(n) & \text{otherwise}
\end{cases}
\]

In most cases we shall express each result in terms of whichever representation function is the most appropriate or the most convenient.

The additive representation functions were studied by many aspects. The first question which raised in this topic that \( R_{2,A}^{(i)}(n) \), \( i = 1, 2, 3 \) can be constant or not. In other words is it possible to design a nontrivial set \( A \), so that, for some misbehaviour at the beginning, \( R_{2,A}^{(i)}(n) \), \( i = 1, 2, 3 \) constant? The answer is NO in every cases. Then how nearly constant can \( R_{2,A}^{(1)}(n) \), be on average? The famous Erdős–Fuchs theorem [ErFu] involves this question.

We can say also that this theorem means the beginning of the research of the additive representation functions. This result has been generalized and extended by many people.

There are many questions and results in the literature which deal with the properties of these functions (i.e. [ErRe], [HalRo]). For example Erdős showed that there exists a sequence \( A \subset \mathbb{N} \) for which every \( n \ R_{2,A}^{(1)}(n) = \Theta(\log n) \). In few papers Erdős, Sárközy and T. Sós studied the regularity property and the monotonicity of the function \( R_{2,A}^{(1)}(n) \) ([ErSa85], [ErSa86], [ErSaTSos87] and [ErSaTSos85]).

One can ask inverse questions also. Namely what could we say about the sets \( A \) and \( B \) if we have information about their representation functions.
Nathanson [Nat78] was the first who studied related questions. In this thesis we extend and generalize some results of Erdős and Nathanson by using generating function method and probabilistic method. We also prove some theorems about the additive complement sets, Sidon basis and representation functions on groups.

In the following sections we give a short summary about the results. Section 1. is about the converse of the Erdős–Fuchs theorem for the $R_{h,A}^{(1)}(n)$, $h > 2$ representation function. In Section 2. we generalize a theorem of Nathanson which is about an inverse question. In Section 3. we prove a conjecture of Chen and Fang about additive complement sets. We study the representation functions on groups in Section 4.. And finally in Section 5. we show the existence of a Sidon sequence which is asymptotic basis of order 3. In this outline we do not write the details of the proofs, while they contain many analytic calculations. Usually we only write about the main ideas.

1 A converse to an extension of a Theorem of Erdős and Fuchs

The result of this section is connected to the famous Erdős-Fuchs theorem. It is based on the article [RoSa13].

For $r > 0$ let $N(r)$ count the number of lattice points inside the boundary of a circle with center at the origin and radius $r$. The famous Gauss-circle conjecture says that

$$N(r) = r^2\pi + O(r^{1/2+\varepsilon}).$$

Nowadays the best result due to Huxley [Hux] is that here $O(r^{1/2+\varepsilon})$ can be replaced by $O(r^{131/208})$. On the other hand, using the techniques of the Fourier analysis, Hardy [Har] proved that

$$N(r) = r^2\pi + O(r^{1/2}(\log r)^{1/4})$$

can’t hold for all sufficiently large $r$.

Let $A = \{0 \leq a_1 \leq a_2 \leq \ldots\}$. We recall the definition of $R_{h,A}^{(1)}$ for this set (i.e. $R_{h,A}^{(1)}$ denotes the number of solutions of the equation $a_{i_1} + \cdots + a_{i_h} = n, a_{i_1}, \ldots, a_{i_h} \in A$ ). Using this definition we can write that

$$N(r) = \sum_{n \leq r^2} R_{2,A}^{(1)}(n)$$
provided \( \mathcal{A} = \{0, 1, 1, 4, 4, 9, 9, 16, 16, \ldots \} \).

From this point let again \( \mathcal{A} = \{0 \leq a_1 < a_2 < \ldots \} \). In [ErFu] (1956), Erdős and Fuchs proved that for any sequence \( \mathcal{A} \) and constant \( c > 0 \),

\[
\sum_{n=0}^{N} R_{2, \mathcal{A}}^{(1)}(n) = cN + o(N \frac{1}{2} (\log N)^{-\frac{1}{2}})
\]

can’t hold for all sufficiently large \( n \). This theorem asserts that \( R_{2, \mathcal{A}}^{(1)}(n) \) cannot behave very regularly. Although here \( o(N \frac{1}{2} (\log N)^{-\frac{1}{2}}) \) is slightly weaker than Hardy’s bound \( O(r \frac{1}{2} (\log r)^{\frac{1}{2}}) \), the Erdős–Fuchs theorem is valid for any sequence of \( \mathcal{A} \) of nonnegative integers, rather than only for the sets of square numbers. Subsequently Jurkat (seemingly unpublished), and later in 1990 Montgomery and Vaughan [MoVa] improved this theorem to the following. The formula

\[
\sum_{n=0}^{N} R_{2, \mathcal{A}}^{(1)}(n) = cN + o(N \frac{1}{2})
\]

cannot hold for any sequence \( \mathcal{A} \) and constant \( c > 0 \) for all sufficiently large \( n \). Nowadays, there are several different generalizations of the Erdős-Fuchs theorem [CheTa11], [Hor01], [Hor02], [Hor04], [Ta09]. For example Tang [Ta09] showed in 2009 that \( R_{h, \mathcal{A}}^{(1)}(n) \) cannot behave very regularly. Namely for \( h \geq 2 \) for any sequence \( \mathcal{A} \)

\[
\sum_{n=0}^{N} R_{h, \mathcal{A}}^{(1)}(n) = cN + o(N \frac{1}{2})
\]

with \( c > 0 \) is impossible.

In the opposite direction Vaughan asked whether a further improvement is possible, or in other words, whether there is a sequence \( \mathcal{A} \) and constant \( c > 0 \) such that

\[
\sum_{n=0}^{N} R_{2, \mathcal{A}}^{(1)}(n) = cN + O(N \frac{1}{4} + \varepsilon).
\]

With help of a probabilistic discussion, Ruzsa [Ru97] gave an affirmative answer to this question in 1997. In fact, he proved the existence of a sequence \( \mathcal{A} \) of integers satisfying

\[
\sum_{n=0}^{N} R_{2, \mathcal{A}}^{(1)}(n) = cN + O(N \frac{1}{2} \log N)
\]

for all \( N \geq 2 \).

It is natural to ask whether Ruzsa’s result can be generalized. In 2012, Dai and Pan [DaPa] extended Ruzsa’s theorem:
Theorem 1.1. (Dai, Pan, 2012)
Suppose that \( h \geq 2 \) is an integer and \( \beta < h \) is a positive real number. Then there exists a sequence \( \mathcal{A} = \{a_1 < a_2 < a_3 < \ldots \} \) of positive integers, satisfying
\[
N \sum_{n=0}^{N} R_{h,A}^{(1)}(n) - CN^\beta = \begin{cases} 
O\left(N^{\beta - \beta(h+1)/h^2} \sqrt{\log N}\right) & \text{if } h > 2\beta, \\
O\left(N^{\beta - 3\beta/(2h)} \sqrt{\log N}\right) & \text{if } h < 2\beta, \\
O\left(N^{\beta - 3/4} \log N\right) & \text{if } h = 2\beta,
\end{cases}
\]
where \( C \) is constant.

In this section we prove a better error term for the case \( \beta = 1 \).

Theorem 1.2. (Rozgonyi, Sándor, 2013)
For every \( h \geq 2 \) there exists a sequence \( \mathcal{A} = \{a_1 < a_2 < a_3 < \ldots \} \) of nonnegative integers such that
\[
N \sum_{n=0}^{N} R_{h,A}^{(1)}(n) = N + O \left(N^{1-\frac{5}{4h}} \log N\right).
\]  (1.1)

In the proof of Theorem 1.2 we shall follow the way of Ruzsa in [Ru97]. The key step of the proof is the probabilistic construction of the set \( \mathcal{A} \). So at first we define an infinite increasing sequence \( S = \{s_0, s_1, s_2, \ldots\} \) of nonnegative integers. We will choose the \( n \)th element of \( \mathcal{A} \) from \( \{s_n, s_n+1, \ldots, s_{n+1}\} \) by probabilistic method.

Denote by \( E_n \) the expectation number that how many times occurs the number \( n \) in the sequence \( \mathcal{A} \). We choose these values \( E_n \) such that
\[
E(R_{h,A}^{(1)}(n)) = 1 \quad \forall n \in \mathbb{N}
\]
hold. If we don’t care with the independence, then we get
\[
E(R_{h,A}^{(1)}(n)) \approx \sum_{(i_1, \ldots, i_h) \atop i_1 + \cdots + i_h = n} E_{i_1} E_{i_2} \cdots E_{i_h}.
\]
So we have to solve the following system of equations:
\[
\sum_{(i_1, \ldots, i_h) \atop i_1 + \cdots + i_h = n} E_{i_1} E_{i_2} \cdots E_{i_h} = 1, \quad \forall n \in \mathbb{N}.
\]
Then
\[
\left( \sum_{n=0}^{\infty} E_n z^n \right)^h = \sum_{n=0}^{\infty} \left( \sum_{(i_1, \ldots, i_h) \atop i_1 + \cdots + i_h = n} E_{i_1} E_{i_2} \cdots E_{i_h} \right) z^n = \sum_{n=0}^{\infty} z^n = \frac{1}{1 - z}.
\]
So
\[ \sum_{n=0}^{\infty} E_n z^n = (1 - z)^{-\frac{1}{h}} = \sum_{n=0}^{\infty} \left( -\frac{1}{n} \right)(-z)^n. \]

Hence a natural choice of \( E_n \) is the following
\[ E_n = (-1)^n \left( -\frac{1}{n} \right) = \frac{1}{h} \frac{h+1}{2h} \frac{2h+1}{3h} \ldots \frac{(n-1)h+1}{nh}. \]

Now we can define the sequence \( S \). Denote by \( s_n \) the following
\[ s_n = \min \left\{ m : \sum_{k=0}^{m} E_k > n \right\}. \]

(The precise estimation is \( s_n = c_1(n - c_2)h + O(1) \), where \( c_1 = c_1(h) > 0 \) and \( c_2 = c_2(h) > 0 \).)

From this we get the random sequence \( A \) in the following way:
\[
P(a_n = a) = \begin{cases} 
\sum_{k=0}^{s_n} E_k - n & \text{if } a = s_n, \\
E_n & \text{if } s_n < a < s_{n+1}, \\
(n + 1) - \sum_{k=0}^{s_{n+1}-1} E_k & \text{if } a = s_{n+1}, \\
0 & \text{otherwise.}
\end{cases}
\]

Using the Hoeffding’s inequality and the Borel–Cantelli lemma we show that with probability 1 this sequence satisfies Theorem 1.2. The main difficulty is to decompose the sum in to a sum of independent variables that’s why we need to make lot of analytic calculations.

2 Generalization of a Theorem of Nathanson and related problems

In this section we write about inverse problems about different additive representation functions. More precisely we want to say something about the structure of the sets, if we have information about their representation function. The first results in this topic are due to Nathanson. Our main result is the generalization of a theorem of Nathanson for \( h \)-term representation functions. The section is mainly based on papers [KiRoSa14a], [RoSa14].
Using generating functions, he proved the following result [Nat78]. Let \( F_A, F_B \) and \( T \) be finite sets of integers. If each residue class modulo \( m \) contains exactly the same number of elements of \( F_A \) as elements of \( F_B \), then we write \( F_A \equiv F_B \pmod{m} \). If the number of solutions of the congruence \( a + t \equiv n \pmod{m} \) with \( a \in F_A, t \in T \) equals to the number of solutions of the congruence \( b + t \equiv n \pmod{m} \) with \( b \in F_B, t \in T \) for each residue class \( n \) modulo \( m \) then we write \( F_A + T \equiv F_B + T \pmod{m} \).

**Theorem 2.1. (Nathanson, 1978)**

Let \( A \) and \( B \) be infinite sets of nonnegative integers, \( A \neq B \). Then \( R_{2,A}^{(1)}(n) = \frac{R_{2,B}^{(1)}(n)}{2} \) from a certain point on if and only if there exist positive integers \( N, m \) and finite sets \( F_A, F_B, T \) with \( F_A \cup F_B \subset \{0,1,\ldots,N\} \) and \( T \subset \{0,1,\ldots,m-1\} \) such that \( F_A + T \equiv F_B + T \pmod{m} \), and \( A = F_A \cup C \) and \( B = F_B \cup C \), where \( C = \{c > N : c \equiv t \pmod{m} \text{ for some } t \in T \} \).

It is clear that \( R_{2,A}^{(2)}(n) = \left\lfloor \frac{R_{2,A}^{(1)}(n)}{2} \right\rfloor \) and \( R_{2,A}^{(3)}(n) = \left\lceil \frac{R_{2,A}^{(1)}(n)}{2} \right\rceil \), so for the sets \( A, B \) in Theorem 2.1 we have \( R_{2,A}^{(2)}(n) = R_{2,B}^{(2)}(n) \) and \( R_{2,A}^{(3)}(n) = R_{2,B}^{(3)}(n) \) also from a certain point on. It is easy to see that the symmetric difference of the sets \( A \) and \( B \) in Theorem 2.1 is finite. A. Sárközy asked whether there exist two infinite sets of nonnegative integers \( A \) and \( B \) with infinite symmetric difference, i.e.

\[
| (A \cup B) \setminus (A \cap B) | = \infty
\]

and

\[
R_{2,A}^{(i)}(n) = R_{2,B}^{(i)}(n)
\]

if \( n \geq n_0 \), for \( i = 1, 2, 3 \). For \( i = 1 \) the answer is negative (see in [Do]). For \( i = 2 \) G. Dombi [Do] and for \( i = 3 \) Y. G. Chen and B. Wang [CheWa] proved that the set of nonnegative integers can be partitioned into two subsets \( A \) and \( B \) such that \( R_{2,A}^{(i)}(n) = R_{2,B}^{(i)}(n) \) for all \( n \geq n_0 \). In [Lev] Lev gave a common proof to the above mentioned results of Dombi [Do] and Chen and Wang [CheWa]. Using generating functions Cs. Sándor [Sa] determined the sets \( A \subset \mathbb{N} \) for which either

\[
R_{2,A}^{(2)}(n) = R_{2,N \setminus A}^{(2)}(n) \quad \text{for all } n \geq n_0
\]

or

\[
R_{2,A}^{(3)}(n) = R_{2,N \setminus A}^{(3)}(n) \quad \text{for all } n \geq n_0.
\]

In [Ta08] M. Tang gave an elementary proof of Cs. Sándor’s results. Y. G. Chen and M. Tang studied related questions in [CheTa09].
Let \( C \) be a finite set of integers. Let \( F_A(z), F_B(z), T(z) \) denote polynomials and \( A(z), B(z) \) denote power series having coefficients from the set \( C \) (i.e. \( A(z) = \sum_{n=0}^{\infty} a_n z^n \), where \( a_n \in C \) and \( z \) is a complex number, \( z = r \cdot e^{2\pi i \theta} \)). These series converge in the open unit disc. If \( C = \{0, 1\} \) then the generating functions of the sets \( A, B, F_A, F_B \) and \( T \subseteq \mathbb{N} \) are special kind of these polynomials and power series.

We have the following notation: \( A(z) \sim B(z) \) means that \( A(z) - B(z) = P(z) \), where \( P(z) \) is a polynomial. Using these we can rewrite Nathanson’s Theorem in equivalent form:

**Theorem 2.2.** (Nathanson, 1978-equivalent form)

Let \( A(z) = \sum_{n=0}^{\infty} a_n z^n, B(z) = \sum_{n=0}^{\infty} b_n z^n, a_n, b_n \in \{0, 1\} \). Then \( A(z)^2 \sim B(z)^2 \) if and only if there exist positive integers \( N_0, m \) and polynomials

\[
F_A(z) = \sum_{n=0}^{mN_0-1} d_n z^n, \quad F_B(z) = \sum_{n=0}^{mN_0-1} e_n z^n, \quad d_n, e_n \in \{0, 1\}
\]

such that

\[
A(z) = F_A(z) + T(z) z^{mN_0} (1 - z^m)^{-1} - 1 \quad \text{and} \quad B(z) = F_B(z) + T(z) z^{mN_0} (1 - z^m)^{-1}
\]

\[
1 - z^m \mid T(z) (F_A(z) - F_B(z))
\]

holds.

S. Z. Kiss, R. Rozgonyi and Cs. Sándor [KiRoSa14a] conjectured that Nathanson’s theorem can be generalized as follows.

**Conjecture 2.1.** (Z. Kiss, Rozgonyi, Sándor, 2014)

Let \( h \geq 2, A \) and \( B \) be infinite sets of nonnegative integers, \( A \neq B \). Then \( R_{h, A}^{(1)}(n) = R_{h, B}^{(1)}(n) \) from a certain point on if and only if there exist positive integers \( N_0, m \) and sets \( F_A, F_B \) and \( T \) such that \( F_A \cup F_B \subseteq \{0, 1, \ldots, mN_0 - 1\} \), \( T \subseteq \{0, 1, \ldots, m - 1\} \),

\[
A = F_A \cup \{ km + t : k \geq N_0, t \in T \}, \\
B = F_B \cup \{ km + t : k \geq N_0, t \in T \},
\]

and

\[
(1 - z^m)^{h-1} \mid T(z)^{h-1} (F_A(z) - F_B(z))
\]
where \( F_A(z) \), \( F_B(z) \) and \( T(z) \) denote the generating functions of the sets \( F_A \), \( F_B \) and \( T \).

Using power series, we can rewrite Conjecture 2.1 in equivalent form.

**Conjecture 2.2.** (Equivalent form of Conjecture 2.1)

Let

\[
A(z) = \sum_{n=0}^{\infty} a_n z^n, \quad B(z) = \sum_{n=0}^{\infty} b_n z^n, \quad a_n, b_n \in \{0, 1\}
\]

Then \( A(z)^h \sim B(z)^h \) if and only if there exist positive integers \( N_0, m \) and polynomials

\[
F_A(z) = \sum_{n=0}^{mN_0-1} d_n z^n, \quad F_B(z) = \sum_{n=0}^{mN_0-1} e_n z^n, \quad d_n, e_n \in \{0, 1\}
\]

and

\[
T(z) = \sum_{n=0}^{m-1} t_n z^n, \quad t_n \in \{0, 1\}
\]

such that

\[
A(z) = F_A(z) + T(z)z^{mN_0-1} - z^m, \quad B(z) = F_B(z) + T(z)z^{mN_0-1} - z^m
\]

and

\[
(1 - z^m)^{h-1} \mid T(z)^{h-1}(F_A(z) - F_B(z))
\]

holds.

We can prove Conjecture 2.2 in the case \( h = p^s \), where \( p \) is prime. (Using generating functions in [KiRoSa14a] we proved the sufficiency part of Conjecture 2.1, and we also proved the Conjecture for the case \( h = 3 \).)

**Theorem 2.3.** (Rozgonyi, Sándor, 2014)

Let \( h = p^s \) and let the set \( C \subseteq \mathbb{Z} \), where \( C \) contains incongruent integers modulo \( p \). Let the series

\[
A(z) = \sum_{n=0}^{\infty} a_n z^n, \quad B(z) = \sum_{n=0}^{\infty} b_n z^n, \quad a_n, b_n \in C
\]

Then \( A(z)^h \sim B(z)^h \) if and only if there exist positive integers \( N_0, m \) and polynomials

\[
F_A(z) = \sum_{n=0}^{mN_0-1} d_n z^n, \quad F_B(z) = \sum_{n=0}^{mN_0-1} e_n z^n, \quad d_n, e_n \in C
\]

and

\[
T(z) = \sum_{n=0}^{m-1} t_n z^n, \quad t_n \in C
\]

such that

\[
A(z) = F_A(z) + \frac{T(z)z^{mN_0-1}}{1 - z^m}, \quad B(z) = F_B(z) + \frac{T(z)z^{mN_0-1}}{1 - z^m}
\]

and

\[
(1 - z^m)^{h-1} \mid T(z)^{h-1}(F_A(z) - F_B(z))
\]

holds.
Corollary 2.4. The set \( \mathcal{C} = \{0, 1\} \) implies that Conjecture 2.1 is true for the case \( h = p^s \).

In order to prove Theorem 2.3 we verify the following three lemmas.

Lemma 2.5. Let \( \mathcal{C} \) be a set of integers. Suppose that there exist positive integers \( N_0, m \) and polynomials \( F_A(z) = \sum_{n=0}^{mN_0-1} d_n z^n \), \( F_B(z) = \sum_{n=0}^{mN_0-1} e_n z^n \), \( d_n, e_n \in \mathcal{C} \) and \( T(z) = \sum_{n=0}^{m-1} t_n z^n \), \( t_n \in \mathcal{C} \) such that

\[
A(z) = F_A(z) + \frac{T(z)z^{mN_0}}{1-z^m} \quad \text{and} \quad B(z) = F_B(z) + \frac{T(z)z^{mN_0}}{1-z^m}
\]

and

\[
(1-z^m)^{h-1} \mid T(z)^{h-1} (F_A(z) - F_B(z))
\]

holds. Then \( A(z)^h \sim B(z)^h \).

The following example shows that for any \( \mathcal{C} \subseteq \mathbb{Z}, |\mathcal{C}| \geq 2 \) and \( h \geq 2 \) there exist different power series \( A(z), B(z) \) having their coefficients from \( \mathcal{C} \) with the property \( A(z)^h \sim B(z)^h \).

Proposition 2.6. Let \( \mathcal{C} \subseteq \mathbb{Z}, |\mathcal{C}| \geq 2 \). Then there exist series

\[
A(z) = \sum_{n=0}^{\infty} a_n z^n, \quad B(z) = \sum_{n=0}^{\infty} b_n z^n, \quad a_n, b_n \in \mathcal{C}
\]

such that \( A(z) \neq B(z) \) and \( A(z)^h \sim B(z)^h \).

In the proof of Theorem 2.3 we only use the fact that \( h \) is a power of prime in the next Lemma.

Lemma 2.7. Let \( h = p^s \) and let the set \( \mathcal{C} \subseteq \mathbb{Z} \), where no element of \( \mathcal{C} \) are congruent modulo \( p \). Let \( A(z) = \sum_{n=0}^{\infty} a_n z^n, B(z) = \sum_{n=0}^{\infty} b_n z^n, a_n, b_n \in \mathcal{C} \). The condition \( A(z)^h \sim B(z)^h \) implies that \( A(z) \sim B(z) \).

The condition of Lemma 2.7 that \( \mathcal{C} \) contains incongruent integers modulo \( p \) is important. Imre Z. Ruzsa gave us the following the identity

\[
(1 + \frac{2z^4}{1-z^2})^2 - \frac{2z^5}{1-z^2} = 1 - 4z^4 - 4z^6.
\]

It means that there exist power series \( A(z) \) and \( B(z) \) having coefficients from the set \( \mathcal{C} = \{-1, 0, 2\} \) such that \( A(z)^2 \sim B(z)^2 \), but \( A(z) \not\sim B(z) \), because

\[
-1 + \frac{2z^4}{1-z^2} - \frac{2z^5}{1-z^2} = -1 + 2 \sum_{n=4}^{\infty} (-1)^n z^n.
\]
We can generalize Imre Z. Ruzsa’s construction in the following way:

**Proposition 2.8.** Let $h$ be a prime number. Then there exist a set $C_h = \{c_1, c_2, \ldots, c_{h+1}\}$, $c_1, \ldots, c_{h+1} \in \mathbb{Z}$ such that $c_1, \ldots, c_h$ form a complete set of residues modulo $h$ and power series $A(z) = \sum_{n=0}^{\infty} a_n z^n$, $B(z) = \sum_{n=0}^{\infty} b_n z^n$, $a_n, b_n \in C_h$ such that $A(z)^h \sim B(z)^h$ but $A(z) \not\sim B(z)$.

**Lemma 2.9.** Let $C$ be a finite set of integers, $A(z) = \sum_{n=0}^{\infty} a_n z^n$, $B(z) = \sum_{n=0}^{\infty} b_n z^n$, $a_n, b_n \in C$. If $A(z)^h \sim B(z)^h$ and $A(z) \sim B(z)$ holds,

then there exist positive integers $N_0$, $m$ and polynomials $F_A(z) = \sum_{n=0}^{mN_0-1} d_n z^n$, $F_B(z) = \sum_{n=0}^{m-1} e_n z^n$, $d_n, e_n \in C$ and $T(z) = \sum_{n=0}^{m-1} t_n z^n$, $t_n \in C$ such that

$$A(z) = F_A(z) + \frac{T(z)z^{mN_0}}{1 - z^m},$$
$$B(z) = F_B(z) + \frac{T(z)z^{mN_0}}{1 - z^m}$$

and

$$(1 - z^m)^{h-1} \mid T(z)^{h-1} (F_A(z) - F_B(z)). \quad (2.1)$$

In 2011, Yang [Ya11] gave another proof of Theorem 2.1 without using generating functions. In his paper he posed the following problem.

**Problem.** (Yang, 2011)

If $p \geq 3$ is a prime and $\mathcal{A}$ is an infinite set of nonnegative integers, then does there exist an infinite set of nonnegative integers $\mathcal{B}$ with $\mathcal{A} \neq \mathcal{B}$ such that $R_{p,\mathcal{A}}^{(1)}(n) = R_{p,\mathcal{B}}^{(1)}(n)$ for all sufficiently large $n$?

We show that the answer of Yang’s question is negative.

**Theorem 2.10.** (Kiss, Sándor, Rozgonyi, 2014)

For every positive $p \geq 2$ prime there exists an infinite set of nonnegative integers $\mathcal{A}$ such that for any infinite set of integers $\mathcal{B}$, $\mathcal{A} \neq \mathcal{B}$, we have $R_{p,\mathcal{A}}^{(1)}(n) \neq R_{p,\mathcal{B}}^{(1)}(n)$ for infinitely many positive integer $n$. 

10
We studied some similar problems and get the following results.

**Theorem 2.11.** (Kiss, Sándor, Rozgonyi, 2014)
For every positive integer $H \geq 2$ there exist infinite sets of nonnegative integers $A, B$, $A \neq B$ such that $R_{h,A}^{(l)}(n) = R_{h,B}^{(l)}(n)$, for every $l = 1, 2, 3$ and $2 \leq h \leq H$ from a certain point on.

In the special case $l = 1$, Theorem 2.11 cannot be extended for infinitely many $h$.

**Theorem 2.12.** (Kiss, Sándor, Rozgonyi, 2014)
If for some infinite sets of nonnegative integers $A$ and $B$ the representation function $R_{h,A}^{(1)}(n) = R_{h,B}^{(1)}(n)$, for $n \geq n_0(h)$, for infinitely many positive integer $h \geq 2$, then $A = B$.

The proofs are mostly based on generating function method and the properties of the cyclotomic polynomials.

## 3 Additive complement sets

This section is based on the paper [KiRoSa14b].

Let $A \subseteq \mathbb{N}$ and $B \subseteq \mathbb{N}$ be finite or infinite sets. Let $R_{A+B}(n)$ such kind of representation function which denotes the number of solutions of the equation

$$a + b = n, \quad a \in A, \quad b \in B.$$

We put

$$A(n) = \sum_{a \leq n, a \in A} 1 \quad \text{and} \quad B(n) = \sum_{b \leq n, b \in B} 1,$$

respectively. We say a set $B \subseteq \mathbb{N}$ is an additive complement of the set $A \subseteq \mathbb{N}$ if every sufficiently large $n \in \mathbb{N}$ can be represented in the form $a + b = n$, $a \in A, b \in B$, i.e., $R_{A+B}(n) \geq 1$ for $n \geq n_0$. Additive complement is an important concept in additive number theory, in the past few decades it was studied by many authors [Dan], [Nar], [Ru99], [SaSze]. In [SaSze] Sárközy and Szemerédi proved a conjecture of Danzer [Dan], namely they proved that for infinite additive complements $A$ and $B$ if

$$\limsup_{x \to +\infty} \frac{A(x)B(x)}{x} \leq 1,$$

then

$$\liminf_{x \to +\infty} (A(x)B(x) - x) = +\infty.$$
In [CheFa10] Chen and Fang improved this result and they proved that for any two infinite additive complements $A$ and $B$, if
\[ \limsup_{x \to +\infty} \frac{A(x)B(x)}{x} > 2, \quad \text{or} \quad \limsup_{x \to +\infty} \frac{A(x)B(x)}{x} < \frac{5}{4}, \]
then
\[ \lim_{x \to +\infty} (A(x)B(x) - x) = +\infty. \]

In the other direction they proved in [CheFa11] that for any integer $a \geq 2$, there exist two infinite additive complements $A$ and $B$ such that
\[ \limsup_{x \to +\infty} \frac{A(x)B(x)}{x} = \frac{2a + 2}{a + 2}, \]
but there exist infinitely many positive integers $x$ such that $A(x)B(x) - x = 1$.

In [CheFa13] they studied the case when $A$ is a finite set. In this case the situation is different from the infinite case. Chen and Fang proved that for any two additive complements $A$ and $B$ with $|A| < +\infty$ or $|B| < +\infty$, if
\[ \limsup_{x \to +\infty} \frac{A(x)B(x)}{x} > 1, \]
then
\[ \lim_{x \to +\infty} (A(x)B(x) - x) = +\infty. \]

They also proved that if
\[ A = \{a + im^s + k_im^{s+1} : i = 0, \ldots, m - 1\}, \]
where $|A| = m$, $a$, $s \geq 0$ and $k_i$ are integers, then there exists an additive complement $B$ of $A$ such that $A(x)B(x) - x = O(1)$. In the special case $|A| = 3$ they proved that if $A$ is not of the form $\{a + i3^s + k_i3^{s+1} : i = 0, 1, 2\}$, where $a$, $s \geq 0$ and $k_i$ are integers, then for any additive complement $B$ of $A$,
\[ \lim_{x \to +\infty} (A(x)B(x) - x) = +\infty \]
holds.

Chen and Fang posed the following conjecture in [CheFa13].

**Conjecture 3.1. (Chen, Fang, 2013)**

If the set of nonnegative integers $A$ is not of the form
\[ A = \{a + im^s + k_im^{s+1} : i = 0, \ldots, m - 1\}, \]
where $a, m > 0$, $s \geq 0$ and $k_i$ are integers, then, for any additive complement $B$ of $A$, we have
\[ \lim_{x \to +\infty} (A(x)B(x) - x) = +\infty. \]
We prove this conjecture, when the number of elements of the set $A$ is prime:

**Theorem 3.1.** (Kiss, Rozgonyi, Sándor, 2014)

Let $p$ be a positive prime and $A$ be a set of nonnegative integers with $|A| = p$. If $A$ is not of the form

$$A = \{a + ip^s + k_ip^{s+1} : i = 0, ..., p - 1\},$$

(3.1)

where $a > 0$, $s \geq 0$ and $k_i$ are integers, then, for any additive complement $B$ of $A$, we have

$$\lim_{x \to +\infty} (A(x)B(x) - x) = +\infty.$$  

(3.2)

When the number of elements of $A$ is a composite number, we disprove Conjecture 3.1:

**Theorem 3.2.** (Kiss, Rozgonyi, Sándor, 2014)

For any composite number $n > 0$, there exists a set $A$ and a set $B$ such that $|A| = n$, $B$ is an additive complement of $A$ and $A$ is not of the form

$$A = \{a + in^s + k_in^{s+1} : i = 0, ..., n - 1\},$$

(3.3)

where $s \geq 0$, $a > 0$, and $k_i$ are integers, and

$$A(x)B(x) - x = O(1).$$

In the proofs we again use the generating function method and the cyclotomic polynomials.

### 4 Representation functions on groups

We can study the representation functions on groups also and usually we have some similar result like in the case of natural numbers. The chapter is mostly based on the paper [KiRoSa14c].

Let $X$ be a semigroup, written additively. Let $A_1, \ldots, A_h$ be nonempty subsets of $X$ and let $x$ be an element of $X$. We denote by $|A|$ the cardinality of the set $A$. We define the ordered representation function

$$R_{A_1, \ldots, A_h}(x) = |\{(a_1, \ldots, a_h) \in A_1 \times \cdots \times A_h : a_1 + \cdots + a_h = x\}|.$$

If $A_i = A$ for $i = 1, \ldots, h$, then we write

$$R_{h,A}^{(1)}(x) = |\{(a_1, \ldots, a_h) : a_i \in A, a_1 + \cdots + a_h = x\}|.$
Let $X$ be an abelian semigroup, written additively. For $A \subset X$, let $A^h$ denote the set of all $h$-tuples of $A$. Two $h$-tuples $(a_1, \ldots, a_h) \in A^h$ and $(a'_1, \ldots, a'_h) \in A^h$ are equivalent if there is a permutation $\alpha : \{1, \ldots, h\} \to \{1, \ldots, h\}$ such that $a_{\alpha(i)} = a'_i$ for $i = 1, \ldots, h$. Two other representation functions arise often and naturally in additive number theory as we mentioned earlier. The unordered representation function $R_{h,A}^{(2)}(x)$ counts the number of equivalence classes of $h$-tuples $(a_1, \ldots, a_h)$ such that $a_1 + \cdots + a_h = x$. The unordered restricted representation function $R_{h,A}^{(3)}(x)$ counts the number of equivalence classes of $h$-tuples $(a_1, \ldots, a_h)$ of pairwise distinct elements of $A$ such that $a_1 + \cdots + a_h = x$. It is easy to see that the definitions of the unordered and the unordered restricted representation functions make sense only in Abelian groups.

Alternative definitions for $R_{2,A}^{(2)}(x)$ and $R_{2,A}^{(3)}(x)$ are the following. Denote by

$$D_A(x) = \#\{a : a \in A, a + a = x\}$$

then

$$R_{2,A}^{(2)}(x) = \frac{1}{2} R_{2,A}^{(1)}(x) + \frac{1}{2} D_A(x)$$

(4.1)

and

$$R_{2,A}^{(3)}(x) = \frac{1}{2} R_{2,A}^{(1)}(x) - \frac{1}{2} D_A(x).$$

(4.2)

Let $X = \mathbb{N}$. Sárközy asked if there exist two sets $A$ and $B$ with $|A \Delta B| = \infty$ such that $R_{2,A}^{(i)}(n) = R_{2,B}^{(i)}(n)$, for $i = 1, 2, 3$ and for all sufficiently large $n$. For $i = 2$ Dombi [Do] proved that the answer is positive and for $i = 1$ the answer is negative. For $i = 3$ Chen and Wang [CheWa] proved that the set of natural numbers can be partitioned into two subsets $A$ and $B$ such that $R_{2,A}^{(3)}(n) = R_{2,B}^{(3)}(n)$ for every $n$ large enough. Lev [Lev] and independently Sándor [Sa] characterized all subsets $A \subset \mathbb{N}$ such that $R_{2,A}^{(2)}(n) = R_{2,\mathbb{N} \setminus A}^{(2)}(n)$ or $R_{2,A}^{(3)}(n) = R_{2,\mathbb{N} \setminus A}^{(3)}(n)$ for big enough $n$. The precise theorems are the following.

**Theorem 4.1.** (Lev, Sándor, 2004)

Let $X = \mathbb{N}$. Let $N$ be a positive integer. The equality $R_{2,A}^{(2)}(n) = R_{2,\mathbb{N} \setminus A}^{(2)}(n)$ holds for $n \geq 2N - 1$ if and only if $|A \cap [0, 2N - 1]| = N$ and $2m \in A \Leftrightarrow m \in A$, $2m + 1 \in A$ $\iff m \notin A$ for $m \geq N$.

**Theorem 4.2.** (Lev, Sándor, 2004)

Let $X = \mathbb{N}$. Let $N$ be a positive integer. The equality $R_{2,A}^{(3)}(n) = R_{2,\mathbb{N} \setminus A}^{(3)}(n)$ holds for $n \geq 2N - 1$ if and only if $|A \cap [0, 2N - 1]| = N$ and $2m \in A \Leftrightarrow m \notin A$, $2m + 1 \in A$ $\iff m \in A$ for $m \geq N$. 

14
Tang [Ta08] gave an elementary proofs of Lev and Sándor’s results. In [CheYa12a], [CheYa12b], [CheYa13], [Ya14] Chen and Yang studied related problems about weighted representation functions. Similar statement to the above theorems can not be formulated for the representation function $R^{(1)}_{2,A}(n)$ because $R^{(1)}_{2,A}(n)$ is odd if and only if $\frac{n}{2} \in A$, therefore either $R^{(1)}_{2,A}(2m)$ or $R^{(1)}_{2,N\setminus A}(2m)$ is odd. A nontrivial result is the following in this direction.

**Theorem 4.3. (Kiss, Rozgonyi, Sándor, 2014)**

Let $X = \mathbb{N}$. The equality $R_{A+B}(n) = R_{N\setminus A+N\setminus B}(n)$ holds from a certain point on if and only if $|N \setminus (A \cup B)| = |A \cap B| < \infty$.

The modular questions were solved by Chen and Yang [CheYa12a].

**Theorem 4.4. (Chen, Yang, 2012)**

Let $X = \mathbb{Z}_m$. The equality $R^{(i)}_{2,A}(n) = R^{(i)}_{2,\mathbb{Z}_m\setminus A}(n)$ holds for all $n \in \mathbb{Z}_m$ if and only if $m$ is even and $|A| = m/2$.

**Theorem 4.5. (Chen, Yang, 2012)**

Let $X = \mathbb{Z}_m$. For $i \in \{2,3\}$, the equality $R^{(i)}_{2,A}(n) = R^{(i)}_{2,\mathbb{Z}_m\setminus A}(n)$ holds for all $n \in \mathbb{Z}_m$ if and only if $m$ is even and $t \in A \iff t + m/2 \notin A$ for $t = 0,1,\ldots,m/2-1$.

We extend this theorem to arbitrary finite group $G$ and the second theorem to finite Abelian group. (From now we denote the groups, subgroups and subsets with capital letters.)

**Theorem 4.6. (Kiss, Rozgonyi, Sándor, 2014)**

Let $X = G$ be a finite group. Then

(i) If there exists $g \in G$ for which the equality $R_{A+B}(g) = R_{G\setminus A+G\setminus B}(g)$ holds, then $|A| + |B| = |G|$.

(ii) If $|A| + |B| = |G|$, then the equality $R_{A+B}(g) = R_{G\setminus A+G\setminus B}(g)$ holds for all $g \in G$.

We generalize theorem 4.5 in the following way.

**Theorem 4.7. (Kiss, Rozgonyi, Sándor, 2014)**

Let $X = G$ be a finite group and $h \geq 2$ a fixed integer.

(i) If the equality $R^{(1)}_{h,A}(g) = R^{(1)}_{h,G\setminus A}(g)$ holds for all $g \in G$, then $|G|$ is even and $|A| = |G|/2$.  

15
(ii) If $h$ is even and $|A| = |G|/2$ then $R_{h,A}^{(1)}(g) = R_{h,G \setminus A}^{(1)}(g)$ holds for all $g \in G$.

We note that the case when $h$ is odd is still open. When $h$ is odd we can only prove the following weaker result.

**Theorem 4.8.** (Kiss, Rozgonyi, Sándor, 2014)
Let $X = \mathbb{Z}_m$ and $h > 2$ be a fixed odd integer. If $A \subseteq \mathbb{Z}_m$ such that $|A| = m/2$ then there exists a $g \in \mathbb{Z}_m$ such that $R_{h,A}^{(1)}(g) \neq R_{h,\mathbb{Z}_m \setminus A}^{(1)}(g)$.

It would be interesting to characterize all that partitions of a finite Abelian group $G$ such that $R_{h,A}^{(1)}(g) = R_{h,A}^{(1)}(j)$ for every $g \in G$.

For the two other representation functions we have the following result (only for the $h = 2$ case).

**Theorem 4.9.** (Kiss, Rozgonyi, Sándor, 2014)
Let $X = G$ be a finite Abelian group. For $i \in \{2, 3\}$ the equality $R_{A}^{(i)}(g) = R_{G \setminus A}^{(i)}(g)$ holds for every $g \in G$, if and only if $D_A(g) = D_{G \setminus A}(g)$ for every $g \in G$.

In the proofs we again use the generating function method.

## 5 On Sidon sets which are asymptotic bases

This section is based on the article [KiRoSa14d].

Let $A = \{a_1, a_2, \ldots\}$, $a_1 < a_2 < \ldots$ be an infinite sequence of positive integers. A (finite or infinite) set $A$ of positive integers is said to be a Sidon set if all the sums $a + b$ with $a, b \in A$, $a \leq b$ are distinct. In other words $A$ is a Sidon set if for every $n$ positive integer $R_{2,A}^{(2)}(n) \leq 1$.

We say a set $A \subseteq \mathbb{N}$ is an asymptotic basis of order $h$, if every large enough positive integer $n$ can be represented as the sum of $h$ terms from $A$, i.e., if there exists a positive integer $n_0$ such that $R_{h,A}^{(2)}(n) > 0$ for $n > n_0$.

In [ErSaTSo94a] and [ErSaTSo94b] P. Erdős, A. Sárközy and V. T. Sós asked if there exists a Sidon set which is an asymptotic basis of order 3. The problem was also appears in [Sar] (with a typo in it: order 2 is written instead of order 3). It is easy to see [GrHaHePi] that a Sidon set cannot be an asymptotic basis of order 2. A few years ago J. M. Deshouillers and A. Plagne in [DesPla] constructed a Sidon set which is an asymptotic basis of order at most 7. In [Kis] S. Kiss proved the existence of a Sidon set which is an asymptotic basis of order 5. In this chapter we will improve this result by proving that there exists an asymptotic basis of order 4 which is a Sidon set by using probabilistic methods.
Theorem 5.1. There exists an asymptotic basis of order 4 which is a Sidon set.

We note that at the same time Javier Cilleruelo [Cil] has proved a slightly stronger result namely the existence of a Sidon set which is an asymptotic basis of order $3 + \varepsilon$. It means, that for any $\varepsilon > 0$ there exists a Sidon sequence $A$ of positive integers such that all positive, large enough integer $n$ can be written as $n = a_1 + a_2 + a_3 + a_4$, $a_1, a_2, a_3, a_4 \in A$, $a_4 \leq n\varepsilon$. He obtained his result independently from our work by using other probabilistic methods.

About the probabilistic method.

An important problem in additive number theory is to prove that a sequence with certain properties exists. One of the essential ways to obtain an affirmative answer for such a problem is actually to construct a sequence with the required properties. But even when this direct approach proves impracticable, it may still be possible to establish the existence of such a sequence. Many such existence theorems have been obtained by Erdős and Rényi. These theorems are the basis of the so-called probabilistic method. There is an excellent summary of this method in the Halberstam–Roth book [HalRo].

Let $\Omega$ denote the set of strictly increasing sequences of positive integers. In this thesis we denote the probability of an event $E$ by $P(E)$ and the expectation of a random variable $\xi$ by $E(\xi)$. The following Lemma plays an important role.

Lemma 5.2. Let $\theta_1, \theta_2, \theta_3, \ldots$ be real numbers satisfying

$$0 \leq \theta_n \leq 1 \ (n = 1, 2, \ldots).$$

Then there exists a probability space $(\Omega, X, P)$ with the following two properties:

(i) For every $n \in \mathbb{N}$, the event $E^{(n)} = \{A : A \in \Omega, n \in A\}$ is measurable, and $P(E^{(n)}) = \theta_n$.

(ii) The events $E^{(1)}$, $E^{(2)}$, $\ldots$ are independent.

See Theorem 13. in [HalRo], p. 142. We denote the characteristic function of the event $E^{(n)}$ by $t_{(A,n)}$ (or $t_n$ in a shorter way, if the set $A$ is obvious). In other way we can say the boolean variable $t_{(A,n)}$ ($t_n$) means that:

$$t_{(A,n)} = t_n = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{if } n \notin A. \end{cases}$$
Furthermore, for some $A = \{a_1, a_2, \ldots\} \in \Omega$ we denote the number of solutions of $a_1 + a_2 + \ldots + a_i = n$ with $a_1, \ldots, a_n \in A$, $1 \leq a_1 < a_2 < \ldots < a_{i_n} < n$ by $r_{h,A}(n)$ (this is the $R^{(3)}_{h,A}(n)$ representation function). Let

$$r_{h,A}(n) = \sum_{l \leq a_i < a_{i_2} < \ldots < a_{i_h} < n} t_{(A,a_{i_1})} t_{(A,a_{i_2})} \ldots t_{(A,a_{i_h})}. \quad (5.1)$$

Let $r^*_{h,A}(n)$ denote the number of those representations of $n$ in the form (5.1) in which there are at least two equal terms. Thus we have

$$R^{(1)}_{h,A}(n) = h! r_{h,A}(n) + r^*_{h,A}(n). \quad (5.2)$$

From (5.2) we can conclude that in the proof we can use $r_{h,A}(n)$ instead of $R^{(1)}_{h,A}(n)$. It is easy to see from (5.1) that $r_{h,A}(n)$ is the sum of random variables. However, for $h > 2$ these variables are not independent because the same $t_{(A,a_i)}$ may appear in many terms. There are some probabilistic results which can help us to overcome this trouble. First we present the method of J. H. Kim and V. H. Vu. We give a short survey of this method. Interested reader can find more details in [KimVu], [TaoVu], [Vu00a], [Vu00b].

Assume that $t_1, t_2, \ldots, t_n$ are independent binary (i.e., all $t_i$’s are in $\{0, 1\}$) random variables. (We can regard these $t_i$-s as characteristic functions.) Consider a polynomial $Y = Y(t_1, \ldots, t_n)$ in $t_1, t_2, \ldots, t_n$ with degree $k$ (where the degree of this polynomial equals to the maximum of the sum of the exponents of the monomials). We say a polynomial $Y$ is totally positive if it can be written in the form $Y = \sum_i e_i \Gamma_i$, where the $e_i$’s are positive and $\Gamma_i$ is a product of some $t_j$’s. Furthermore, $Y$ is regular if all of its coefficients are between zero and one. We also say $Y$ is simplified, if all of its monomials are square-free (i.e. do not contain any factor of $t_i^2$), and homogeneous if all the monomials have the same degree. Thus for instance a boolean polynomial is automatically regular and simplified, though not necessarily homogeneous.

Given any multi-index $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$, we define the partial derivative $\partial^\alpha(Y)$ of $Y$ as

$$\partial^\alpha(Y) = \left( \frac{\partial}{\partial t_1} \right)^{\alpha_1} \ldots \left( \frac{\partial}{\partial t_n} \right)^{\alpha_n} Y(t_1, \ldots, t_n).$$

For instance, if $Y = t_1 t_2$ and $\alpha_1 = (1, 1)$ and $\alpha_2 = (1, 2)$, then $\partial^{\alpha_1} = 2t_1$ and $\partial^{\alpha_2} = 2$. If $\alpha$ equals to zero vector, then $\partial^\alpha(Y) = Y$. Let denote the order of $\alpha$ as $|\alpha| = \alpha_1 + \ldots + \alpha_n$. For any order $d \geq 0$, we denote $E_d(Y) = \max_{\alpha:|\alpha|=d} E(\partial^\alpha Y)$. Thus for instance $E_0(Y) = E(Y)$ and $E_d(Y) = 0$ if $d$ exceeds the degree of $Y$. We also define $E_{\geq d}(Y) = \max_{d'\geq d} E_{d'}(Y)$. The following result is due to Kim and Vu.
Theorem 5.3. (J. H. Kim and V. H. Vu, 2000) Let $k \geq 1$ and $Y = Y(t_1, \ldots, t_n)$ be a totally positive polynomial of $n$ independent boolean variables $t_1, \ldots, t_n$. Then there exists a constant $C_k > 0$ depending only on $k$ (which is the degree of the polynomial) such that

$$\mathbb{P} \left( |Y - \mathbb{E}(Y)| \geq C_k \lambda^{k-\frac{1}{2}} \sqrt{\mathbb{E}_{z_2}(Y) \mathbb{E}_{z_1}(Y)} \right) = O_k \left( e^{-\frac{1}{4}(k-1)\log n} \right)$$

for all $\lambda > 0$.

See [KimVu] for the proof. Informally this theorem asserts that when the derivatives of $Y$ are smaller on average than $Y$ itself, and the degree of $Y$ is small, then $Y$ is concentrated around its mean.

**Sketch of the proof.** Define the sequence $\theta_n$ in Lemma 5.2 by

$$\theta_n = n^{-\frac{5}{7}}, \quad (5.3)$$

that is $\mathbb{P}(\{A : A \in \Omega, n \in A\}) = n^{-\frac{5}{7}}$, for $n \in \mathbb{N}$. For a given set $A \in \Omega$ let the set $B$ be the following

$$B = \{ b : b \in A, \exists a', a'', a''' \in A : b + a' = a'' + a''' = a'' + a''', a', a'', a''', b < b \}. \quad (5.4)$$

Thus $A \setminus B$ is a Sidon set. We will prove that $A \setminus B$ is an asymptotic basis of order 4 with probability 1. This means that there exists integer $N_0$ such that with probability 1, $r_{4,A \setminus B}(n) > 0$ for $n \geq N_0$. Since

$$r_{4,A \setminus B}(n) = r_{4,A}(n) - (r_{4,A}(n) - r_{4,A \setminus B}(n)),$$

if we get a lower bound for $r_{4,A}(n)$ and an upper bound for $(r_{4,A}(n) - r_{4,A \setminus B}(n))$ then we will have a lower bound for $r_{4,A \setminus B}(n)$. So formally we will show that there are positive constants $C_1$ and $N_1$ such that with probability 1,

$$r_{4,A}(n) > C_1 n^\frac{1}{7}, \quad n \geq N_1, \quad (5.5)$$

and there are positive constants $C_2$ and $N_2$ such that with probability 1,

$$r_{4,A}(n) - r_{4,A \setminus B}(n) < C_2 (\log n)^{6.5}, \quad n \geq N_2. \quad (5.6)$$

In order to prove (5.5) and (5.6) we use Theorem 5.3 and lot of analytic calculations.
6 Summary

This thesis was devoted to the different properties of the additive representation functions and related problems just like Sidon sequences, additive complement sets etc. We can say that the existence of these recent results shows that the additive representation functions is a famous field of the additive number theory researches. For possible directions of future research, there is a wide variety of open questions.

For example it is still an open question that in the converse of the Erdős–Fuchs theorem could we give a better error term or not. The original \( h = 2 \) case is sharp, and in the lower estimate Tang got the same result for every \( h \geq 2 \). Nowadays the best upper error term is only \( O(N^{1/4} \log N) \) which is far from \( N^{1/2} \). It seems to be sure that for better error term we need to use other probabilistic construction.

It is also an interesting question whether Conjecture 2.1 is true when \( h \) is composite number \( h \neq p^s \) or not. Recently we can not prove this case, and it can happen that the theorem is not true in that case.

We can ask some similar question about additive complement sets like Chen and Fang did and also we can study the properties of the representation functions in (Abelian) groups. For example Theorem 4.7 is still open in the case when \( h \) is odd. And it would be interesting to characterize all that partitions of a finite Abelian group \( G \) such that \( R_{h,A_1}^{(1)}(n) = R_{h,A_2}^{(1)}(n) \) for every \( g \in G \).

Of course it is still an open question that there exists a Sidon set which is asymptotic basis of order 3 or not. J. Cilleruelo showed that the modular version of this conjecture true, namely for all large enough \( N \), the cyclic group \( \mathbb{Z}_N \) contains a Sidon set \( S \subset \mathbb{Z}_N \) which is an asymptotic basis of order 3 in \( \mathbb{Z}_N \). So using better probabilistic construction we might be able to prove for the positive integers also. At this moment it seems to be a hard exercise.

Finally we can conclude that in this thesis we worked on interesting problems and there are several ways to continue it.

References


[Cil] J. Cilleruelo, Sidon basis, *arXiv: 1304.5351*


[RoSa14] E. Rozgonyi, Cs. Sándor: An extension of a Nathanson’s Theorem, *Combinatorica*, accepted


