Testing linear-invariant non-linear properties: A short report

Arnab Bhattacharyya¹, Victor Chen², Madhu Sudan³, and Ning Xie⁴

 ¹ MIT CSAIL Cambridge, MA abhatt@mit.edu
² Institute of Theoretical Computer Science Tsinghua University Beijing, China victor.vc@gmail.com
³ Microsoft Research New England Cambridge, MA madhu@microsoft.com
⁴ MIT CSAIL Cambridge, MA ningxie@csail.mit.edu

Abstract. The rich collection of successes in property testing raises a natural question: Why are so many different properties turning out to be locally testable? Are there some broad "features" of properties that make them testable? Kaufman and Sudan (STOC 2008) proposed the study of the relationship between the invariances satisfied by a property and its testability. Particularly, they studied properties that were invariant under linear transformations of the domain and gave a characterization of testability in certain settings. However, the properties that they examined were also linear. This led us to investigate linear-invariant properties that are not necessarily linear. Here we describe some of the resulting works which consider natural linear-invariant properties, specifically properties that are described by forbidden patterns of values that a function can take, and show testability under various settings.

Keywords: property testing, regularity lemma, linear invariance

1 Introduction

The field of property testing, initiated by the works in [BLR93,BFL91] and defined formally in [RS96,GGR98], has seen an enormous and diverse collection of successes lately. The rich collection of properties that turn out to be testable extremely locally (with say, constant number of queries) relative to the size of the object being tested, leads to a natural question: Why are so many properties locally testable? Are there some broad unifying themes in the properties being tested, and the testers being used? In an attempt to explain this richness and diversity, Kaufman and Sudan [KS08] suggested that the "invariances" shown by a property may play a central role in their testability. A property of functions mapping a domain D to a range R is said to be invariant under a map $\pi: D \to D$, if whenever a function f satisfies the property, so does the function $f \circ \pi$. In particular, if π is a permutation, then this says that the property is invariant if the domain is relabelled according to π . Kaufman and Sudan suggest that many properties that are known to be testable have a rich collection of invariances and often testability is implied by such invariances. They then focus on algebraic properties in particular and notice that the properties in consideration are defined over domains that are vector spaces over some field, and the properties are invariant under linear, and sometimes affine, transformations of the domain. They also show that using very few additional features of the property, one can deduce testability, thus unifying many previous results (including those in [BLR93,RS96,AKK⁺05,KR06,JPRZ04]).

One of the more restrictive "additional features" of the properties studied by [KS08] is that the property itself is "linear", the range of the functions being considered is a field and the property forms a vector space over this field. While this feature is definitely exhibited by all algebraic properties, it is a very different requirement to the requirement of linear-invariance; and motivated our work [BCSX09] where we attempt to extend the study of "testing based on invariance" beyond this restriction. The principal results of our work is an infinite class of "natural non-linear, linear-invariant properties" which we show to be testable. In the process we describe an even richer class of linear-invariant properties whose testability remains open, which if shown to be locally testable would unify the results of this work, with those studied in the algebraic setting (including those of [KS08]). We describe our problems and results in greater detail below.

2 Definitions: Constraints, Characterizations, Invariance and Orbits

We consider properties of functions mapping some domain D to some range R. We let $\{D \to R\}$ denote the set of all such functions and describe a property by the set of functions $\mathcal{F} \subseteq \{D \to R\}$ that satisfy the property. Throughout this article, we will consider functions mapping the domain $D = \{0, 1\}^n$ to the range $\{0, 1\}$, where the domain is viewed as the *n*-dimensional vector space over the binary⁵ field \mathbb{F}_2 . By an abuse of notation, \mathcal{F} will actually refer to an ensemble of properties, one for each value of $n \in \mathbb{Z}^+$.

We measure the distance between functions in the (by now) standard way: the distance between f and g, denoted $\delta(f,g)$, is the quantity $\delta(f,g) = \Pr_{x \in D}[f(x) \neq g(x)]$. The distance of f to a property \mathcal{F} is the quantity $\delta(f,\mathcal{F}) = \min_{g \in \mathcal{F}} \{\delta(f,g)\}$. We say f is δ -close to \mathcal{F} if $\delta(f,\mathcal{F}) \leq \delta$ and δ -far otherwise. A $(k(\delta), \tau(\delta))$ -local (one-sided) *tester* for \mathcal{F} is a probabilistic oracle algorithm T that takes as input

⁵ Most notions also extend to the case where the domain is a vector space over an arbitrary finite field, and the range is an arbitrary finite set.

a parameter δ and queries an oracle for $f k(\delta)$ times and accepts functions in \mathcal{F} with probability one, while rejecting functions that are δ -far with probability at least $\tau(\delta)$. If such a tester exists, \mathcal{F} is said to be *locally testable*. Note that we are interested only in testers where $\tau(\delta) > 0$ for every $\delta > 0$. Also, neither $k(\cdot)$ nor $\tau(\cdot)$ is a function of n. If k is furthermore independent of δ , we say that the tester is *proximity-oblivious*, following Goldreich and Ron [GR09].

Next, we turn to the notion of invariance. For a function $\pi : D \to D$, we say that a property \mathcal{F} is *invariant* under π if the function $f \in \mathcal{F}$ implies $f \circ \pi \in \mathcal{F}$. A property $\mathcal{F} \subseteq \{\{0,1\}^n \to \{0,1\}\}$ is *linear-invariant* if for every linear function $L : \{0,1\}^n \to \{0,1\}^n$, \mathcal{F} is invariant under L. Our hope is to describe a large collection of natural linear-invariant properties that are locally testable.

A very broad collection of natural testable properties are what may be described as "locally characterized properties" – we describe these next. A k-local constraint $C = (a_1, \ldots, a_k; S)$ is given by a k-tuple $a_1, \ldots, a_k \in D$ and nonempty set $S \subseteq \mathbb{R}^k$. We say that a function $f: D \to \mathbb{R}$ satisfies the constraint Cif $(f(a_1), \ldots, f(a_k)) \notin S$. We say that a property \mathcal{F} satisfies the constraint C if every function $f \in \mathcal{F}$ satisfies C. A collection of constraints C_1, \ldots, C_m k-locally characterizes a property \mathcal{F} if each constraint is k-local and $f \in \mathcal{F}$ if and only if f satisfies C_j for every $j \in \{1, \ldots, m\}$. If k does not depend on n, we say the property is locally characterized.

It is natural to analyze the testability of locally characterized properties, and indeed the early work of Rubinfeld and Sudan [RS96] does suggest analyzing the "robustness" of characterizations to design and analyze local tests for properties. (Roughly, a characterization is robust if the only functions that satisfy most constraints in the characterization are those that are close to the property.) Characterizations are effectively also a necessary condition for the existence of non-adaptive proximity-oblivious tests [GR09], which are the prevalent ones in the algebraic setting. Finally, for linear-invariant properties, characterizations take on an especially nice form, as we describe next.

Given a k-local constraint $C = (a_1, \ldots, a_k; S)$ on functions mapping D to Rand a map $\pi : D \to D$, let the π -rotation of C, denoted $\pi \circ C$, be the k-local constraint $\pi \circ C = (\pi(a_1), \ldots, \pi(a_k); S)$. Note that if \mathcal{F} is invariant under π and \mathcal{F} satisfies C, then it also satisfies $\pi \circ C$. For linear-invariant properties, it follows that the existence of a single constraint C implies an abundance of constraints $L \circ \pi$, one for each linear function L mapping the domain to itself. We refer to the set of constraints $\{L \circ C | L \text{ is linear }\}$ as the *orbit* of the constraint C. Given this abundance of local constraints satisfied by a property \mathcal{F} , one could even hope that the family is characterized by the orbit of a single constraint. To this end we say that \mathcal{F} has a k-local single orbit characterization if there exists a k-local constraint C such that its orbit characterizes \mathcal{F} . At first glance, the existence of a single orbit characterization may seem like a very strong requirement, but not at second glance! In particular the following proposition is easy to show:

Proposition 1. If $\mathcal{F} \subseteq \{\{0,1\}^n \to \{0,1\}\}$ is k-locally characterized and linearinvariant, then it has a K-local single orbit characterization, for some $K \leq 2^k$. (When the domain is a vector space over a field of cardinality q, the bound weakens to $K \leq q^k$.) The existence of such a nice and very "uniform" characterization of \mathcal{F} suggests a very natural test for the propery \mathcal{F} locally characterized by the orbit of a single constraint C: Pick a random linear map L and verify that f satisfies $L \circ C$. If this test can be shown to be sound, then it would imply that every locally characterized linear-invariant property is locally testable. This question remains open (see more in Section 4.1), and our work [BCSX09] takes some first steps towards understanding the testability of this class of properties (and shows testability of a proper, but infinite, subclass). We describe our specific results next.

3 Our results in [BCSX09]

To understand the class of properties that are linear-invariant and not linear, it is useful to start with a simple example (that is not already covered by the results of [KS08]). Our work starts with the "triangle-freeness" property introduced by Green [Gre05] and extends it. A function $f : \{0,1\}^n \to \{0,1\}$ is said to be *triangle-free* if the set $f^{-1}(1)$ does not contain a triple of the form x, y, x + y. In our language, the property of being triangle-free could be describe by the family \mathcal{F} characterized by the orbit of the constraint $C = (a, b, a+b; S = \{111\})$ where aand b are two (arbitrary) linearly independent vectors over the domain $\{0,1\}^n$. Green [Gre05] shows that the property of being triangle-free is indeed locally testable, though the analysis is quite different from the analyses in algebraic settings. In our work, we extend this test to a broader collection of constraints.

To describe this extension, we need to introduce a few more pieces of notation. We say that a property \mathcal{F} characterized by the orbit of a constraint $C = (a_1, \ldots, a_k; S)$ is monotone if S is an upward closed set, i.e., for $x, y \in \{0, 1\}^k$, if $x \in S$ and $x_i \leq y_i$ for all $i \in [k]$, then $y \in S$. (In other words, removing elements from the support of a function satisfying a monotone property keeps the function in the property.) We call the constraint $C = (a_1, \ldots, a_k; S)$ a pattern if the set S has only one element. Note that if C is a pattern, it is monotone exactly when $S = \{1^k\}$. We refer to the property described by the orbit of a single monotone pattern C as being C-free.

Notice that the family described by a constraint $C = (a_1, \ldots, a_k; S)$ is essentially a function of the underlying "matroid". The matroid perspective simply views a_1, \ldots, a_k as an abstract set of k elements and tells us which subsets of these elements are independent and which ones are not. (The exact definition is not important to us, since we retain the linear-algebraic descriptions in our definition below; but the notions is from matroid theory.) We say a_1, \ldots, a_k form a graphic matroid if there exists an undirected graph G = (V, E) with k edges $E = \{e_1, \ldots, e_k\}$ such that for every subset $S \subseteq \{1, \ldots, k\}$ the set $\{a_i | i \in S\}$ is linearly independent if and only if the graph $G_S = (V, \{e_i | i \in S\})$ has no cycles. We say that a constraint C is based on a graphic matroid if the constraint points a_1, \ldots, a_k form a graphic matroid.

Our main theorem in [BCSX09] can now be stated.

Theorem 1 ([BCSX09]). For a k-local monotone pattern C based on a graphic matroid, the property of being C-free is locally testable. Specifically, there exists a function $\tau = \tau_k : \Re^+ \to \Re^+$ and a k-query test T that accepts C-free functions with probability one, while rejecting functions that are δ -from being C-free with probability at least $\tau(\epsilon)$.

As a consequence, any monotone linear-invariant property locally characterized by the orbit of a constraint C based on a graphic matroid is locally testable with a proximity-oblivious tester.

The bound on τ is quite weak. Let W(t) denote a tower of twos with height $\lceil t \rceil$. Our proof only guarantees that $\tau(\epsilon) \geq W(\operatorname{poly}(1/\epsilon))^{-1}$, a rather fast vanishing function. In fact, all known proofs, even for the property of being triangle-free, have this tower-behavior inherently because they rely on some form of a "regularity lemma", which we now describe.

To analyze the triangle-freeness property, Green developed a regularity lemma for groups, which is analogous to Szemerédi's regularity lemma for graphs. In the boolean case, Green's regularity lemma shows how, given any function $f: \{0,1\}^n \to \{0,1\}$, one can find a subgroup H of $\{0,1\}^n$ such that the restriction of f to almost all cosets of H is "regular", where "regularity" is defined based on the "Fourier coefficients" of f.

This lemma continues to play a central role in [BCSX09] as well. To extract a large feasible class of matroids, we also use a notion from a work of Green and Tao [GT06] of the complexity of a linear system (or matroids). The "least complex" matroids have complexity 1, and it was shown that the regularity lemma can be applied to all matroids of complexity 1 to show that they are testable.

The presence of the many restrictions on the nature of the constraint C leads to a natural question: Are there many (or any) new properties that can be tested based on Theorem 1? Of course, there are infinitely many different constraints C, but the property of being C-free need not be different for different C's. For example, one can permute the points a_1, \ldots, a_k and the coordinates of S to obtain essentially the same constraint. Alternately, one can replace the constraint C by the constraint $L \circ C$ for an invertible linear map L and get the same family. But equivalence goes beyond such syntactic concerns. For example, suppose Cis a constraint based on a graphic matroid, where the underlying graph is one whose biconnected components are triangles. Then being C-free is essentially the same as being triangle-free, in that every triangle-free function is also Cfree, while every C-free function is $O(2^{-n})$ -close to being triangle free. Thus one needs to prove explicitly that the class of properties being tested include (infinitely many) new ones. (We also advocate that this concern ought to be addressed explicitly in any work in property testing that aims to work for a broad class of properties.)

In [BCSX09], we consider the following two infinite classes of (monotone) patterns based on graphic matroids. For $\ell = 3, 4, \ldots$, let O_{ℓ} be the constraint $O_{\ell} = (a_1, \ldots, a_{\ell}; \{1^{\ell}\})$ where $a_1, \ldots, a_{\ell-1} \in \{0, 1\}^n$ are linearly independent and $a_{\ell} = \sum_{i < \ell} a_i$. O_{ℓ} is thus based on the graphic matroid corresponding to the

cycle of length ℓ . Similarly for $\ell = 2, 3, \ldots$, let K_{ℓ} be the constraint on $k = {\ell \choose 2}$ points based on the graphic matroid of the complete graph on ℓ vertices. Note that O_{ℓ} -freeness and K_{ℓ} -freeness are testable for every ℓ , by Theorem 1. The following theorem shows that these (infinite class of properties) are all pairwise distinct (i.e., for every pair, at least one property contains elements which are $\Omega(1)$ -far from the other).

Theorem 2 ([BCSX09]). The class of C-free properties for C being a monotone pattern based on graphic matroids include infinitely many distinct ones. In particular:

- 1. For every odd $\ell \geq 3$, if f is $O_{\ell+2}$ -free, then it is also O_{ℓ} -free. However, there exist functions g that are O_{ℓ} -free but far from being $O_{\ell+2}$ -free.
- 2. For every $\ell \geq 2$, if f is K_{ℓ} -free, then it is also $K_{\ell+1}$ -free. However, for $\ell \geq 3$ there exists a function g that is K_{ℓ} -free but far from being $K_{\binom{\ell}{2}+2}$ -free.

Theorems 1 and 2 combine to give some room for optimism that one may get an exact understanding of the class of linear-invariant properties that have O(1)-query proximity oblivious tests.

Our results show that, at least under severe restrictions, the natural test for such a property does work, and that, despite the restrictions, this does lead to an infinite class of new properties. Fortunately, subsequent work revealed that several of the limitations in Theorem 1 above turned out to be limitations of the proof technique alone, and stronger techniques can be brought to bear on this class of problems. We discuss some of the subsequent work next.

4 Subsequent work and Open problems

4.1 Boolean functions over \mathbb{F}_2^n

Our work can be viewed as a step towards the proof of the following conjecture.

Conjecture 1. Suppose \mathcal{F} is a linear-invariant property of functions mapping $\{0,1\}^n$ to $\{0,1\}$. Then, \mathcal{F} is locally testable with a proximity-oblivious tester *if* and only if \mathcal{F} is locally characterized.

It's not hard to show one direction, namely that any linear-invariant property that has a proximity-oblivious local tester is locally characterized. The proof of this is analogous to the proof of the corresponding statement for graphs in Theorem 4.7 of [GR09]. Our work in [BCSX09] makes some progress in the opposite direction but is restricted due to two obstacles. The first restriction is that we have to assume that the characterization of the property corresponds to a graphic matroid, and secondly, we have to assume that the property is monotone.

The restriction that the underlying matroid be graphic was tackled independently by Král et al. [KSV08] and Shapira [Sha09]. (It turns out that such a step also relates closely to a conjecture of Green [Gre05] about solutions to linear systems over the integers.) They showed⁶ the following in our terminology.

Theorem 3 ([KSV08,Sha09]). If a linear-invariant property is locally characterized and monotone, then it is locally testable with a proximity-oblivious tester.

The techniques used to prove this theorem were somewhat different from those in [BCSX09]. Both [KSV08] and [Sha09] gave ingenious reductions to testing whether a hypergraph is free from a fixed collection of sub-hypergraphs. Powerful tools for tackling the latter problem were already known [FR02,RS04,NRS06,Gow07,AT08], which could then be applied. Unfortunately, it is not at all clear how to reduce to a sub-hypergraph-freeness property if the linear-invariant property is not monotone.

More recently, Bhattacharyya et al. [BGS10] could remove the monotonicity condition but now again had to insist that the underlying matroid be graphic. The restriction to graphic matroids is essentially because of the same reason as in our paper [BCSX09].

Theorem 4 ([**BGS10**]⁷). If a linear-invariant property is locally characterized by the orbit of a constraint based on a graphic matroid, then it is locally testable with a proximity-oblivious tester.

It remains open how to combine Theorems 3 and 4. In fact, even the special case when the property is characterized by the orbit of a single non-monotone *pattern* remains unresolved. We note that a positive resolution to questions such as the above would lead to a single unifying result capturing the theorems of Alon et al. $[AKK^+05]$ as well as Green [Gre05] – a unification that we don't have yet.

4.2 Finite-valued functions over \mathbb{F}_{q}^{n}

A general open direction is to extend the results of the previous section to arbitrary finite-valued functions over arbitrary, but constant sized, fields. There has been some partial progress for boolean-valued functions over field \mathbb{F}_q^n for fixed prime power q. Theorem 3 is known to hold in this setting. (In fact, [KSV09] even shows testability for certain monotone properties of boolean functions over nonabelian groups!) The authors of [BGS10] conjecture that their techniques can be extended to prove the analog of Theorem 4 for boolean-valued functions over \mathbb{F}_q^n . We are not aware of any nontrivial progress for the analogous questions for non-boolean-valued functions.

⁶ More precisely, Theorem 3 follows from the main result of [KSV08] and [Sha09], along with a twist to handle non-uniformity of the property with respect to n, similar to what is done in the proof of Theorem 4.7 in [GR09].

⁷ We note that the main result of [BGS10] is actually stronger, since it also shows testability for certain properties which are not locally characterized, and so, do not have proximity-oblivious testers.

More generally one could also consider functions over \mathbb{F}_q^n where the field size is not a constant. We note that in such a case, single orbit characterizations do not necessarily capture all locally characterized properties, but understanding the testability of single-orbit characterized properties would remain a challenging first step.

4.3 Improving the soundness analysis

One of the intriguing aspects of testing non-linear linear-invariant properties is that the proof techniques employed thus far have been very different from the techniques used in the linear cases. One implication of the difference in techniques is that the "soundness" analysis is much weaker. In particular this leads to $\tau(\epsilon)$ being much smaller than any polynomial in ϵ in Theorem 1 (as well as in the stronger forms). In contrast, in the case of linear, linear-invariant properties, the growth of $\tau(\epsilon)$ is linear in ϵ (Theorem 5.20 of [KS08]). This leads to the question: Is such subpolynomial growth inherent? A positive answer to this question would be insightful in that it would explain (somewhat) the need for new proof techniques in the case of testing non-linear, linear-invariant properties. Partial progress in this direction is reported in the work of Bhattacharyya and Xie [BX10]. They show that distinguishing triangle-free functions from those ϵ -far from triangle-free with constant probability requires $(1/\epsilon)^{1+\alpha}$ queries for some positive constant α , thus separating non-linear linear-invariant properties from linear linear-invariant ones.

In the other direction, Fox has recently shown [Fox10] that the use of the Szemerédi regularity lemma can be avoided for the analysis of testing subgraph-freeness, and the soundness analysis can be (very) mildly improved. This translates to a corresponding improvement for the properties considered in [BCSX09] also. Perhaps it is possible to strengthen such an approach to get much better bounds than we currently have.

References

- AKK⁺05. Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing Reed-Muller codes. *IEEE Transactions on Information The*ory, 51(11):4032–4039, 2005.
- AT08. T. Austin and T. Tao. On the testability and repair of hereditary hypergraph properties. *Random Structures and Algorithms (To appear)*, 2008. http://arxiv.org/abs/0801.2179.
- BCSX09. Arnab Bhattacharyya, Victor Chen, Madhu Sudan, and Ning Xie. Testing linear-invariant non-linear properties. In Symposium on Theoretical Aspects of Computer Science, pages 135–146, 2009.
- BFL91. László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. Computational Complexity, 1(1):3–40, 1991.
- BGS10. Arnab Bhattacharyya, Elena Grigorescu, and Asaf Shapira. A unified framework for testing linear-invariant properties. To appear in FOCS, 2010.

- BLR93. Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. J. Comp. Sys. Sci., 47:549–595, 1993. Earlier version in STOC'90.
- BX10. Arnab Bhattacharyya and Ning Xie. Lower bounds for testing trianglefreeness in boolean functions. In Proc. 21st ACM-SIAM Symposium on Discrete Algorithms, pages 87–98, 2010.
- Fox10. Jacob Fox. A new proof of the graph removal lemma. Technical report, June 2010. http://arxiv.org/abs/1006.1300.
- FR02. Peter Frankl and Vojtech Rödl. Extremal problems on set systems. Random Structures and Algorithms, 20(2):131–164, 2002.
- GGR98. Oded Goldreich, Shafi Goldwasser, and Dana Ron. Property testing and its connection to learning and approximation. *Journal of the ACM*, 45:653–750, 1998.
- Gow07. William T. Gowers. Hypergraph regularity and the multidimensional Szemerédi theorem. Annals of Mathematics, 166(3):897–946, 2007.
- GR09. Oded Goldreich and Dana Ron. On proximity oblivious testing. In Proc. 41st Annual ACM Symposium on the Theory of Computing, pages 141–150, 2009.
- Gre05. Ben Green. A Szemerédi-type regularity lemma in abelian groups, with applications. Geom. Funct. Anal., 15(2):340–376, 2005.
- GT06. Ben Green and Terence Tao. Linear equations in primes. Annals of Mathematics (to appear), 2006.
- JPRZ04. Charanjit S. Jutla, Anindya C. Patthak, Atri Rudra, and David Zuckerman. Testing low-degree polynomials over prime fields. In Proc. 45th Annual IEEE Symposium on Foundations of Computer Science, pages 423–432, 2004.
- KR06. Tali Kaufman and Dana Ron. Testing polynomials over general fields. SIAM J. on Comput., 36(3):779–802, 2006.
- KS08. Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In *Proc. 40th Annual ACM Symposium on the Theory of Computing*, pages 403–412, New York, NY, USA, 2008. ACM.
- KSV08. Daniel Král', Oriol Serra, and Lluís Vena. A removal lemma for systems of linear equations over finite fields, 2008.
- KSV09. Daniel Král', Oriol Serra, and Lluís Vena. A combinatorial proof of the removal lemma for groups. Journal of Combinatorial Theory, 116(4):971– 978, May 2009.
- NRS06. Brendan Nagle, Vojtěch Rödl, and Mathias Schacht. The counting lemma for regular k-uniform hypergraphs. *Random Structures and Algorithms*, 28(2):113–179, 2006.
- RS96. Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. on Comput.*, 25:252–271, 1996.
- RS04. Vojtěch Rödl and Jozef Skokan. Regularity lemma for k-uniform hypergraphs. *Random Structures and Algorithms*, 25(1):1–42, 2004.
- Sha09. Asaf Shapira. Green's conjecture and testing linear-invariant properties. In Proc. 41st Annual ACM Symposium on the Theory of Computing, pages 159–166, 2009.