Department of Mathematics and Systems Analysis

# Real Algebraic Geometry in Additive Number Theory

Erik Sjöland

Aalto University

DOCTORAL DISSERTATIONS

Aalto University publication series
**DOCTORAL DISSERTATIONS** 162/2014

# Real Algebraic Geometry in Additive Number Theory

**Erik Sjöland**

A doctoral dissertation completed for the degree of Doctor of Science in Technology to be defended, with the permission of the Aalto University School of Science, at a public examination held in lecture hall D at Otsvängen 1, Otnäs, on 28 November 2014 at 13:00.

**Aalto University**
**School of Science**
**Department of Mathematics and Systems Analysis**

**Supervising professor**
Prof. Alexander Engström

**Thesis advisor**
Prof. Alexander Engström

**Preliminary examiners**
Prof. Markus Schweighofer
Universität Konstanz
Germany

Prof. Cynthia Vinzant
University of Michigan
United States

**Opponents**
Prof. Raman Sanyal
Freie Universität Berlin
Germany

Aalto University publication series
**DOCTORAL DISSERTATIONS** 162/2014



ISBN 978-952-60-5913-6 (printed)
ISBN 978-952-60-5914-3 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)
http://urn.fi/URN:ISBN:978-952-60-5914-3

Unigrafia Oy
Helsinki 2014

Finland

441 697
Printed matter

Aalto University

# Abstract

Aalto University, P.O. Box 11000, FI-00076 Aalto www.aalto.fi

**Author**
Erik Sjöland

**Name of the doctoral dissertation**
Real Algebraic Geometry in Additive Number Theory

**Publisher** School of Science

**Unit** Department of Mathematics and Systems Analysis

**Series** Aalto University publication series DOCTORAL DISSERTATIONS 162/2014

**Field of research** Mathematics

**Manuscript submitted** 8 August 2014 **Date of the defence** 28 November 2014

**Permission to publish granted (date)** 20 October 2014 **Language** English

☐ **Monograph** ☒ **Article dissertation (summary + original articles)**

**Abstract**

During the last decade new techniques have been developed in order to solve polynomial optimization problems that are invariant under the action of a group using semidefinite programming. In this thesis we apply these methods to additive number theory. In particular we set up a novel machinery for counting arithmetic progressions using real algebraic geometry. We prove several new results related to Szemerédi's theorem. We prove results for arithmetic progressions of length 3 that one has not been able to prove using Fourier analytic methods or ergotic theory, which are the most commonly used tools in additive number theory. Instead of trying to prove existence of arithmetic progressions we do the most natural generalization: we count them. To our knowledge we give the first results on the form "There are at least W(k,G,d) arithmetic progressions of length k in any subset S of the elements of G with |S|=|G|d.", and we discuss how our results could possibly be improved in order to give a new proof of Szemerédi's theorem using real algebraic geometry. A similar type of results are theorems on the form "There are at least R(k,G,c) monochromatic arithmetic progressions of length k in any c-coloring of the finite group G.". There are many theorems of this type for 2-colorings, and we prove several new results in this thesis. Some of the new results hold for any finite group G, including non-abelian groups, which are very difficult to analyze using Fourier analytic methods.

**Keywords** Real algebraic geometry, additive number theory, arithmetic progressions, semidefinite programming

**ISBN (printed)** 978-952-60-5913-6 **ISBN (pdf)** 978-952-60-5914-3

**ISSN-L** 1799-4934 **ISSN (printed)** 1799-4934 **ISSN (pdf)** 1799-4942

**Location of publisher** Helsinki **Location of printing** Helsinki **Year** 2014

**Pages** 161 **urn** http://urn.fi/URN:ISBN:978-952-60-5914-3

Aalto-universitetet

# Sammandrag

**Aalto-universitetet, PB 11000, 00076 Aalto** www.aalto.fi

**Författare**
Erik Sjöland

**Doktorsavhandlingens titel**
Reell algebraisk geometri i additiv talteori

**Utgivare** Högskolan för teknikvetenskaper

**Enhet** Institutionen för matematik och systemanalys

**Seriens namn** Aalto University publication series DOCTORAL DISSERTATIONS 162/2014

**Forskningsområde** Matematik

**Inlämningsdatum för manuskript** 08.08.2014 **Datum för disputation** 28.11.2014

**Beviljande av publiceringstillstånd (datum)** 20.10.2014 **Språk** Engelska

☐ **Monografi** ☒ **Sammanläggningsavhandling (sammandrag plus separata artiklar)**

**Sammandrag**

Under det senaste årtiondet har nya metoder utvecklats för att lösa polynoma optimeringsproblem som är invarianta under gruppverkan genom att använda semidefinit optimering. I den här avhandlingen använder vi de här metoderna för att lösa problem från additiv talteori. Mer specifikt utvecklar vi nya metoder för att räkna aritmetiska talföljder genom att använda oss av reell algebraisk geometri. Vi bevisar flera nya resultat relaterade till Szemerédis sats. Vi har nya resultat för aritmetiska talföljder av längd tre, vilka inte har bevisats med Fourier-analytiska metoder eller ergodisk teori, de mest använda metoderna i additiv talteori. Istället för att försöka visa existensen av aritmetiska talföljder så gör vi den mest naturliga generaliseringen: vi räknar dem. Så vitt vi vet ger vi de första resultaten på formen ″Det finns åtminstone W(k,G,d) aritmetiska talföljder av längd k i alla olika delmängder S av elementen i den ändliga gruppen G där |S| = |G|d.″. Vi diskuterar hur våra resultat eventuellt kan förbättras för att ge ett nytt bevis av Szemerédis sats baserat på reell algebraisk geometri. Liknande resultat är satser på formen ″Det finns åtminstone R(k,G,c) enfärgade aritmetiska talföljder av längd k i alla olika c-färgningar av den ändliga gruppen G.″. Det finns många satser av den här typen för två-färgningar, och vi bevisar flera nya resultat i den här avhandlingen. Vissa av våra resultat håller för alla olika ändliga grupper G, även för icke-abelska grupper, vilka är väldigt svåra att analysera med Fourier-analytiska metoder.

**Nyckelord** Reell algebraisk geometri, additiv talteori, aritmetiska talföljder, semidefinit optimering

| | | |
|---|---|---|
| **ISBN (tryckt)** 978-952-60-5913-6 | **ISBN (pdf)** 978-952-60-5914-3 | |
| **ISSN-L** 1799-4934 | **ISSN (tryckt)** 1799-4934 | **ISSN (pdf)** 1799-4942 |
| **Utgivningsort** Helsingfors | **Tryckort** Helsingfors | **År** 2014 |
| **Sidantal** 161 | **urn** http://urn.fi/URN:ISBN:978-952-60-5914-3 | |

# Preface

I am extremely grateful for all of the guidance my thesis supervisor Alexander Engström has provided me. He is extremely knowledgeable and has with patience taught me a great deal of mathematics. Without his support and tremendous optimism throughout these years I honestly don't know if I would have finished this thesis. I am certain that our close friendship will last for many years to come.

I am very grateful to my opponent Raman Sanyal for taking the time to come to Helsinki to attend my defense. I want to thank my pre-examiners Cynthia Vinzant and Markus Schweighofer for their well-motivated feedback and comments, which significantly improved the quality of my thesis. I am grateful that they put a great deal of their time to carefully examine my thesis.

I want to thank Cordian Riener for all the help I have received and all the discussions we have had. His ideas have had a huge impact on my work. Cordian is very knowledgeable, helpful and a good friend. I am deeply grateful to Oscar Kivinen for our collaboration, which might lead to further results in this direction. I also want to express my gratitude to Patrik Norén, Mathew Stamps, Jonathan Browder, Emanuele Ventura, Wouter Van Heijst, Ragnar Freij, Teemu Päkkilä, Jerri Nummenpalo, Rob Davis, Kaie Kubjas and all other friends who have inspired and motivated me during my time in Finland. You all mean a great deal to me.

Finally, I want to thank my family for their support and unconditional love. Christel, my parents Magnus and Barbro, and my brothers Anders and Patrik bring joy and happiness to my life and have always been there for me, even through the toughest times. Without them life wouldn't be the same.

Helsinki, October 16, 2014,

Erik Sjöland

# Contents

# List of Publications

This thesis consists of an overview and of the following publications which are referred to in the text by their Roman numerals.

**I** Erik Sjöland. Enumeration of monochromatic three term arithmetic progressions in two-colorings of cyclic groups. *arxiv:1408.1058*, 15 Pages, 2014.

**II** Erik Sjöland. Enumeration of monochromatic three term arithmetic progressions in two-colorings of any finite group. *arxiv:1408.1088*, 16 Pages, 2014.

**III** Erik Sjöland. Enumeration of three term arithmetic progressions in fixed density sets. *arxiv:1408.1063*, 62 Pages, 2014.

**IV** Erik Sjöland. Using real algebraic geometry to solve combinatorial problems with symmetries. *arxiv:1408.1065*, 29 Pages, 2014.

# Author's Contribution

**Publication I: "Enumeration of monochromatic three term arithmetic progressions in two-colorings of cyclic groups"**

The author did everything in this publication.

**Publication II: "Enumeration of monochromatic three term arithmetic progressions in two-colorings of any finite group"**

The author did everything in this publication.

**Publication III: "Enumeration of three term arithmetic progressions in fixed density sets"**

The author did everything in this publication.

**Publication IV: "Using real algebraic geometry to solve combinatorial problems with symmetries"**

The author did everything in this publication.

# Abbreviations and Notation

$\mathbb{R}[x] = \mathbb{R}[x_1, \ldots, x_n]$ denotes the set of all polynomials in the variables $x_1, \ldots, x_n$.

$\deg(f)$ denotes the degree of a polynomial $f \in \mathbb{R}[x]$.

*LMI* is short for linear matrix inequality, and we use the symbol $\succeq$ for linear matrix inequalities.

*LP* is short for linear programming.

*SDP* is short for semidefinite programming.

$\phi(k)$ denotes the Euler phi function; $\phi(k) = |\{t \in \{1, \ldots, k\} : t, k \text{ coprime}\}|$.

$\mathrm{orb}(x)$ denotes the *orbit* through $x$: $\mathrm{orb}(x) = \{g \cdot x | g \in G\}$.

$G_x$ denotes the *stabilizer* of $x$; $G_x = \{g \in G | g \cdot x = x\}$.

The *conjugacy class* containing $g \in G$ is denoted $\mathrm{Cl}(g)$.

The *centralizer* of $g$ is denoted $C_G(g)$.

The set of the first $n$ positive integers are usually denoted $[n] = \{1, \ldots, n\}$.

The *symmetric group of degree* $n$ is denoted $S_n$.

If $V$ and $W$ are vector spaces then *the set of all* $\mathbb{C}$*-linear maps* $V \to W$ is denoted $Hom_{\mathbb{C}}(V, W)$. When $V = W$ we write $End_{\mathbb{C}}(V) = Hom_{\mathbb{C}}(V, V)$.

The *automorphism group* of a vector space $V$ is denoted $Aut(V)$.

$M_n(\mathbb{C})$ denotes the set of all $n \times n$ matrices.

$GL(n, \mathbb{C})$, *the general linear group*, denotes the set of all invertible $n \times n$ matrices.

The *trace of* $A$ is denoted $\mathrm{tr}(A)$.

The *inner product* of $x$ and $y$ is denoted $\langle x, y \rangle$.

The *dimension* of a representation is denoted $\dim V$.

The *principal representation* is denoted $1_G$.

$\ker f$ denotes the kernel of $f$.

$\mathrm{im}\ f$ denotes the image of $f$.

We denote the set of $G$-morphism from $V_1$ to $V_2$ by $Hom_G(V_1, V_2)$, and in the case when $V_1 = V_2 = V$ we write $End_G(V) = Hom_G(V, V)$.

The *character* of a representation $\Theta : G \to Aut(V)$ is denoted $\chi$. $\chi$ is also called the character of $V$, and is occasionally denoted $\chi_V$.

We denote the set of all irreducible characters of $G$ by $Irr(G)$.

The number of elements in a group $G$ is denoted $|G|$.

*co-lex order* is the abbreviation of co-lexicographic order, which means that strings are sorted by increasing value of their last symbol.

The *crossing number* of a graph $G$ is denoted $\mathrm{cr}(G)$.

The *kissing number* in $n$-dimensional Euclidean space is denoted $\tau_n$.

The *(upper) density* of a set $S \subseteq \mathbb{N}$ is denoted $\rho(S)$.

$W(k, G, \delta)$ denotes the minimal number of arithmetic progressions of length $k$ in any set $S \subset G$ with $|S| = |G|\delta$ of the finite group $G$.

$R(k, G, c)$ denotes the minimal number of monochromatic arithmetic progressions of length $k$ in any $c$-coloring of the finite group $G$.

We denote by $N(k, \delta)$ the smallest positive integer such that any subset of $\{1, \ldots, N(k, \delta)\}$ of cardinality $\delta N(k, \delta)$ contains an arithmetic progression of length $k$.

$\delta(N, k)$ denotes the smallest density such that any subset of $\{1, \ldots, N\}$ of cardinality $\delta(N, k)N$ contains an arithmetic progression of length $k$.

$h(x) = o(f(x))$ is equivalent to that $\frac{h(x)}{f(x)} \to 0$ as $x \to \infty$ and $g(x) = O(f(x))$ to that $\frac{f(x)}{g(x)} \to 0$ as $x \to \infty$ for polynomials $f(x), g(x), h(x)$.

$a \uparrow b$ denotes $a^b$, $a \uparrow b \uparrow c$ denoted $a^{b^c} = a^{(b^c)}$.

$\sigma(a; b_0, b_1, \ldots, b_{n-1})$ is compact notation for $a + \sum_{i,j \in \mathbb{Z}_n} b_{j-i} x_i x_j$.

# 1. Introduction

## 1.1 Introduction to invariant semidefinite programming

Semidefinite programming dates back to the 1960s, and is closely linked to real algebraic geometry by the connections between sums of squares and positive semidefinite matrices. Starting with Hilbert's 17th problem, which asks if a positive polynomial can be written as a sum of squares of rational functions and which was affirmed by Artin in 1927, several sum of squares based certificates have been developed to guarantee positivity of a polynomial $f$ on a basic closed semialgebraic set $K$. Some important contributions includes the Positivstellensätze by Krivine, Stengle, Schmüdgen and Putinar. Both Schmüdgen's and Putinar's Positivstellensätze are very useful in practice since they can be relaxed by bounding the degrees to find lower bounds of $f$ using an optimization problem on the form $\max\{\lambda : f - \lambda = \text{relaxed certificate of positivity}\}$. With Schmüdgens and Putinar's Positivstellensätze the certificates are of a form such that the optimization problem is a semidefinite program. The duals to these problems are known to be within a special instance of the generalized moment problem. A hierarchy of relaxations to the primal and dual problems is already known, and is referred to as the Lasserre hierarchy.

In the case when the semidefinite optimization problems arising from the relaxation of Putinar's Positivstellensatz are invariant under the actions of a group we can use ideas from representation theory to reduce the dimension of the problem. Sometimes a block diagonalization is possible to further simplify the problem. Inspired by de Klerk, Pasechnik and Schrijver we use methods from representation theory to simplify the problem.

Many combinatorial problems can be formulated as invariant semidefi-

nite programs, and the best known bounds to many problems have been obtained in this way. We show how the methods can be applied to count arithmetic progressions, and provide several novel results.

## 1.2 Introduction to arithmetic progressions

One of the most challenging problems in additive number theory is to determine the existence of arithmetic progressions in fixed density sets of the integers. The first major contribution was when Roth in 1953 showed, using exponential sums, that arithmetic progressions of length 3 exist in any subset of the integers with positive density. In 1969 Szemerédi proved the existence of arithmetic progressions of length 4, and in 1975 he generalized the result and proved that subsets of integers with positive density will contain arbitrary long arithmetic progressions. This theorem is one of the most important theorems in combinatorics; nevertheless, the proof is extremely complicated and does not provide a satisfactory lower bound $N = N(k, \delta)$ such that $S \cap \{1, \dots, N\}$ contains an arithmetic progression of length $k$ when $|S \cap \{1, \dots, N\}| = \delta N$. Using ergodic theory, Furstenberg gave a new proof of Szemerédi's theorem in 1977. The proof is much simpler, but does not provide better bounds. By generalizing Roth's idea, Gowers gave a third proof in 2001. Gowers lower bound for $N$ is the current optimal bound, which is doubly exponential in $\delta^{-1}$ and quintuply exponential in $k$. The bounds when $k = 3$ and $k = 4$ are much sharper than the results for general $k$, but it seems almost impossible to use any of these methods to get better bounds for $k \geq 5$. All the mentioned results were extremely difficult to prove, and to prove them a lot of Fourier analytic methods were developed. On the strength of these results and methods all the mentioned authors have been awarded with honorable prizes, including the Fields medal and Abel prize.

Similar results hold for arithmetic progressions in $\mathbb{Z}_n$, and results for other abelian groups can be carried out using Fourier-analytic methods. But the methods do not apply in a non-abelian setting, and hence very little is known about arithmetic progressions in non-abelian groups.

In combinatorial problems the ultimate goal is always to count, and results about existence is a first step that provides an understanding in various limits when counting. Let $R(k, G, c)$ denote the minimal number of monochromatic $k$-arithmetic progressions in a $c$-coloring of a finite group $G$, and let $W(k, G, \delta)$ denote the minimal number of $k$-arithmetic

progressions in any subset $S$ of $G$ with $|S| = \delta|G|$. Szemerédi's theorem is equivalent to that for any fixed $k \geq 3$ we have that $\lim_{n\to\infty} \min\{\delta : W(k, \mathbb{Z}_n, \delta) > 0\} = 0$. A lot of current research is about finding upper and lower bounds for $R(k, G, c)$ and $W(k, G, \delta)$ for various inputs, and in this thesis we provide several new results. It would be a major achievement if one could find a lower bound to $W(k, \mathbb{Z}_n, \delta)$ that additionally implies Szemerédi's theorem. We discuss why such bound is theoretically possible due to Putinar's positivstellensatz, and discuss the possibilities and limitations in practice when the proposed methods are implemented.

## 1.3 Methods

In this thesis we develop methods that can count monochromatic arithmetic progressions of length $k$ in a 2-coloring of any finite group. Further we develop methods that can count $k$-arithmetic progressions in any subset of a finite group, which directly provides lower bounds for $c$-colorings. These methods are applicable to any group, including non-abelian groups.

An arithmetic progression in $G$ of length $k$ is a set of $k$ distinct element $\{a, b \cdot a, \ldots, b^{k-1} \cdot a\}$ where $a \in G$ and $b \in G \setminus \{0\}$. Also, to clarify, when the sum is taken over all arithmetic progressions, then $\{1, 2, 3\}$, $\{1, 3, 2\}$, $\{2, 1, 3\}$, $\{2, 3, 1\}$, $\{3, 1, 2\}$ and $\{3, 2, 1\}$ denote the same set and hence to avoid double counting we only use one representative.

To count monochromatic arithmetic progressions in a 2-coloring $\chi : G \to \{-1, 1\}$, let $x_g = \chi(g)$ and $f_{a,b,\chi,k}$ equal

$$\frac{(1 + x_a)(1 + x_{b\cdot a}) \cdots (1 + x_{b^{k-1}\cdot a}) + (1 - x_a)(1 - x_{b\cdot a}) \cdots (1 - x_{b^{k-1}\cdot a})}{2^k}.$$

Note that $f_{a,b,\chi,k} = 1$ if the $k$-arithmetic progression is monochromatic under the coloring $\chi$ and $f_{a,b,\chi,k} = 0$ if it is not. In other words, counting monochromatic arithmetic progressions can be translated into evaluating polynomials. In particular

$$R(k, G, 2) = \min_{\chi} \sum_{\{a, b\cdot a, \ldots, b^{k-1}\cdot a\}} f_{a,b,\chi,k}$$

where the sum is over all $k$-arithmetic progressions.

To count arithmetic progressions in a subset $S \subseteq G$ let $x_g = 1$ if $g \in S$ and $x_g = 0$ otherwise. It follows that the monomial $x_a x_{b\cdot a} \cdots x_{b^{k-1}\cdot a}$ is one

if $a, b \cdot a, \ldots, b^{k-1} \cdot a \in S$ and zero otherwise. In particular

$$W(k, G, \delta) = \min_{x \in \{0,1\}^{|G|}} \{ \sum_{\{a, b\cdot a, \ldots, b^{k-1}\cdot a\}} x_a x_{b\cdot a} \cdots x_{b^{k-1}\cdot a} : \sum_{g \in G} x_g = \delta |G| \}$$

where the sum is over all $k$-arithmetic progression.

The goal is to find as sharp and as general lower bounds as possible for $R(k, G, 2)$ and $W(k, G, \delta)$. To find lower bounds we use a combination of results from real algebraic geometry, including Putinar's Positivstellensatz and the Lasserre hierarchy, to reduce the problem to a semidefinite programming problem. To solve the semidefinite programming problem we first reduce the size of the problem using methods from representation theory. From the semidefinite programming problem we get numerical lower bounds to $R(k, G, 2)$ and $W(k, G, \delta)$ for groups of low order, which through hard work can be turned into algebraic certificates for infinite families of groups in some cases.

# 2. Summaries of Publications

## 2.1 Summary of Publication I

In this publication we develop methods based on real algebraic geometry to find lower bounds for the minimal number of monochromatic arithmetic progressions of length $3$ in a $2$-coloring of cyclic groups, $R(3, \mathbb{Z}_n, 2)$. We also find good colorings for the cyclic groups, providing upper bounds for $R(3, \mathbb{Z}_n, 2)$. The lower and upper bounds we find are in many cases equal, and in other cases they differ by a constant. We list the main theorem of Publication I, and a corollary that follows:

The case $n \mod 24 \in \{1, 5, 7, 11, 13, 17, 19, 23\}$ had previously been shown by Cameron, Cilleruelo and Serra in 2007. Their methods are purely combinatorial and the other cases cannot be obtained by those methods. All other cases are new.

**Theorem 2.1.1.** *Let $n$ be a positive integer and let $R(3, \mathbb{Z}_n, 2)$ denote the minimal number of monochromatic 3-term arithmetic progressions in any two-coloring of $\mathbb{Z}_n$. $n^2/8 - c_1 n + c_2 \leq R(3, \mathbb{Z}_n, 2) \leq n^2/8 - c_1 n + c_3$ for all values of $n$, where the constants depends on the modular arithmetic and*

*are tabulated in the following table.*

| $n \mod 24$ | $c_1$ | $c_2$ | $c_3$ |
|---|---|---|---|
| $1, 5, 7, 11, 13, 17, 19, 23$ | $1/2$ | $3/8$ | $3/8$ |
| $8, 16$ | $1$ | $0$ | $0$ |
| $2, 10$ | $1$ | $3/2$ | $3/2$ |
| $4, 20$ | $1$ | $0$ | $2$ |
| $14, 22$ | $1$ | $3/2$ | $3/2$ |
| $3, 9, 15, 21$ | $7/6$ | $3/8$ | $27/8$ |
| $0$ | $5/3$ | $0$ | $0$ |
| $12$ | $5/3$ | $0$ | $18$ |
| $6, 18$ | $5/3$ | $1/2$ | $27/2$ |

It requires little work to see that the following result follows:

**Corollary 2.1.2.** *Let $n$ be a positive integer. Let $R(3, \mathbb{Z}_n, 2)$ and $R(3, D_{2n}, 2)$ denote the minimal number of monochromatic $3$-term arithmetic progressions in any two-coloring of $\mathbb{Z}_n$ and $D_{2n}$ respectively. The following equality holds*

$$R(3, D_{2n}, 2) = 2R(3, \mathbb{Z}_n, 2).$$

*In particular $n^2/4 - 2c_1 n + 2c_2 \leq R(D_{2n}; 3) \leq n^2/4 - 2c_1 n + 2c_3$ where the constants can be found in the table of Theorem 2.1.1.*

## 2.2 Summary of Publication II

In this publication we develop methods based on real algebraic geometry to find lower bounds for the minimal number of monochromatic arithmetic progressions of length $3$ in a $2$-coloring of finite groups, $R(3, G, 2)$. The lower bounds we find holds for any finite group $G$, including non-abelian groups. We present the main result of Publication II.

The theorem holds for any finite group $G$, including non-abelian groups for which very little is known about arithmetic progressions. The only information that is needed to get a lower bound for a specific group $G$ is the number of elements of the different orders of $G$. The lower bound is sharp for some groups, for example $\mathbb{Z}_p$ with $p$ prime, but is not optimal for most groups. Lower bounds were previously just known for a few specific groups, for example lower bounds for cyclic groups whose order is coprime to six was found by Cameron, Cilleruelo and Serra in 2007, but the author has not been able to find any theorem of this generality in the literature.

**Theorem 2.2.1.** *Let $G$ be any finite group and let $R(3, G, 2)$ denote the minimal number of monochromatic 3-term arithmetic progressions in any two-coloring of $G$. Let $G_k$ denote the set of elements of $G$ of order $k$, $N = |G|$ and $N_k = |G_k|$. Denote the Euler phi function $\phi(k) = |\{t \in \{1, \ldots, k\} : t \text{ and } k \text{ are coprime}\}|$. Let $K = \{k \in \{5, \ldots, n\} : \phi(k) \geq \frac{3k}{4}\}$. For any $G$ there are $\sum_{k=4}^{n} \frac{N \cdot N_k}{2} + \frac{N \cdot N_3}{6}$ arithmetic progressions of length 3. At least*

$$R(3, G, 2) \geq \sum_{k \in K} \frac{N \cdot N_k}{8}(1 - 3\frac{k - \phi(k)}{\phi(k)}).$$

*of them are monochromatic in a 2-coloring of $G$.*

## 2.3 Summary of Publication III

In this paper we are interested in quantifying how many arithmetic progressions there are in any subset $S$ of $\mathbb{Z}_n$ of cardinality $D = |S|$. We let $W(k, \mathbb{Z}_n, D/n)$ denote the minimal number of arithmetic progressions of length $k$ in any of the subsets $S \subset \mathbb{Z}_n$ of cardinality $|D|$.

We begin the study by considering small examples, and use a bubble language to quickly run through all subsets of a given density in a given cyclic group $\mathbb{Z}_n$ with $n \leq 32$. The results are tabulated in an appendix of the article.

Going through all possible fixed sets of a given density is not possible for larger cyclic groups, and thus we need to use other methods to get results for higher $n$. Using methods based on real algebraic geometry we find the first results that holds for any prime $p$. The paper also contains a discussion how it might be possible to improve on the results. When doing so, if the sharper bounds are strong enough a generalization of the famous theorem by Szémeredi would follow. Even though it is theoretically possible to achieve such bounds, it might not be possible in practice with these methods as the problem is very complicated. One of the main results of the paper is the following theorem:

**Theorem 2.3.1.** *Let $p$ be prime. A lower bound to*

$$W(3, \mathbb{Z}_p, D/p) = \min\{\sum_{\{i,j,k\} \text{ A.P. in } \mathbb{Z}_p} x_i x_j x_k : x_i \in \{0, 1\}, \sum_{i=0}^{p-1} x_i = D\}$$

*is*

$$\lambda = \frac{D^3 - (\frac{p+3}{2})D^2 + (\frac{p+3}{2} - 1)D}{p - 1}.$$

*A certificate for the lower bound is given by:*

$$\sum_{\{i,j,k\}\ \textit{A.P. in}\ \mathbb{Z}_p} X_iX_jX_k - \lambda = \sum_{i=0}^{p-1}\sigma_{1,i}X_i + \sum_{i=0}^{p-1}\sigma_{2,i}X_i + \sigma_3(D - \sum_{i=0}^{p-1}X_i^3) + \sigma_4(\sum_{i\neq j}X_i^2X_j - D(D-1)),$$

*where*

$$\sigma_{1,i} = \frac{1}{p-1}\sum_{0<j<k<(p-1)/2}(X_{j+i} - X_{j+k+i} - X_{n-j-k+i} + X_{n-j+i})^2$$

$$\sigma_{2,i} = \frac{1}{p-1}(DX_i - \sum_{j=0}^{p-1}X_j)^2$$

$$\sigma_3 = \frac{(D-1)^2}{p-1}$$

$$\sigma_4 = \frac{4D-p+3}{2(p-1)}.$$

In fact, finding bounds sharper than those in Theorem 2.3.1 can be done very efficiently for relatively small primes using a simple degree 3 relaxation. As shown in the following theorem we can reformulate a certain relaxation as a linear program:

**Theorem 2.3.2.** *Let $r$ be a primitive root of the prime $p$. Let further*

$$V_{ij} = \left|\left\{\{0,1,r^i\} : \{0,1,r^i\} = \{0,r^t,r^{j+t}\}\ \textit{for}\ t = 0,\ldots,p-2\right\}\right|$$

*for all $i,j \in \{0,\ldots,p-1\}$,*

$$C_{ij} = cos(\frac{2\pi(i-1)(j-1)}{p-1})$$

*for all $i,j \in \{0,\ldots,p-1\}$*

$$u = [u_0, u_1, \ldots, u_{\frac{p-3}{2}}, u_{\frac{p-1}{2}}, u_{\frac{p-3}{2}}, \ldots, u_1]^T,$$

$$u_+ = 1^Tu = u_0 + 2u_1 + \cdots + 2u_{(p-3)/2} + u_{(p-1)/2}$$

*and*

$$v_i = \begin{cases} 1 & \textit{if}\ r^i = 2 \\ 0 & \textit{otherwise.} \end{cases}$$

*for $i \in \{0,\ldots,p-1\}$.*

*The following optimization problems attain the same optimal value:*

*(a)*

$$\max\{\lambda : \sum_{\{i,j,k\} \text{ A.P. in } \mathbb{Z}_p} X_i X_j X_k - \lambda = S\}$$

*where*

$$\begin{aligned} S = & \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(\sum_{k=1}^{p-1} a_{ijk}X_k)^2 X_i + b\sum_{i=0}^{p-1}(DX_i - \sum_{j=0}^{p-1} X_j)^2 X_i \\ & + c(\sum_{i=0}^{p-1} X_i^3 - D) + d(\sum_{i,j} X_i^2 X_j - D(D-1)) \end{aligned}$$

*for* $a_{ijk}, c, d \in \mathbb{R}$ *and* $b \geq 0$.

*(b)*

$$\max\{\frac{u_+}{p-1}(D-1-\frac{u_0}{u_+}(p-1))D(D-1) : Cu \geq 0, Vu = v\}.$$

Next we provide algebraic certificates for lower bounds to $W(3, \mathbb{Z}_p, D/p)$ for some small primes, which follow from 2.3.2. The reason we can find nice algebraic bounds for $p \leq 17$ has to do with that the trigonometric functions in Theorem 2.3.2 are on a nice form. It would be possible to find algebraic certificates for slightly larger $p$, but it would require more work and the bounds would contain messy combinations of trigonometric functions.

**Theorem 2.3.3.** *There are algebraic certificates with polynomials up to degree 3 giving the following bounds*

$$W(3, \mathbb{Z}_5, D/5) \geq \frac{D^3 - 3D^2 + 2D}{6},$$

$$W(3, \mathbb{Z}_7, D/7) \geq \frac{D^3 - 4D^2 + 3D}{8},$$

$$W(3, \mathbb{Z}_{11}, D/11) \geq \frac{\sqrt{5}D^3 + (15 - 12\sqrt{5})D^2 + (-15 + 11\sqrt{5})D}{30},$$

$$W(3, \mathbb{Z}_{13}, D/13) \geq \frac{21 - 2\sqrt{3}}{286}D^3 + \frac{28\sqrt{3} - 151}{286}D^2 + \frac{5 - \sqrt{3}}{11}D$$

*and*

$$W(3, \mathbb{Z}_{17}, D/17) \geq \frac{1}{24}D^3 - \frac{1}{4}D^2 + \frac{5}{24}D.$$

As is shown in the paper (Proposition 2.4 in Publication III) it follows by

Szemerédi's theorem that

$$\lim_{n\to\infty} \min\{\delta \in \mathbb{R}_{>0} : W(k, \mathbb{Z}_n, \delta) > 0\} = 0.$$

The following corollary which follows from Theorem 2.3.1 and Theorem 2.3.2 shows that there is room to improve the bounds further.

**Corollary 2.3.4.** *Let $p$ be prime, and denote the optimal solution to problem (a) in Theorem 2.3.2 by $\lambda_p(D)$;*

$$\lambda_p(D) = \max\{\lambda : \sum_{\{i,j,k\} \text{ A.P. in } \mathbb{Z}_p} X_i X_j X_k - \lambda = S\}$$

*where*

$$\begin{aligned} S = \; & \sum_{i=0}^{p-1}\sum_{j=0}^{p-1}(\sum_{k=1}^{p-1} a_{ijk}X_k)^2 X_i + b\sum_{i=0}^{p-1}(DX_i - \sum_{j=0}^{p-1} X_j)^2 X_i \\ & + c(\sum_{i=0}^{p-1} X_i^3 - D) + d(\sum_{i,j} X_i^2 X_j - D(D-1)) \end{aligned}$$

*for $a_{ijk}, c, d \in \mathbb{R}$ and $b \geq 0$. For all $p$*

$$\left\lceil \frac{p+3}{4} \right\rceil \leq \min\{D \in \mathbb{Z}_+ : \lambda_p(D) > 0\} \leq \frac{p+3}{2}$$

It is highly non-trivial to find lower bounds for $W(k, \mathbb{Z}_p, D/p)$ that generalizes Szemerédi's theorem even for $k = 3$. In Publication III we discuss how the problem of finding a sharper lower bound can be approached for arithmetic progressions of length $3$ as well as for longer arithmetic progressions.

## 2.4 Summary of Publication IV

In Publication IV we explain the methods we developed to prove the results in Publication I, Publication II and Publication III. These methods are applicable to other combinatorial problems as well, so in the article we aim to keep the methods as general as possible not to exclude any possible applications. The article includes an extensive survey of how a polynomial optimization problem can be solved using semidefinite programming. The article further explores the theory of sums of squares, and gives an overview of several Positivstellensätze that are useful for polynomial optimization problems. It is also discussed how a polynomial

optimization problem can be solved using the theory of moments, and how this is dual to a sum of squares based approach.

Further, it is discussed how symmetries in the problem can be exploited to reduce the size of the problem, and we highlight seven recent contributions in which symmetry reduction has been used to improve results in combinatorial problems through semidefinite programming.

The article discuss implementation of a polynomial optimization problem. Through a 3-step procedure the article highlights the main challenges of implementing the code. Through an example it is possible to see how to make a degree 3-relaxation of the polynomial optimization problem, and the computational limitations are discussed.

Aalto-DD 162/2014

ISBN 978-952-60-5913-6 (printed)
ISBN 978-952-60-5914-3 (pdf)
ISSN-L 1799-4934
ISSN 1799-4934 (printed)
ISSN 1799-4942 (pdf)

**Aalto University**
**School of Science**
**Department of Mathematics and Systems Analysis**
**www.aalto.fi**

BUSINESS +
ECONOMY

ART +
DESIGN +
ARCHITECTURE

SCIENCE +
TECHNOLOGY

CROSSOVER

**DOCTORAL
DISSERTATIONS**