LINEAR FORMS AND HIGHER-DEGREE UNIFORMITY FOR FUNCTIONS ON $\mathbb{F}_p^n$

W.T. GOWERS AND J. WOLF

Abstract. In [GW1] we began an investigation of the following general question. Let $L_1, \ldots, L_m$ be a system of linear forms in $d$ variables on $\mathbb{F}_p^n$, and let $A$ be a subset of $\mathbb{F}_p^n$ of positive density. Under what circumstances can one prove that $A$ contains roughly the same number of $m$-tuples $L_1(x_1, \ldots, x_d), \ldots, L_m(x_1, \ldots, x_d)$ with $x_1, \ldots, x_d \in \mathbb{F}_p^n$ as a typical random set of the same density? Experience with arithmetic progressions suggests that an appropriate assumption is that $\|A - \delta 1\|_{U^k}$ should be small, where we have written $A$ for the characteristic function of the set $A$, $\delta$ is the density of $A$, $k$ is some parameter that depends on the linear forms $L_1, \ldots, L_m$, and $\| \cdot \|_{U^k}$ is the $k$th uniformity norm. The question we investigated was how $k$ depends on $L_1, \ldots, L_m$. Our main result was that there were systems of forms where $k$ could be taken to be 2 even though there was no simple proof of this fact using the Cauchy–Schwarz inequality. Based on this result and its proof, we conjectured that uniformity of degree $k - 1$ is a sufficient condition if and only if the $k$th powers of the linear forms are linearly independent. In this paper we prove this conjecture, provided only that $p$ is sufficiently large. (It is easy to see that some such restriction is needed.) This result represents one of the first applications of the recent inverse theorem for the $U^k$ norm over $\mathbb{F}_p^n$ by Bergelson, Tao and Ziegler [TZ2], [BTZ]. We combine this result with some abstract arguments in order to prove that a bounded function can be expressed as a sum of polynomial phases and a part that is small in the appropriate uniformity norm. The precise form of this decomposition theorem is critical to our proof, and the theorem itself may be of independent interest.

1 Introduction

In [GW1] we investigated which systems of linear equations have the property that any uniform subset of $\mathbb{F}_p^n$ contains the “expected” number of solutions. By the “expected” number we mean the number of solutions one would expect in a random subset of the same density, and by a “uniform subset of $\mathbb{F}_p^n$” we mean a set $A$ of density $\delta$ such that $\|A - \delta 1\|_{U^2}$ is small, where $A$ is the characteristic function of $A$.

Keywords and phrases: Higher order Fourier analysis, uniformity norms, solutions to systems of linear equations

2010 Mathematics Subject Classification: 11B30

Both authors gratefully acknowledge the hospitality of the Mathematical Sciences Research Institute, Berkeley, where important parts of this work were carried out.
More generally, we asked the same question with the $U^2$ norm replaced by any other $U^k$ norm. Note that the $U^k$ norms increase as $k$ increases, so the condition that $\|A - \delta 1\|_{U^k}$ is small becomes stronger, and there are more sets of linear forms for which it is sufficient.

This question arises naturally in the context of Szemerédi’s theorem. If $x_0, \ldots, x_{k-1}$ satisfy the equations $x_i - 2x_{i+1} + x_{i+2} = 0$ for $i = 0, 1, 2, \ldots, k - 3$, then they lie in an arithmetic progression (in the sense that there exists $d \in \mathbb{F}_p$ such that $x_i = x_0 + id$ for each $i$). It was shown in [G1] that if $\|A - \delta 1\|_{U^{k-1}}$ is small, then $A$ contains roughly the number of arithmetic progressions of length $k$ that you would expect if the elements of $A$ had been selected randomly and independently with probability $\delta$. (More precisely, this was shown in $\mathbb{Z}_N$ rather than $\mathbb{F}_p^n$, but the proof carries over very easily.) The proof used multiple applications of the Cauchy–Schwarz inequality. Moreover, this result is sharp, in the sense that $\|A - \delta 1\|_{U^{k-2}}$ can be small without $A$ containing roughly the expected number of progressions of length $k$.

In their investigations of solutions of linear equations in the primes, Green and Tao [GrT4] worked out the most general result that could be proved using this kind of approach. Note first that by parametrizing the set of solutions to a system of linear equations one can talk equivalently about systems of linear forms. For instance, instead of the equations $x_i - 2x_{i+1} + x_{i+2} = 0$ for $i = 0, 1, 2, \ldots, k - 3$ mentioned above one can look at the system of linear forms $x, x + y, x + 2y, \ldots, x + (k - 1)y$.

Green and Tao defined a notion of “complexity” for a system of linear forms in $d$ variables $x_1, \ldots, x_d$, and proved that for a system $L_1, \ldots, L_m$ of complexity $k$ you will get roughly the expected number of images $L_1(x_1, \ldots, x_d), \ldots, L_m(x_1, \ldots, x_d)$ in $A$ provided that $\|A - \delta 1\|_{U^{k+1}}$ is small. However, if one also works out the most general result that can be obtained by straightforwardly adapting the examples that prove that the $U^{k-1}$ norm is needed for progressions of length $k$, then a discrepancy emerges. It is easy to show that if the functions $L_1^k, \ldots, L_m^k$ are linearly dependent, then there exists $A$ such that $\|A - \delta 1\|_{U^k}$ is small but $A$ does not have roughly the expected number of solutions. However, there are systems of linear forms that have complexity $k$ while the functions $L_1^k, \ldots, L_m^k$ are linearly independent, and the easy arguments do not tell us how they behave. The main result of [GW1] was that for at least some such systems it is enough for $\|A - \delta 1\|_{U^k}$ to be small. More specifically, we showed that there are systems of equations of complexity 2 such that it is enough to assume that $\|A - \delta 1\|_{U^2}$ is small, whereas a direct application of the argument of Green and Tao would require $\|A - \delta 1\|_{U^3}$ to be small.

To state our result in a concise way, we defined the true complexity of a system of linear equations in $d$ variables to be the smallest $k$ with the following property. For every $\eta > 0$ there exists $\epsilon > 0$ such that for every $\delta \in [0, 1]$ and every subset $A \subset \mathbb{F}_p^n$ of density $\delta$, if $\|A - \delta 1\|_{U^{k+1}} < \epsilon$ then $p^{-nd}$ times the number of $m$-tuples $L_1(x_1, \ldots, x_d), \ldots, L_m(x_1, \ldots, x_d)$ in $A$ lies within $\eta$ of what one would expect in the random case (assuming that there are no degeneracies). To distinguish our notion of complexity from that of Green and Tao, we referred to theirs as Cauchy–Schwarz complexity.