1B-2

素体上多項式に対する計算困難な関数

Andrej Bogdanov† 河内 亮周‡ 田中 秀宗‡
†香港中文大学 ‡東京工業大学

1 Background

Hardness amplificationis a method for turning a function that is somewhat hard to compute into one that is very hard to compute against a given class of adversaries. The existence of many objects in average-case complexity and cryptography, such as hard on average NP problems and one-way functions, rely on unproven assumptions. In many cases, hardness amplification allows us to prove that if weakly hard versions of such objects exist, then strongly hard ones exist as well.

In settings where complexity lower bounds are known, applications of hardness amplification are not so common. Nevertheless, the method can sometimes be used to turn unconditional weak lower bounds into strong ones. Viola and Wigderson [7] showed an XOR lemma that amplifies the hardness of functions $f : \mathbb{F}_2^n \to \mathbb{F}_2$ against low-degree polynomials over finite fields. There are many examples of weakly hard functions for this class of adversaries. The result of Viola and Wigderson allows us to turn these into functions of related complexity that are very hard to approximate (in terms of approximation accuracy) by polynomials of the same degree.

Low-degree polynomials are fundamental objects in theoretical computer science, with applications in error-correcting codes, circuit complexity, probabilistically checkable proofs, and so on. Applications often require the use of polynomials over fields larger than $\mathbb{F}_2$. In some cases results about polynomials over $\mathbb{F}_2$ can be easily extended to other finite fields, but in other cases different ideas are required for binary and non-binary fields.

2 Our Results

In this work, we generalize the XOR lemma of Viola and Wigderson [7] to arbitrary prime fields. We prove the following. Here, $\mathbb{F}_q$ is a finite field of prime order q, and $\delta_d(f) = \min_{p \text{ of degree } d} \Pr_x[f(x) \neq p(x)]$, that is the distance between f and its nearest degree-d polynomials.

Theorem 1. *Let q be a prime number, and $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function such that $\delta_d(f) \geq \frac{q}{(d+1)2^{d+1}}$. If*

$$t \geq \frac{q^2 \cdot (d+1) \cdot 2^{2d+3}}{3} \ln\left\{\left(\frac{q-1}{q}\right)\varepsilon^{-1}\right\},$$

then

$$\delta_d\left(f^{+t}\right) \geq \frac{q-1}{q} - \varepsilon.$$

where $f^{+t} : (\mathbb{F}_q^n)^t \to \mathbb{F}_q$ is the sum over $\mathbb{F}_q$ of t independent copies of f.

Since $\delta_d(f) \leq \frac{q-1}{q}$ for any function f, Theorem 1 allows us to construct functions that are arbitrarily close to having optimal hardness against degree-d polynomials over $\mathbb{F}_q$, by choosing $t = t(d, q, \varepsilon)$ sufficiently large.

Applying our argument, we obtain an explicit function that is very hard to approximate by polynomials of degree d:

Theorem 2. *Let $d \geq 0$ be an integer and m be an integer coprime to q, where $m < q$, and $\mathsf{MOD}_m(x_1, ..., x_n) := x_1 + x_2 + \cdots + x_n \bmod m$, where $+$ is the addition over $\mathbb{F}_q$. Then,*

$$\delta_d(\mathsf{MOD}_m) \geq \frac{q-1}{q} - \frac{q-1}{q} \exp\left(-\frac{\pi^2}{q^3}\left(\frac{q-1}{q}\right)^{d+1} \frac{n}{2^{d+2}}\right).$$

Hardness of modulo functions for low-degree polynomials for different settings of parameters has been studied in several works. Directly applying our hardness amplification to a function $f(x) = x \bmod m$, we would prove the hardness of another modulo function as an explicit function, similarly to Theorem 2. However, q and d are then forced to satisfy $\delta_d(f) \geq \frac{q}{(d+1)2^{d+1}}$, and moreover, the obtained bound is weaker than that of Theorem 2.

3 Our proof

We generalize the proof of Viola and Wigderson [7] over $\mathbb{F}_2$. Their argument makes use of the *Gowers d-norm* $\|\cdot\|_{U^d}$ [4, 5]. Starting from a function $f : \mathbb{F}_2^n \to \mathbb{F}_2$ that is mildly far from degree-d polynomials over $\mathbb{F}_2$, Viola and Wigderson reason as follows: (1) From the low-degree test analysis of Alon et al. [1], we know that if f is mildly far from degree-d polynomials, then $\|f\|_{U^{d+1}}$ is bounded away from one. (2) By the multiplicativity of the Gowers norm,

Hard Functions for Low-degree Polynomials over Prime Fields (Extended Abstract)
Andrej BOGDANOV†, Akinori KAWACHI‡, and Hidetoki TANAKA‡
†Department of Computer Science and Engineering, the Chinese University of Hong Kong, ‡Department of Mathematical and Computing Sciences, Tokyo Institute of Technology

$\|f^{+t}\|_{U^{d+1}} = \|f\|_{U^{d+1}}^t$, so $\|f^{+t}\|_{U^{d+1}}$ is close to zero for t sufficiently large. (3) For any polynomial p of degree d, $\|f^{+t} - p\|_{U^1} \leq (\|f\|_{U^{d+1}}^{2^{d+1}})^t$, so $\|f^{+t} - p\|_{U^1}$ must be close to zero as well. The last quantity simply measures the correlation between f^{+t} and p, so p must be far from all degree-d polynomials over $\mathbb{F}_2$.

Step (2) of this analysis extends easily to prime fields; step (3) requires some additional but standard technical tools. However, step (1) relies on the analysis of the low-degree test of Alon et al., which was designed specifically for the binary field. Our main technical contribution is the extension of this test (in fact, a slight variant of it) to arbitrary fields. We believe that our presentation of this test is also simpler and more modular.

Our test, which we call the Gowers test, works as follows: Given a function $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$, choose a random set of points $x, y_1, \ldots, y_{d+1} \in \mathbb{F}_q^n$, and query f at all inputs of the form $x + a_1y_1 + \cdots + a_{d+1}y_{d+1}$, where $(a_1, \ldots, a_{d+1})$ ranges over $\{0,1\}^{d+1}$. If the evaluations are consistent with a degree-d polynomial accept, otherwise reject.

Let us call the collection of queries $\{x + a_1y_1 + \cdots + a_{d+1}y_{d+1}\colon (a_1, \ldots, a_{d+1}) \in \{0,1\}^{d+1}\}$ a *subcube* of $\mathbb{F}_q^n$. In the case $q = 2$, something special happens: With high probability, a subcube of $\mathbb{F}_q^n$ coincides with a rank $d+1$ affine subspace of $\mathbb{F}_q^n$. This fact plays a crucial property in the analysis of Bhattacharyya et al. [2], who obtain tight lower bounds (within a constant factor) on the rejection probability of the Gowers test over $\mathbb{F}_2$.

The low-degree test of Kaufman and Ron [6] over general fields also works by choosing a random affine subspace of appropriate dimension and checking that the restriction of f on this space is a polynomial of degree d. Their work suggests that the proper way to generalize the Gowers test to larger fields is by viewing it as a random subspace test, and not a random subcube test. However, we do not see how the Kaufman-Ron test can be used to argue hardness amplification. Unlike the Gowers test, their test does not seem to be naturally related to the Gowers norm or any other measure on functions that is multiplicative and bounds the correlation with degree-d polynomials, and so we cannot proceed with steps (2) and (3) of the Viola-Wigderson argument.

We show that if f is δ-far from a degree-d polynomial, then the Gowers test performs 2^{d+1} queries and rejects f with probability $\min\{\delta/q, 1/(d+1)2^{d+1}\}$. The Gowers test has higher query complexity than the Kaufman-Ron test.* However, its rejection probability is closely related to the Gowers norm over $\mathbb{F}_q$, and we can conclude the proof.

Our analysis of the Gowers test is a generalization of the linearity test analysis of Blum, Luby, and Rubinfeld [3]. Given a function $f\colon \mathbb{F}_q^n \to \mathbb{F}_q$ that the test accepts with high probability, they define a function $g\colon \mathbb{F}_q^n \to \mathbb{F}_q$ that is close to f, and then they argue that g must be linear. The linearity of g is proved using a self-reducibility argument, which relates evaluations of g at arbitrary inputs to evaluations at random inputs, where the identity $g(x) + g(y) = g(x+y)$ holds with high probability.

We proceed along the same lines: Given f, we define a function g that is close to f, and then argue that g must be a degree-d polynomial. To argue the second part, we use a self-reducibility argument that relates evaluations of g at arbitrary subcubes to evaluations at random subcubes.

The reason why we suppose prime fields in our results is that the characterization of polynomials used in the Gowers test makes sense only over prime fields. We need to discover a new characterization of polynomials over non-prime fields connected to the Gowers norm for further generalization.

*The Kaufman-Ron test makes q^ℓ queries, where $\ell = \lceil (d+1)/(q - q/p) \rceil$ and $q = p^k$ for a prime p and integer k and has rejection probability about $\min\{\Omega(\delta_d(f)q^\ell), 1/(\ell q^{\ell+1})\}$.

References

[1] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing low-degree polynomials over GF(2). In *Proceedings of RANDOM-APPROX*, pages 188–199, 2003.

[2] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of Reed-Muller codes. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science*, 2010. To appear. See also TR09-86, Electronic Colloquium on Computational Complexity.

[3] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/Correcting with Applications to Numerical Problems. *Journal of Computer and System Sciences*, (3):549–595, 1993.

[4] Timothy Gowers. A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geometric and Functional Analysis*, 8(3):529–551, 1998.

[5] Timothy Gowers. A new proof of Szemerédi's theorem. *Geometric and Functional Analysis*, 11(3):465–588, 2001.

[6] Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM Journal on Computing*, 36(3):779–802, 2006.

[7] Emanuele Viola and Avi Wigderson. Norms, XOR lemmas, and lower bounds for polynomials and protocols. *Theory of Computing*, 4(1):137–168, 2008.