Higher-order Fourier Analysis and Applications

Other titles in Foundations and Trends® in Theoretical Computer Science

Coding for Interactive Communication: A Survey
Ran Gelles
ISBN: 978-1-68083-346-1

Hashing, Load Balancing and Multiple Choice
Udi Wieder
ISBN: 978-1-68083-282-2

Scalable Algorithms for Data and Network Analysis
Shang-Hua Teng
ISBN: 978-1-68083-130-6

Communication Complexity (for Algorithm Designers)
Tim Roughgarden
ISBN: 978-1-68083-114-6

Quantum Proofs
Thomas Vidick and John Watrous
ISBN: 978-1-68083-126-9

Higher-order Fourier Analysis and Applications

Hamed Hatami
McGill University
hatami@cs.mcgill.ca

Pooya Hatami
Ohio State University
pooyahat@gmail.com

Shachar Lovett
UC San Diego
slovett@cs.ucsd.edu

the essence of knowledge
Boston — Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

H. Hatami, P. Hatami and S. Lovett. *Higher-order Fourier Analysis and Applications*. Foundations and Trends® in Theoretical Computer Science, vol. 13, no. 4, pp. 247–448, 2019.

ISBN: 978-1-68083-593-9

Editorial Scope

Topics

Foundations and Trends® in Theoretical Computer Science publishes survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians

Foundations and Trends® in Theoretical Computer Science, 2019, Volume 13, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Contents

Higher-order Fourier Analysis and Applications

Hamed Hatami[1], Pooya Hatami[2] and Shachar Lovett[3]

[1] *McGill University; hatami@cs.mcgill.ca*

[2] *Ohio State University; pooyahat@gmail.com*

[3] *University of California, San Diego; slovett@cs.ucsd.edu*

ABSTRACT

Fourier analysis has been extremely useful in many areas of mathematics. In the last several decades, it has been used extensively in theoretical computer science. Higher-order Fourier analysis is an extension of the classical Fourier analysis, where one allows to generalize the “linear phases” to higher degree polynomials. It has emerged from the seminal proof of Gowers of Szemerédi’s theorem with improved quantitative bounds, and has been developed since, chiefly by the number theory community. In parallel, it has found applications also in theoretical computer science, mostly in algebraic property testing, coding theory and complexity theory.

The purpose of this book is to lay the foundations of higher-order Fourier analysis, aimed towards applications in theoretical computer science with a focus on algebraic property testing.

Hamed Hatami, Pooya Hatami and Shachar Lovett (2019), “Higher-order Fourier Analysis and Applications”, Foundations and Trends® in Theoretical Computer Science: Vol. 13, No. 4, pp 247–448. DOI: 10.1561/0400000064.

1

Introduction

The purpose of this text is to provide an introduction to the field of higher-order Fourier analysis with an emphasis on its applications to theoretical computer science. Higher-order Fourier analysis is an extension of the classical Fourier analysis. It was initiated by a seminal paper of Gowers [37] on a new proof for Szemerédi's theorem, and has been developed by several mathematicians over the past few decades in order to study problems in an area of mathematics called additive combinatorics, which is primarily concerned with linear patterns such as arithmetic progressions in subsets of integers. While most of the developments in additive combinatorics were focused on the group $\mathbb{Z}$, it was quickly noticed that the analogous questions and results for the group $\mathbb{F}_2^n$ are of great importance to theoretical computer scientists as they are related to basic concepts in areas such as property testing and coding theory.

Classical Fourier analysis is a powerful tool that studies functions by expanding them in terms of the Fourier characters, which are "linear phase functions" such as $n \mapsto e^{-\frac{2\pi i}{N}n}$ for the group $\mathbb{Z}_N$, or $(x_1, \ldots, x_n) \mapsto (-1)^{\sum a_j x_j}$ for the group $\mathbb{F}_2^n$. Note that n and $\sum a_j x_j$ are both linear functions. Fourier analysis has been extremely successful in the study of certain linear patterns such as three-term arithmetic progressions. For example, if the number of three-term arithmetic progressions in a subset $A \subseteq \mathbb{Z}_N$ deviates from the expected number of them in a random subset of $\mathbb{Z}_N$ with the same cardinality as A, then A must have significant correlation with a linear phase function. In other words, the characteristic function of A must have a large non-principal Fourier coefficient. Roth [66] used these ideas to show that every subset of integers of positive upper density contains an arithmetic progression of length 3. However, classical Fourier analysis seems to be inadequate in detecting more complex linear patterns such as four-term or longer arithmetic progressions. Indeed, one can easily construct dense sets $A \subseteq \mathbb{Z}_N$ that do not have significant correlation with any linear phase function, and nevertheless do not contain the number of four-term arithmetic progressions that one expects by considering random subsets of the same cardinality. Hence in order to generalize Roth's theorem to arithmetic progressions of arbitrary length, Szemerédi [76, 77] departed from the Fourier analytic approach and appealed to purely combinatorial ideas. However, his proof of this major result, originally conjectured by Erdös and Turán [27], provided poor quantitative bounds on the minimal density that guarantees the existence of the arithmetic progressions of the desired length. Later Furstenberg [31] developed an ergodic-theoretic framework and gave a new proof for Szemerédi's theorem, but his proof was still qualitative. His theory is further developed by - to name a few - Host, Kra, Ziegler, Bergelson, Tao (See e.g. [51], [88], and [10, 82]), and there are important parallels between this theory and higher-order Fourier analysis. Indeed some of the terms that are commonly used in higher-order Fourier analysis such as "phase functions" or "factors" are ergodic theoretic terms.

Generalizing Roth's original proof and obtaining good quantitative bounds for Szemerédi's theorem remained a challenge until finally Gowers [37] discovered that the essential idea to overcome the obstacles described above is to consider higher-order phase functions. His proof laid the foundation for the area of higher-order Fourier analysis, where one studies a function by approximating it by a linear combination of few higher-order phase functions. Although the idea of using higher-order phase functions already appears in Gowers's work [37], it was not until more than fifteen years later that some of the major technical difficulties in achieving a satisfactory theory of higher-order Fourier analysis have been resolved. By now, due to great contributions by prominent mathematicians such as Gowers, Green, Tao, Szegedy, Host, Kra and Ziegler (See [75] and [80] and the references there), there is a deep understanding of qualitative aspects of this theory. However, despite these major breakthroughs, still very little is known from a quantitative perspective as many of the proofs are based on soft analytic techniques, and obtaining efficient bounds is one of the major challenges in this area.

This survey will emphasize the applications of the theory of higher-order Fourier analysis to theoretical computer science, and to this end, we will present the foundations of this theory through such applications, in particular to the area of property testing. In the early nineties, it was noticed by Blum *et al.* [20] and Babai *et al.* [6] that Fourier analysis can be used to design a very efficient algorithm that distinguishes linear functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ from functions that are far from being linear. This initiated the area of property testing, the study of algorithms that query their input a very small number of times and with high probability decide correctly whether their input satisfies a given property or is "far" from satisfying that property. It was soon noticed that generalizing the linearity test of Blum *et al.* [20] and Babai *et al.* [6] to other properties such as the property of being a quadratic polynomial requires overcoming the same obstacles that one faces in an attempt to generalize Fourier analytic study of three-term arithmetic progressions to four-term arithmetic progressions. Hence in parallel to additive combinatorics, theoretical computer scientists have also been working on developing tools in higher-order Fourier analysis to tackle such problems. In fact some of the most basic results, such as the inverse theorem for the Gowers U^3 norm for the group $\mathbb{F}_2^n$, were first proved by Samorodnitsky [70] in the context of property testing for quadratic polynomials.

In Part I we discuss the linearity test due to Blum *et al.* [20] and its generalization to higher degree polynomials. We will see how this naturally necessitates the development of a theory of higher-order Fourier analysis. In Part II we present the fundamental results of the theory of higher-order Fourier analysis. Since we are interested in the applications to theoretical computer science, we will only consider the group $\mathbb{F}_p^n$ where p is a fixed prime, and asymptotics are as n tends to infinity. Higher-order Fourier analysis for the group $\mathbb{Z}_N$, which is of more interest for number theoretic applications, shares the same basic ideas but differs on some technical aspects. For this group, the higher order phase functions, rather than being exponentials of polynomials, are the so called nilsequences. We refer the interested reader to Tao [80] for more details. In Part III we use the tools developed in Part II to prove some general results about property testing for algebraic properties.

Throughout most of the text, we will consider fields of constant prime order, namely $\mathbb{F} = \mathbb{F}_p$ where p is a constant, and study functions from $\mathbb{F}_p^n$ to $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{F}_p$ when n is growing. Our choice is mainly for simplicity of exposition, as there have been recent research that extend several of the tools from higher-order Fourier analysis to large or non-prime fields. We refer the interested reader to a paper by Bhattacharyya *et al.* [12] for treatment of non-prime fields. In Chapter 8 we will discuss a paper by Bhowmick and Lovett [19] considering the case $\mathbb{F}_p^n$ when p is allowed to grow as a function of n.

References

[1] Alon, N. and R. Beigel (2001). "Lower bounds for approximations by low degree polynomials over Z m". In: *Computational Complexity, 16th Annual IEEE Conference on, 2001.* IEEE. 184–187.

[2] Alon, N., E. Fischer, I. Newman, and A. Shapira (2009). "A combinatorial characterization of the testable graph properties: it's all about regularity". *SIAM J. Comput.* 39(1): 143–167. DOI: 10.1137/060667177.

[3] Alon, N., T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron (2005). "Testing Reed-Muller codes". *IEEE Trans. Inform. Theory.* 51(11): 4032–4039.

[4] Alon, N. and A. Shapira (2008a). "A Characterization of the (Natural) Graph Properties Testable with One-Sided Error". *SIAM J. on Comput.* 37(6): 1703–1727.

[5] Alon, N. and A. Shapira (2008b). "Every Monotone Graph Property Is Testable". *SIAM J. on Comput.* 38(2): 505–522.

[6] Babai, L., L. Fortnow, and C. Lund (1992). "Addendum to: "Nondeterministic exponential time has two-prover interactive protocols" [Comput. Complexity **1** (1991), no. 1, 3–40; MR1113533 (92h:68031)]". *Comput. Complexity.* 2(4): 374. DOI: 10.1007/BF01200430.

[7] Babai, L., L. Fortnow, L. A. Levin, and M. Szegedy (1991). "Checking computations in polylogarithmic time". In: *Proc. 23rd Annual ACM Symposium on the Theory of Computing*. New York: ACM Press. 21–32.

[8] Balog, A. and E. Szemerédi (1994). "A statistical theorem of set addition". *Combinatorica*. 14(3): 263–268. URL: http://dx.doi.org/10.1007/BF01212974.

[9] Bellare, M., D. Coppersmith, J. Håstad, M. Kiwi, and M. Sudan (1996). "Linearity testing over characteristic two". *IEEE Trans. Inform. Theory*. 42(6): 1781–1795.

[10] Bergelson, V., T. Tao, and T. Ziegler (2010). "An inverse theorem for the uniformity seminorms associated with the action of $\mathbb{F}_p^\infty$". *Geom. Funct. Anal.* 19(6): 1539–1596. DOI: 10.1007/s00039-010-0051-1.

[11] Bhattacharyya, A. (2014). "Polynomial decompositions in polynomial time". *Tech. rep.* http://eccc.hpi-web.de/report/2014/018. Electronic Colloquium on Computational Complexity (ECCC).

[12] Bhattacharyya, A., A. Bhowmick, and C. Gupta (2016). "On Higher-Order Fourier Analysis over Non-Prime Fields". In: *LIPIcs-Leibniz International Proceedings in Informatics*. Vol. 60. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

[13] Bhattacharyya, A., V. Chen, M. Sudan, and N. Xie (2011). "Testing linear-invariant non-linear properties". *Theory Comput.* 7: 75–99. DOI: 10.4086/toc.2011.v007a006.

[14] Bhattacharyya, A., E. Fischer, H. Hatami, P. Hatami, and S. Lovett (2013a). "Every locally characterized affine-invariant property is testable". In: *Proceedings of the 45th annual ACM symposium on Symposium on theory of computing. STOC '13*. Palo Alto, California, USA: ACM. 429–436. DOI: 10.1145/2488608.2488662.

[15] Bhattacharyya, A., E. Fischer, and S. Lovett (2013b). "Testing Low Complexity Affine-Invariant Properties". In: *Proc. 24th ACM-SIAM Symposium on Discrete Algorithms*. 1337–1355.

[16] Bhattacharyya, A., E. Grigorescu, and A. Shapira (2010a). "A Unified Framework for Testing Linear-Invariant Properties". In: *Proc. 51st Annual IEEE Symposium on Foundations of Computer Science*. 478–487.

[17] Bhattacharyya, A., P. Hatami, and M. Tulsiani (2015). "Algorithmic regularity for polynomials and applications". In: *Proceedings of the Twenty-Sixth Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2015, San Diego, CA, USA, January 4-6, 2015*. 1870–1889. DOI: 10.1137/1.9781611973730.125.

[18] Bhattacharyya, A., S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman (2010b). "Optimal testing of Reed-Muller codes". In: *2010 IEEE 51st Annual Symposium on Foundations of Computer Science FOCS 2010*. IEEE Computer Soc., Los Alamitos, CA. 488–497.

[19] Bhowmick, A. and S. Lovett (2015). "Bias vs structure of polynomials in large fields, and applications in effective algebraic geometry and coding theory". *arXiv preprint arXiv:1506.02047*.

[20] Blum, M., M. Luby, and R. Rubinfeld (1993). "Self-testing/correcting with applications to numerical problems". In: *Proceedings of the 22nd Annual ACM Symposium on Theory of Computing (Baltimore, MD, 1990)*. Vol. 47 (3). 549–595. DOI: 10.1016/0022-0000(93)90044-W.

[21] Bogdanov, A. and E. Viola (2007). "Pseudorandom Bits for Polynomials". In: *Proc. 48th Annual IEEE Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society. 41–51. DOI: http://dx.doi.org/10.1109/FOCS.2007.56.

[22] Borgs, C., J. Chayes, L. Lovász, V. T. Sós, B. Szegedy, and K. Vesztergombi (2006). "Graph limits and parameter testing". In: *STOC'06: Proceedings of the 38th Annual ACM Symposium on Theory of Computing*. ACM, New York. 261–270. DOI: 10.1145/1132516.1132556.

[23] Cohen, H. (2008). *Number theory: Volume I: Tools and diophantine equations*. Vol. 239. Springer Science & Business Media.

[24] Conlon, D., J. Fox, and B. Sudakov (2010). "Hypergraph Ramsey numbers". *Journal of the American Mathematical Society*. 23(1): 247–266.

[25] Erdös, P. and R. Rado (1952). "Combinatorial theorems on classifications of subsets of a given set". *Proceedings of the London mathematical Society*. 3(1): 417–439.

[26] Erdös, P. and G. Szekeres (1935). "A combinatorial problem in geometry". *Compositio Mathematica*. 2: 463–470.

[27] Erdös, P. and P. Turán (1936). "On Some Sequences of Integers". *J. London Math. Soc.* S1-11(4): 261. DOI: 10.1112/jlms/s1-11.4.261.

[28] Feige, U., S. Goldwasser, L. Lovász, S. Safra, and M. Szegedy (1996). "Interactive proofs and the hardness of approximating cliques". *J. ACM*. 43(2): 268–292.

[29] Fischer, E. (2004). "The art of uninformed decisions: A primer to property testing". In: *Current Trends in Theoretical Computer Science: The Challenge of the New Century*. Ed. by G. Paun, G. Rozenberg, and A. Salomaa. Vol. 1. World Scientific Publishing. 229–264.

[30] Fischer, E. and I. Newman (2007). "Testing versus estimation of graph properties". *SIAM J. Comput.* 37(2): 482–501 (electronic). DOI: 10.1137/060652324.

[31] Furstenberg, H. (1977). "Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions". *J. Analyse Math.* 31: 204–256.

[32] Goldreich, O., S. Goldwasser, and D. Ron (1998). "Property testing and its connection to learning and approximation". *J. ACM*. 45(4): 653–750. DOI: 10.1145/285055.285060.

[33] Goldreich, O. and T. Kaufman (2011). "Proximity oblivious testing and the role of invariances". In: *Approximation, randomization, and combinatorial optimization*. Vol. 6845. *Lecture Notes in Comput. Sci.* Heidelberg: Springer. 579–592. DOI: 10.1007/978-3-642-22935-0_49.

[34] Goldreich, O. and L. A. Levin (1989). "A hard-core predicate for all one-way functions". In: *Proceedings of the twenty-first annual ACM symposium on Theory of computing*. ACM. 25–32.

[35] Goldreich, O. and D. Ron (2011). "On proximity-oblivious testing". *SIAM J. Comput.* 40(2): 534–566. DOI: 10.1137/100789646.

[36] Gopalan, P., R. O'Donnell, R. A. Servedio, A. Shpilka, and K. Wimmer (2009). "Testing Fourier Dimensionality and Sparsity". In: *Proc. 36th Annual International Conference on Automata, Languages, and Programming*. 500–512.

[37] Gowers, W. T. (2001). "A new proof of Szemerédi's theorem". *Geom. Funct. Anal.* 11(3): 465–588. DOI: 10.1007/s00039-001-0332-9.

[38] Gowers, W. T. (2010). "Decompositions, approximate structure, transference, and the Hahn-Banach theorem". *Bull. Lond. Math. Soc.* 42(4): 573–606. DOI: 10.1112/blms/bdq018.

[39] Gowers, W. T. and J. Wolf (2010). "The true complexity of a system of linear equations". *Proc. Lond. Math. Soc. (3)*. 100(1): 155–176. DOI: 10.1112/plms/pdp019.

[40] Gowers, W. T. and J. Wolf (2011). "Linear forms and higher-degree uniformity for functions on $\mathbb{F}_p^n$". *Geom. Funct. Anal.* 21(1): 36–69. DOI: 10.1007/s00039-010-0106-3.

[41] Green, B. (2007). "Montréal notes on quadratic Fourier analysis". In: *Additive combinatorics*. Vol. 43. *CRM Proc. Lecture Notes*. Providence, RI: Amer. Math. Soc. 69–102.

[42] Green, B. and T. Tao (2008). "An inverse theorem for the Gowers U^3-norm". *Proc. Edin. Math. Soc.* 51: 73–153.

[43] Green, B. and T. Tao (2009). "The distribution of polynomials over finite fields, with applications to the Gowers norms". *Contrib. Discrete Math.* 4(2): 1–36.

[44] Green, B. and T. Tao (2010a). "An equivalence between inverse sumset theorems and inverse conjectures for the U 3 norm". In: *Mathematical Proceedings of the Cambridge Philosophical Society*. Vol. 149. No. 01. Cambridge Univ Press. 1–19.

[45] Green, B. and T. Tao (2010b). "Linear equations in primes". *Ann. of Math. (2)*. 171(3): 1753–1850. DOI: 10.4007/annals.2010.171.1753.

[46] Hatami, H., P. Hatami, and J. Hirst (2014a). "Limits of Boolean functions on $\mathbb{F}_p^n$". *Electron. J. Combin.* 21(4): Paper 4.2, 15.

[47] Hatami, H., P. Hatami, and S. Lovett (2014b). "General systems of linear forms: equidistribution and true complexity". *arXiv preprint arXiv:1403.7703*.

[48] Hatami, H. and S. Lovett (2011). "Higher-order Fourier analysis of $\mathbb{F}_p^n$ and the complexity of systems of linear forms". *Geom. Funct. Anal.* 21(6): 1331–1357. DOI: 10.1007/s00039-011-0141-8.

[49] Hatami, H. and S. Lovett (2013). "Estimating the distance from testable affine-invariant properties". In: *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*. IEEE. 237–242.

[50] Hatami, H. and S. Lovett (2014). "Correlation Testing for Affine Invariant Properties on $\mathbb{F}_p^n$ in the High Error Regime". *SIAM Journal on Computing*. 43(4): 1417–1455.

[51] Host, B. and B. Kra (2005). "Nonconventional ergodic averages and nilmanifolds". *Ann. of Math. (2)*. 161(1): 397–488. DOI: 10.4007/annals.2005.161.397.

[52] Jutla, C. S., A. C. Patthak, A. Rudra, and D. Zuckerman (2004). "Testing Low-Degree Polynomials over Prime Fields". In: *Proc. 45th Annual IEEE Symposium on Foundations of Computer Science*. 423–432.

[53] Kaufman, T. and S. Litsyn (2005). "Almost orthogonal linear codes are locally testable". In: *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*. IEEE. 317–326.

[54] Kaufman, T. and S. Lovett (2008). "Worst Case to Average Case Reductions for Polynomials". *Foundations of Computer Science, IEEE Annual Symposium on*: 166–175. URL: http://doi.ieeecomputersociety.org/10.1109/FOCS.2008.17.

[55] Kaufman, T. and D. Ron (2006). "Testing Polynomials over General Fields". *SIAM J. on Comput.* 36(3): 779–802.

[56] Kaufman, T. and M. Sudan (2008). "Algebraic property testing: the role of invariance". In: *Proc. 40th Annual ACM Symposium on the Theory of Computing*. 403–412.

[57] Lovett, S. (2009). "Unconditional Pseudorandom Generators for Low Degree Polynomials". *Theory of Computing*. 5(1): 69–82. DOI: 10.4086/toc.2009.v005a003. URL: http://www.theoryofcomputing.org/articles/v005a003.

[58] Lovett, S. (2012). "Equivalence of polynomial conjectures in additive combinatorics". *Combinatorica*. 32(5): 607–618. DOI: 10.1007/s00493-012-2714-z.

[59] Lovett, S. (2015). *An Exposition of Sanders' Quasi-Polynomial Freiman-Ruzsa Theorem*. *Graduate Surveys*. No. 6. Theory of Computing Library. 1–14. DOI: 10.4086/toc.gs.2015.006. URL: http://www.theoryofcomputing.org/library.html.

[60] Lovett, S., R. Meshulam, and A. Samorodnitsky (2011). "Inverse conjecture for the Gowers norm is false". *Theory Comput.* 7: 131–145. DOI: 10.4086/toc.2011.v007a009.

[61] Lucas, E. (1878). "Théorie des Fonctions Numériques Simplement Périodiques". *American Journal of Mathematics*. 1(2): 184–196. URL: http://www.jstor.org/stable/2369308.

[62] MacWilliams, F. J. and N. J. A. Sloane (1977). *The theory of error-correcting codes*. Elsevier.

[63] O'Donnell, R. (2014). *Analysis of boolean functions*. Cambridge University Press.

[64] Reingold, O., L. Trevisan, M. Tulsiani, and S. Vadhan (2008). "Dense subsets of pseudorandom sets". In: *Foundations of Computer Science, 2008. FOCS'08. IEEE 49th Annual IEEE Symposium on*. IEEE. 76–85.

[65] Ron, D. (2009). "Algorithmic and Analysis Techniques in Property Testing". *Foundations and Trends in Theoretical Computer Science*. 5(2): 73–205.

[66] Roth, K. F. (1953). "On certain sets of integers". *J. London Math. Soc.* 28: 104–109.

[67] Rubinfeld, R. (1999). "On the robustness of functional equations". *SIAM Journal on Computing*. 28(6): 1972–1997.

[68] Rubinfeld, R. (2006). "Sublinear time algorithms". In: *Proceedings of International Congress of Mathematicians 2006*. Vol. 3. 1095–1110.

[69] Rubinfeld, R. and M. Sudan (1996). "Robust characterizations of polynomials with applications to program testing". *SIAM J. Comput.* 25(2): 252–271. DOI: 10.1137/S0097539793255151.

[70] Samorodnitsky, A. (2007). "Low-degree tests at large distances". In: *STOC'07—Proceedings of the 39th Annual ACM Symposium on Theory of Computing*. New York: ACM. 506–515. DOI: 10.1145/1250790.1250864.

[71] Sanders, T. (2012). "On the Bogolyubov-Ruzsa lemma". *Analysis & PDE*. 5(3): 627–655.

[72] Sanders, T. (2013). "The structure theory of set addition revisited". *Bulletin of the American Mathematical Society*. 50: 93–127.

[73] Shapira, A. (2009). "Green's conjecture and testing linear-invariant properties". In: *STOC'09—Proceedings of the 2009 ACM International Symposium on Theory of Computing*. ACM, New York. 159–166.

[74] Sudan, M. (2010). "Invariance in Property Testing". *Tech. rep.* No. 10-051. Electronic Colloquium in Computational Complexity.

[75] Szegedy, B. (2012). "On higher order Fourier analysis". *arXiv preprint arXiv:1203.2260*.

[76] Szemerédi, E. (1969). "On sets of integers containing no four elements in arithmetic progression". *Acta Math. Acad. Sci. Hungar.* 20: 89–104.

[77] Szemerédi, E. (1975). "On sets of integers containing no k elements in arithmetic progression". *Acta Arith.* 27: 199–245. Collection of articles in memory of Juriui Vladimirovivc Linnik.

[78] Tao, T. (2007). "Structure and randomness in combinatorics". In: *Foundations of Computer Science, 2007. FOCS'07. 48th Annual IEEE Symposium on*. IEEE. 3–15.

[79] Tao, T. (2008). "Some notes on "non-classical" polynomials in finite characteristic". *Blog post available at https://terrytao.wordpress.com/2008/11/13/some-notes-on-non-classical-polynomials-in-finite-characteristic*.

[80] Tao, T. (2012). *Higher order Fourier analysis*. Vol. 142. American Mathematical Soc.

[81] Tao, T. and V. H. Vu (2010). *Additive combinatorics*. Vol. 105. *Cambridge Studies in Advanced Mathematics*. Paperback edition [of MR2289012]. Cambridge University Press, Cambridge. xviii+512.

[82] Tao, T. and T. Ziegler (2010). "The inverse conjecture for the Gowers norm over finite fields via the correspondence principle". *Anal. PDE*. 3(1): 1–20. DOI: 10.2140/apde.2010.3.1.

[83] Tao, T. and T. Ziegler (2012). "The inverse conjecture for the Gowers norm over finite fields in low characteristic". *Ann. Comb.* 16(1): 121–188. DOI: 10.1007/s00026-011-0124-3.

[84] Viola, E. (2011). "Selected Results in Additive Combinatorics: An Exposition." *Theory of Computing, Graduate Surveys*. 2: 1–15.

[85] Viola, E. (2009). "The Sum of D Small-Bias Generators Fools Polynomials of Degree D". *Computational Complexity*. 18(2): 209–217.

[86] Yoshida, Y. (2014a). "A characterization of locally testable affine-invariant properties via decomposition theorems". In: *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*. ACM. 154–163.

[87] Yoshida, Y. (2014b). "Gowers Norm, Function Limits, and Parameter Estimation". *arXiv preprint arXiv:1410.5053*.

[88] Ziegler, T. (2007). "Universal characteristic factors and Furstenberg averages". *J. Amer. Math. Soc.* 20(1): 53–97 (electronic). DOI: 10.1090/S0894-0347-06-00532-7.