Invariance in Property Testing

Madhu Sudan*

March 26, 2010

Abstract

Property testing considers the task of testing rapidly (in particular, with very few samples into the data), if some massive data satisfies some given property, or is far from satisfying the property. For "global properties", i.e., properties that really depend somewhat on every piece of the data, one could ask how it can be tested by so few samples? We suggest that for "natural" properties, this should happen because the property is invariant under "nice" set of "relabellings" of the data. We refer to this set of relabellings as the "invariance class" of the property and advocate explicit identification of the invariance class of locally testable properties. Our hope is the explicit knowledge of the invariance class may lead to more general, broader, results.

After pointing out the invariance classes associated with some the basic classes of testable properties, we focus on "algebraic properties" which seem to be characterized by the fact that the properties are themselves vector spaces, while their domains are also vector spaces and the properties are invariant under affine transformations of the domain. We survey recent results (obtained with Tali Kaufman, Elena Grigorescu and Eli Ben-Sasson) that give broad conditions that are sufficient for local testability among this class of properties, and some structural theorems that attempt to describe which properties exhibit the sufficient conditions.

1 Introduction: Property Testing and Invariance

We assume the reader of this article has some passing familiarity with some of the basic motivations and nature of questions in Property Testing, and jump directly to establishing our notations.

In this article, we will consider testing properties of *functions* mapping some finite domain D to a finite range R. We let $\{D \to R\}$ denote the set of all such functions. A property will be specified by the set of functions $\mathcal{P} \subseteq \{D \to R\}$. (More generally, we may consider a parameterized family of domains D_n one for each positive integer n, and the property will be given by $\mathcal{P} = \{\mathcal{P}_n\}_n$, where $\mathcal{P}_n \subseteq \{D_n \to R\}$.)

We will measure distance between functions via the normalized Hamming distance (as is standard in Property Testing). Specifically, for $f, g : D \to R$, the *distance* between f and g, denoted $\delta(f, g)$, is given by $\delta(f, g) = \Pr_{x \leftarrow_U D}[f(x) \neq g(x)]$, where the notation $x \leftarrow_U D$ denotes a random variable x drawn uniformly from the domain D. The distance from f to a family $\mathcal{F} \subseteq \{D \to R\}$, denoted $\delta(f, \mathcal{F})$, is the quantity $\min_{g \in \mathcal{F}}\{\delta(f, g)\}$. We say f is δ-*close* to $\mathcal{F}$ if $\delta(f, \mathcal{F}) \leq \delta$ and δ-*far* otherwise.

*Microsoft Research, One Memorial Drive, Cambridge, MA 02142, USA, madhu@mit.edu

Definition 1.1 *A $(k, \epsilon_1, \epsilon_2, \delta)$ tester for a property $\mathcal{P}$ is a probabilistic algorithm T with oracle access to a function $f : D \to R$ that makes at most k queries to the oracle for f, and accepts $f \in \mathcal{P}$ with probability at least $1 - \epsilon_2$, while rejecting f that is δ-far from $\mathcal{P}$ with probability at least ϵ_1.*

A principal focus in property testing is on properties that are defined for infinitely many n where the tests are parameterized by δ. and for every $\delta > 0$, $k = O(1)$ while $\epsilon_1 - \epsilon_2 = \Omega(1) > 0$. (In particular, k and $\epsilon_1 - \epsilon_2$ do not depend on n.) We will also focus mostly on one-sided error tests, i.e., tests where $\epsilon_2 = 0$. In such a case, we simply refer to the tester as a (k, ϵ, δ)-tester.

1.1 Invariances

We now move to the definition of central interest to this article, namely the invariances of a property.

We say that $\mathcal{P}$ is *invariant* under a function $\pi : D \to D$ if for every $f \in \mathcal{P}$ it is the case that the function $f \circ \pi$, defined as $f \circ pi(x) = f(pi(x))$, is also in $\mathcal{P}$. We say that $\mathcal{P}$ is invariant under a set $G \subseteq \{D \to D\}$ if for every $\pi \in G$, $\mathcal{P}$ is invaraint under π. The set of all functions π under which $\mathcal{P}$ is invariant is termed the invariance class of $\mathcal{P}$. (The invariance class is a semi-group under composition.) The set of all *permutations* (bijections) π under which $\mathcal{P}$ is invariant is the *automorphism group* of $\mathcal{P}$.

The notion of examining testability of properties with explicit attention on their invariance is a slowly emerging theme. An early result of Babai, Shpilka and Stefankovic [7] gave lower bounds on rates of locally testable codes for cyclic codes is perhaps the first to explicitly relate testability to invariances, albeit to give negative results. The work by Goldreich and Sheffet [33] also uses symmetries to give lower bounds on query complexity. Alon et al. [3] were possibly the first to suggest this might lead to positive results. The work by Kaufman and Sudan [40] seems to be the first to to explicitly focus on invariances to derive positive results.

The goal of this article is two-fold: The first is a collection of observations pointing out that several earlier results in property testing describe natural properties that have nice invariance classes (and in some cases, the invariance classes characterize the properties completely). The second, more technical aspect, is to describe the invariances of algebraic properties. In this part we survey several recent works [40, 36, 37, 15], joint with Ben-Sasson, Grigorescu, and Kaufman, that study the relationship between testability and the invariance classes of the property.

2 Invariances of some well-studied properties

2.1 Statistical Properties

One of the oldest examples of a "property test" may be "polling", which tests for "approximate majority". This test can be formalized by considering functions mapping some finite universe D to the range $R = \{0, 1\}$ and the property $\mathcal{P}$ includes all functions f that take the value 1 on at least $|D|/2$ inputs. (Thus the set D may be thought of as the names of a set of people, f denotes their preference among the two choices in the set R. $\mathcal{P}$ then consists of all possible preference functions in which the majority prefers the choice $1 \in R$.) The standard test (sample f on k random inputs and accept if the majority is 1) and analysis shows that if $k = \Omega(1/\delta^2)$, then we can get $\epsilon_1 - \epsilon_2 = \Omega(1)$.

The invariance class of this property equals its automorphism group and is the full group of permutations from $D \to D$. We now assert that this group of permutations is what leads to the testability of this property.

Indeed any property $\mathcal{P}$ of functions mapping D to R that is invariant under the full group of permutations from $D \to D$ depends on only $|R|$ frequency counts $\{\eta_y\}_{y \in R}$ where $\eta_y = \Pr_{x \in_U D}[f(x) = y]$. To separate $f \in \mathcal{P}$ from f that is δ-far from $\mathcal{P}$ it suffices to get an approximation $\{\nu_y\}_{y \in R}$ to the vector $\{\eta_y\}_{y \in R}$ of ℓ_1 error at most 2δ (i.e., $\sum_{y \in R} |\eta_y - \nu_y| \leq 2\delta$). It is straightforward to get such an approximation with $O(|R| \log |R|)$ queries into f (by getting a pointwise approximation of $O(\delta/|R|)$. A better approximation in time $O(|R|)$ is also not too hard (see [48]). We note that the recent results in testing properties of distributions [30, 10, 8, 9, 11, 1, 52, 50, 55] have revealed many properties that can be tested in $o(|R|)$ samples, and in several cases given nearly-tight bounds (to within $|R|^{o(1)}$ factors) on the query complexity of such tests.

2.2 Graph Property Testing

One of the most actively investigated themes in property testing is the testing of "graph properties", initiated in [28], with recent progress [2, 20] characterizing the properties of "dense graphs" that can be tested with constant queries.

The basic model (the "dense graph" model) considers functions from $D = \binom{V}{2}$ to the range $R = \{0, 1\}$ (where V is some finite set and $\binom{V}{2}$ denotes the collection of all subsets of size of V).

We note that a property $\mathcal{P}$ is considered a graph property if and only if it is invariant under permutations on $\binom{V}{2}$ "induced" by permutations of V. Specifically, say that a permutation $\pi : \binom{V}{2} \to \binom{V}{2}$ is a graph-permutation if there exists a permutation $\sigma : V \to V$ such that for all $u, v \in V$, $\pi(u, v) = (\sigma(u), \sigma(v))$. A property $\mathcal{P}$ is a graph property if and only if its automorphism group contains all graph-permutations. It follows (trivially) that the success of graph-property testing (i.e., the understanding of testability to the extent of getting a necessary and sufficient condition for testing with $O(1)$ queries) is attributable to the underlying automorphism group.

We note that the above explanation of graph-properties in terms of symmetries seems to apply only to the "dense-graph" model, but not the "bounded-degree" graph model [31], where it is natural to think of the inputs as functions from $V \times [d] \to V$. To include graph properties on such representations of graphs, one could expand the notion of symmetries to consider permutations from $D \times R$ to $D \times R$, but we won't attempt to do so here.

We note that an upcoming work of Goldreich and Kaufman [29] investigates various aspects of property testing and in particular graph-property testing, even in the bounded-degree case, in terms of invariances.

2.3 Properties of Boolean functions

Another broad class of properties that have been explored recently are properties of "Boolean functions". Sample properties here include monotonicity testing, dictator-testing, junta-testing, testing if a function is given by a real half-space, testing various forms of concise representations etc. [24, 27, 23, 12, 49, 25, 18, 46, 21]. Boolean properties have nice symmetries too.

Here the domain is the set $D = \{0,1\}^n$ and the invariant group includes all permutations π that are induced by permutations on the coordinates, i.e., permutations $\pi : \{0,1\}^n \to \{0,1\}^n$ for which there exists a corresponding permutation $\sigma : [n] \to [n]$ such that $\pi(\langle b_1, \ldots, b_n \rangle) = \langle b_{\sigma(1)}, \ldots, b_{\sigma(n)} \rangle$.

Unlike in the previous settings, where the invariant group leads to a complete characterization of testable properties, such a characterization is notably missing in this setting.

3 Algebraic Properties

We now move to the topic of focus of this article, namely a large class of "algebraic properties". This class of property tests indeed form the origins of property testing with the seminal work of Blum, Luby and Rubinfeld [19] proposing the now famous "linearity-test" (a test for homomorphisms between groups). Somewhat independently, and with significantly different motivation, Babai, Fortnow, and Lund [6] proposed and analyzed a test to check if a multivariate function over a finite subset of the integers was a multilinear function (linear in each variable). This result was one of the key technical ingredients behind the remarkable result "MIP=NEXP" which formed the predecessor for the modern PCP theory and its connection to inapproximability. Subsequently, Babai, Fortnow, Levin and Szegedy [5] analyzed a property test for when a multivariate function over a vector space over a finite field was a polynomial of a specified (low) degree in each variable. While both of these tests were quite efficient they could work with "constant" queries only when both the degree and the number of variables were constant. Partly to remedy this, Rubinfeld and Sudan [53], proposed and analyzed a low-degree test generalizing the test of [19]. This test would test if a multivariate function over a finite field was a polynomial of low "total" degree (with degree being somewhat smaller than field size). If the degree bound specified was a constant, then the query complexity of this test was a constant independent of the number of variables. Both the linearity test and the low-degree test played a crucial role in the work of Arora et al. [4] leading to the PCP theorem. Indeed a significant component of PCP theory focusses on new/improved analyses of various linearity/low-degree tests.

The ability to test algebraic functions in constant time for constant degree, is not restricted only to the case where the degree is smaller than the field size. This was first shown by Alon et al. [3] for the case of multivariate functions over the binary field, and then independently by Kaufman and Ron [39] and Jutla et al. [38] for functions over arbitrary fields as well. The work reported below is an attempt to unify the properties, tests and analyses reported in the many works above, in particular those of [19, 53, 3, 39, 38].

3.1 A generalization of algebraic properties

From this point onwards, throughout this section we will be consider functions from an n-dimensional vector space over a field $\mathbb{K}$ of size Q to a subfield $\mathbb{F}$ of size q and characteristic p.[1] Let $q = p^s$ and $Q = q^t$. Throughout we will think of q as a constant. The two extreme cases of interest to us will be (1) Q is also a constant and $n \to \infty$; and (2) $n = 1$ and Q (or t) is the parameter going to infinity.

[1] We note that it is possible to consider a broader class of properties allowing $\mathbb{F}$ to be an arbitrary field, and not just a subfield of $\mathbb{K}$. However we are not aware of any results that work in this more general setting.

We will consider properties $\mathcal{P}$ of functions mapping $\mathbb{K}^n \to \mathbb{F}$ that are "linear" and "affine-invariant", where we define the terms below.

Linear Properties A property $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ is said to be ($\mathbb{F}$-)linear if for every $f, g \in \mathcal{P}$ and $\alpha, \beta \in \mathbb{F}$ the function $\alpha \cdot f + \beta \cdot g$ is also in $\mathcal{P}$, where $\alpha \cdot f + \beta \cdot g$ is the function given by $(\alpha \cdot f + \beta \cdot g)(x) = \alpha f(x) + \beta g(x)$

Affine-invariant Properties A function $A : \mathbb{K}^n \to \mathbb{K}^n$ is said to be affine if there exists a matrix $M \in \mathbb{K}^{n \times n}$ and a vector $b \in \mathbb{K}^n$ such that $A(x) = Mx + b$ for $x \in \mathbb{K}^n$. A property $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ is said to be affine-invariant (over $\mathbb{K}^n$) if for every $f \in \mathcal{P}$ and affine function $A : \mathbb{K}^n \to \mathbb{K}^n$ it is the case that $f \circ A \in \mathcal{P}$, where $f \circ A(x) = f(A(x))$.

Since both linearity and affine-invariance seem to impose some sort of "vector-space" restrictions, we stress the different role of the two restrictions. Note that while linearity depends on the range of the functions, the invariance only depends on the domain of the function. And while the latter property (invariance) is more close to the focus of this article, the former assumption (linearity) will be crucial to the rest of this section. Indeed it is possible to consider properties that are linear without focussing on invariances (as was done by Ben-Sasson et al. [14]), or on properties that are affine-invariant, while not being linear (as done in Bhattacharyya et al. [16] and Shapira [54]). We will discuss the latter setting in a later section, and use some of the results in the former setting in this section to motivate our analysis.

In the future, we refer to the set of affine transformations from $\mathbb{K}^n \to \mathbb{K}^n$ as the *affine semi-group*. (They form a semi-group under multiplication.)

3.2 Constraints and Characterizations

One of the basic and very useful observations from the work of Ben-Sasson et al. [14] for linear properties is that tests for such properties might as well be non-adaptive, and make one-sided error. In other words, a k-query tester would pick (based on its internal randomness) some k points $\alpha_1, \ldots, \alpha_k \in \mathbb{K}^n$, and a predicate $P : \mathbb{F}^k \to \{0, 1\}$ and accept a function f if and only if $P(f(\alpha_1), \ldots, f(\alpha_k)) = 1$. Non-adaptivity refers to the fact that $\alpha_1, \ldots, \alpha_k$ are chosen without knowledge of f on any of the other points. One-sided error implies that if $P(f(\alpha_1), \ldots, f(\alpha_k)) = 0$ then $f \notin \mathcal{P}$. Finally [14] also show that the acceptance predicate can also be chosen to be a linear system, i.e., the set $V = P^{-1}(1)$ is a vector subspace of $\mathbb{F}^k$. This motivates our notion of a (k-local) constraint.

Definition 3.1 *A k-local constraint C is given by $C = (\langle \alpha_1, \ldots, \alpha_k \rangle; V)$ where $\alpha_i \in \mathbb{K}^n$ and $V \subsetneq \mathbb{F}^k$ is a vector subspace of $\mathbb{F}^k$. A function f is said to satisfy the constraint C if $\langle f(\alpha_1), \ldots, f(\alpha_k) \rangle \in V$. A property $\mathcal{P}$ satisfies a constraint C if every function $f \in \mathcal{P}$ satisfies C.*

In the language of constraints, the above-mentioned result of [14] could be interpreted as asserting that a k-query tester for a property $\mathcal{P}$ is simply a distribution on k-local constraints. Given oracle access to a function f, the tester simply picks a k-local constraint (according to the distribution) and accepts if f satisfies the chosen constraint. Thus in order for a test to exist, a property $\mathcal{P}$

must satisfy many k-local constraints; and while it is not (a prioiri) necessary that the constraints completely determine the property $\mathcal{P}$, for many properties considered above, local constraints do seem to determine the property. The notion of a characterization below formalizes this concept.

Definition 3.2 *A collection of k-local constraints $C_1, \ldots, C_m$ form a k-local characterization of a a property $\mathcal{P}$ if $f \in \mathcal{P}$ if and only if f satisfies C_j for every $j \in [m]$.*

In general, the fact that a property satisfies even one local constraint may seem to be a rare event. To find a whole collection of local constraints satisfied by a property, to the extent that they even characterize it, may seem even more so. But for properties that exhibit some (invariances), this is not as suprising (and indeed this is what motivates some of the study of invariances of properties in the context of local testing). If a property $\mathcal{P}$, invariant under a function π satisfies the constraint $C = (\langle \alpha_1, \ldots, \alpha_k \rangle; V)$ then it also satisfies the constraint $C \circ \pi = (\langle \pi(\alpha_1), \ldots, \pi(\alpha_k) \rangle; V)$. This motivates our definition below of the *orbit* of a constraint C under a set of invariances G.

Definition 3.3 *Given a property $\mathcal{P}$ invariant under a set G that satisfies a constraint C, we say that the orbit of C under G is the set of constraints $\{C \circ \pi | \pi \in G\}$.*

Of course the definition above makes sense even when no "property" is mentioned, but the definition makes the most sense when applied to some property $\mathcal{P}$ satisfying C and invariant under G. If we are (seemingly incredibly) lucky, then the orbit of a constraint may provide enough constraints to actually charaterize a property $\mathcal{P}$. This concept, while seemingly too restrictive turns out to be central to our analysis of property testing.

Definition 3.4 (Single-orbit characterization) *A property $\mathcal{P} \subseteq \{D \to R\}$ is said to have a* k-single orbit characterization *under a set G of invariances if there exists a k-ary constraint C such that $f \in \mathcal{P}$ if and only if f satisfies $C \circ \pi$ for every $\pi \in G$.*

For this section, properties of interest will be those with a k-single orbit characterization over the affine semi-group. As we explain below a k-single-orbit characterization over the affine semi-group immediately leads to local testability; and this explains the results of [53, 3, 39, 38]. We then describe structural results about affine-invariant properties and give examples of new properties that end up being testable as a consequence.

3.3 Testability of linear affine-invariant properties

In joint work with Tali Kaufman [40] we show that a property that has a k-single orbit characterization under the affine semi-group has a k-query tester. The following theorem gives the precise soundness condition of the test.

Theorem 3.5 ([40, Theorem 2.9]) *Let $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ have a k-single orbit characterization under the affine semi-group. Then there exists a k-query test T that accepts $f \in \mathcal{P}$ with probability one, while rejecting f that is δ-far from $\mathcal{P}$ with probability* $\min\left\{\delta/2, \frac{1}{(2k+1)(k-1)}\right\}$.

The test T above is the "natural" one. Recall that the k-single orbit characterization implies that there exists a constraint $C = (\langle \alpha_1, \ldots, \alpha_k \rangle; V)$ such that for every $g \in \mathcal{P}$ and every affine map $A : \mathbb{K}^n \to \mathbb{K}^n$ it is the case that $\langle g(A(\alpha_1)), \ldots, g(A(\alpha_k)) \rangle \in V$. Given oracle access to a function $f : \mathbb{K}^n \to \mathbb{F}$, the test T simply picks a random affine map $A : \mathbb{K}^n \to \mathbb{K}^n$ and accepts if and only if $\langle f(A(\alpha_1)), \ldots, f(A(\alpha_k)) \rangle \in V$. The completeness analysis follows from the definition, while the soundness analysis (though not so small that we can summarize it here) essentially abstracts the common elements of the proofs of [19, 53, 3, 39, 38] while unifying the seemingly different parts by using the concept of "tensor products of linear spaces". [2]

To apply the theorem above to recover the results of [19, 53, 3, 39, 38] one needs appropriate single orbit characterizations for the appropriate families. Below we list some of the known ones.

Example 3.6 (Affine functions from $\mathbb{K}^n \to \mathbb{K}$, for $n \geq 2$) *Let $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{K}\}$ be the set of affine functions, i.e., $\mathcal{P} = \{f(x) | \exists a_1, \ldots, a_n, b \in \mathbb{K}$ s.t. $f(x_1, \ldots, x_n) = \sum_{i=1}^n a_i x_i + b\}$.*

For $n \geq 2$, let $\alpha, \beta, \in \mathbb{K}^n$ be (any) two linearly independent vectors in $\mathbb{K}^n$. Let $V \subseteq \mathbb{K}^4$ be the set $\{\langle a, b, c, a + b + c \rangle | a, b, c \in \mathbb{K}\}$. Let C be the constraint $(\langle 0, \alpha, \beta, \alpha + \beta \rangle; V)$.

Then $\mathcal{P}$ has a 4-single orbit characterization under the affine semi-group, given by the constraint C.

The characterization above, combined with Theorem 3.5 above, effectively captures the essential elements of the linearity test of [19], though in fact it is only a variation (affineness, instead of linearity) of a special case (linearity of maps over finite fields, as opposed to homomorphisms between abelian groups) of their main result.

Example 3.7 (Degree d polynomials from $\mathbb{K}^n \to \mathbb{K}$, for $|\mathbb{K}| = p^r \geq d + 1 + p^{r-1}$.) *Let $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{K}\}$ be the set of n-variate polynomials of degree at most d.*

Let $\alpha \in \mathbb{K}^n$ be any non-zero vector, and let $\omega \in \mathbb{K}$ be a primitive element (i.e., $\omega^i \neq 1$ for $i < |\mathbb{K}| - 1$).

Let $V = \{\langle p(1), p(\omega), p(\omega^2), \ldots, p(\omega^{d+1}) \rangle | p : \mathbb{K} \to \mathbb{K}$ is a univariate polynomial of degree at most $d\}$. Then the constraint $C = (\langle \alpha, \omega \cdot \alpha, \omega^2 \cdot \alpha, \ldots, \omega^{d+1} \cdot \alpha \rangle, V)$ is a $d+2$-single orbit characterization of $\mathcal{P}$.

The above characterization follows essentially from [53, 26] and implies that the property of being a degree d polynomial is testable with $O(d)$ queries over any large enough field (of size greater than d). What about the case when the field size $Q < d$? In such a case also one can get a single orbit characterization, where the locality of the queries is however exponential in d.

Example 3.8 (Degree d polynomials from $\mathbb{K}^n \to \mathbb{K}$ [39]) *Let $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{K}\}$ be the set of n-variate polynomials of degree at most d. Let $\ell = (d + 1 + Q/p)/(Q - 1)$ (recall $Q = |\mathbb{K}|$ and p*

[2] Given two vector spaces $U \subseteq \mathbb{K}^n$ and $V \subseteq \mathbb{K}^m$, their tensor product $U \otimes V \subseteq \mathbb{K}^{n \times m}$ can be thought of as the collection of $n \times m$ matrices each of whose rows is an element of V and columns is an element of U. The "key" (though simple) fact about this tensor product space is that its dimension is the product of dimensions of U and V. This fact turns out be the heart of the "creative steps" in the analyses of of [19, 53, 3, 39, 38].

is its characteristic). Let U be an arbitrary ℓ dimensional subspace of $\mathbb{K}^n$, and let $\alpha \in (\mathbb{K}^n)^{Q^\ell}$ be an (arbitrary) enumeration of the points of U. Let $V \subseteq \mathbb{K}^{Q^\ell}$ be the set of all evaluations of degree d, n-variate polynomials on the sequence α. Then the constraint $C = (\alpha, V)$ is a Q^ℓ-single orbit characterization of $\mathcal{P}$.

Applying Theorem 3.5 to the characterization above one can get the main result of [39] (which in turn subsumes the results of [3] and [38]).

3.4 Structure of linear affine-invariant properties

While the examples of the previous section describe how many previously known results can be unified under the perspective of invariance, to get new families that can be testable, one needs to understand more about affine-invariant properties. Here we describe some of the basic results that characterize affine invariant properties in terms of the supporting monomials.

Recall first that every function from $\mathbb{K}^n \to \mathbb{K}$, and hence every function from $\mathbb{K}^n \to \mathbb{F}$, is a polynomial in n-variables of degree at most $Q-1$ in each variable. Thus the "monomials", i.e., functions of the form $m(x_1, \ldots, x_n) = \prod_{i=1}^n x_i^{d_i}$ for some $d_1, \ldots, d_n \in \{0, \ldots, Q-1\}$ form a linear basis of all functions from $\{\mathbb{K}^n \to \mathbb{F}\}$. We let $\mathcal{M}$ denote the set of all monomials. Recalling that every function $f : \mathbb{K}^n \to \mathbb{K}$ can be written uniquely as $f(x) = \sum_{m \in \mathcal{M}} c_m m(x)$. We say that the *support* of f is the set of all monomials m whose coefficient c_m is non-zero.

Most polynomials would not map the the domain $\mathbb{K}^n$ to elements of $\mathbb{F}$ (and would often take on values from $\mathbb{K} - \mathbb{F}$). To get a basis for functions from $\mathbb{K}^n \to \mathbb{F}$, one needs to look at "traces" of monomials. The Trace function mapping $\mathbb{K} \to \mathbb{F}$ is defined as $\mathrm{Tr}(x) = x + x^q + x^{q^2} + \cdots + x^{q^{t-1}}$. (Recall that $\mathbb{F} = \mathbb{F}_q$ and $\mathbb{K} = \mathbb{F}_Q = \mathbb{F}_{q^t}$.) The reader may verify that the Trace function indeed maps all $\mathbb{K}$ to $\mathbb{F}$ (by verifying that $\mathrm{Tr}(x)^q = \mathrm{Tr}(x)$ for every $x \in \mathbb{K}$), and that it is linear, i.e., $\mathrm{Tr}(x+y) = \mathrm{Tr}(x) + \mathrm{Tr}(y)$ and $\mathrm{Tr}(\alpha x) = \alpha \mathrm{Tr}(x)$ for every $x, y \in \mathbb{K}$ and $\alpha \in \mathbb{F}$. It follows that $\mathrm{Tr}(g(x))$ is a function mapping $\mathbb{K}^n$ to $\mathbb{F}$ for every n-variate polynomial g. The following proposition establishes the converse.

Proposition 3.9 *Every function f from $\mathbb{K}^n \to \mathbb{F}$ is the trace of some polynomial g from $\mathbb{K}^n \to \mathbb{K}$. Furthermore, there always exists such a polynomial g whose support is contained in the support of f.*

Of course, given that the number of polynomials from $\mathbb{K}^n \to \mathbb{K}$ is much more than the number of functions from $\mathbb{K}^n \to \mathbb{F}$, it must be the case that different polynomials have the same trace. Some explicit examples include $\mathrm{Tr}(x) = \mathrm{Tr}(x^q)$, and $\mathrm{Tr}((\alpha + \alpha^q).x^{1+q+q^2+\cdots+q^{t-1}}) = \mathrm{Tr}(0)$. (This is why the proposition only claims that some polynomial g has its support contained in the support of f.) Nevertheless the traces give a very useful understanding of affine invariant families thanks to the following lemma (essentially from [40]) which shows that the affine-invariant properties are captured by the monomials in their support.

Lemma 3.10 (Monomial Extraction [40]) *For every affine-invariant property $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ there exists a set $\mathcal{D} \subseteq \mathcal{M}$ such that a function $f \in \mathcal{P}$ if and only if there exists a polynomial $g : \mathbb{K}^n \to \mathbb{K}$ supported on $\mathcal{D}$ such that $f = \mathrm{Tr}(g)$. Furthermore there is a unique maximal such set $\mathcal{D}$ for any affine-invariant property $\mathcal{P}$.*

We refer to the unique maximal set as the *degree set* of $\mathcal{P}$.

To see some examples, first lets consider the simpler case of $\mathbb{K} = \mathbb{F}$. In this case the Trace function is simply the identity function; and the set $\mathcal{D}$ is simply the union of the support of all functions in $\mathcal{P}$. Thus in this case if the function, say, $3x^5 + 2x^2 + 1$ is in $\mathcal{P}$, it follows that $\{1, x^2, x^5\} \subseteq \mathcal{D}$ and thus the functions x^5, x^2 and $2x^5 + x^2 + 4$ are also in $\mathcal{P}$.

One of the uses of the lemma above, is that it allows us to focus on the degree set of an affine invariant property to understand its local-testability (and in particular in understanding when it may have a single orbit characterization).

But before investigating the locality of tests we first note that not every set $\mathcal{D}$ is a degree set of some affine-invariant property $\mathcal{P}$. While a compact description of exactly which degree sets are valid sets for affine-invariant properties is not easy to describe (and depends on n, p, q, Q etc.) this is well-understood. When $n = 1$ this is somewhat easier to describe, and we do so next.

Definition 3.11 $\mathcal{D} \subseteq \mathbb{K}[x]$ *is* (q, Q)-modular *if* $x^d \in \mathcal{D} \Rightarrow x^{q \cdot d (\mathrm{mod} Q-1)} \in \mathcal{D}$

Definition 3.12 *For non-negative integers e and d and prime p, let $e_0, \ldots, e_i, \ldots$, and $d_0, \ldots, d_i, \ldots$ denote the p-ary representation of e and d (i.e., $e_0, \ldots, e_i, \ldots \in \{0, \ldots, p-1\}$ and $e = \sum_{i=0}^{\infty} e_i p^i$). We say that e is in the* p-shadow *of d if $e_i \leq d_i$ for every i. We say that a set $\mathcal{D} \subseteq \mathbb{Z}^{\geq 0}$ is* p-shadow-closed *if for every d and e in the p-shadow of d, we have $x^d \in \mathcal{D} \Rightarrow x^e \in \mathcal{D}$.*

We are now ready to describe degree sets of univariate affine-invariant properties.

Lemma 3.13 *$\mathcal{D}$ is the degree set of an affine-invariant property $\mathcal{P} \subseteq \{\mathbb{F}_Q \to \mathbb{F}_q\}$ where $Q = q^t$ and $q = p^s$ for prime p if and only if $\mathcal{D}$ is (q, Q)-modular and $\mathcal{D}$ is p-shadow-closed.*

We note in passing that the case $n = 1$ is really the most general case, since every affine-invariant property from $\{K^n \to \mathbb{F}\}$ can also be viewed as an affine-invariant property from $\{\mathbb{L} \to \mathbb{F}\}$ where $\mathbb{L}$ is the nth degree extension of $\mathbb{K}$ (i.e. $\mathbb{L} = \mathbb{F}_{Q^n}$).

While the lemmas above describe some basic features of affine-invariant properties, they don't explain when they may be locally testable. In particular when can they have local constraints, local characterizations, and even single-orbit characterizations? These questions are more novel, and less well-understood.

If one considers the case where Q, q are just constants, and only n is going to infinity, then, as shown in [40], the degree of the highest degree monomial in $\mathcal{D}$ roughly determines the best possible locality of the constraints and single orbit characterizations. Specifically they show:

Lemma 3.14 *Let $\mathcal{P} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ be an affine-invariant property with degree set $\mathcal{D}$ and let d be the largest degree of a monomial in $\mathcal{D}$. Then every constraint on $\mathcal{P}$ has locality at least $Q^{(d/Q^2-1)}$. Conversely it has a $Q^{2(d+Q)/p}$-local single orbit characerization.*

To understand the above lemma, note that it implies that if an affine-invariant propery has a *single* k-local constraint then it has k'-local characterization, and in fact, a k'-single orbit characterization, and is hence k'-locally testable for $k' \approx Q^2 \cdot k^{2Q^2}$. This appears to be far from tight and indeed the analysis in [40] is quite sloppy allowing for tighter characterizations. Indeed, we believe it should be possible to get a k'-local characterization for $k' = \text{poly}(Q, k)$.

A somewhat more optimistic conjecture might be that one can get $k' = \text{poly}(k)$ (or some other function of k which is independent of Q). Indeed such a relationship was effectively conjectured by [3] (for a broader class of properties than affine-invariant ones). However this turned out be false as shown by [36].

Theorem 3.15 *There exists an affine invariant family mapping $\{\mathbb{F}_{2^t} \to \mathbb{F}_2\}$ with an 8-local constraint, but no $(t/2-2)$-local characterization.*

The family given by [36] is easy to describe in the language developed so far: Their family $\mathcal{P}$ has, as its degree set, the set $\mathcal{D} = \{x^{2^i+2^{i+j}} | i \in \{0,\ldots,t-1\}, j \in \{0,\ldots,t/2-2\}\} \cup \{x^{2^i} | i \in \{0,\ldots,t-1\} \cup \{x^0\}$. It is easy to check that $\mathcal{D}$ is 2-shadow closed, and $(2,2^t)$-modular, and so $\mathcal{P}$ is indeed an affine invariant family. It is also easy to show that every function $f \in \mathcal{P}$ satisfies the constraint $f(x+y+z) = f(x+y)+f(x+z)+f(y+z)+f(x)+f(y)+f(z)+f(0)$ and thus $\mathcal{P}$ has an 8-local constraint. The main contribution of [36] is to show that $\mathcal{P}$ has no $t/2-2$ local constraints that are not constraints also on the larger family $\mathcal{P}'$ given by its degree set $\mathcal{D}' = \mathcal{D} \cup \{x^{2^i+2^{i+(t/2-1)}} | i\}$. Since $\mathcal{P}'$ is strictly larger than $\mathcal{P}$ it follows that $\mathcal{P}$ can not have a $t/2-2$-local characterization. Furthermore, since $\mathcal{P}'$ contains functions that are quite far from functions in $\mathcal{P}$, it follows that $\mathcal{P}$ also does not have any tests of locality $t/2-2$.

We remark that most examples of single orbit characterizations have been natural ones; i.e., the properties have a natural characterization that happens to be a single orbit one. Indeed all the examples given above (affine functions, low-degree polynomials etc.) had this property. One significant class of exceptions is given in [37] who show that every "sparse" affine invariant property from $\mathcal{P} \subseteq \{\mathbb{F}_{2^t} \to \mathbb{F}_2\}$, with $|\mathcal{P}| \leq 2^{t\ell}$, has a $k = k(\ell)$-single orbit characterization, if t is prime. (Here "sparse" refers to the fact that the size of $\mathcal{P}$ is a polynomial in the domain size. Note that the locality of the characterization is independent of the domain size and depends only on the exponent relating the size of $\mathcal{P}$ with the size of the domain.) The result of [37] is also obtained by analyzing the degree sets of sparse affine-invariant properties and noticing that functions satisfying such properties can be expressed as traces of sparse polynomials, and then combining recent results from additive number theory with classical results from coding theory to conclude that these properties have a local single orbit characterization. These results are interesting in that they yield single orbit characterizations for a very rich class of properties - so rich that it would take $\Omega(\log t)$ bits to describe a typical such property and so a "totally uniform" characterization (with $O(1)$-bits) would be out of question. Natural "local" characterizations of such properties involve describing roughly 2^t constraints each requiring $O(t)$ bits to specify. The single-orbit characterization, in contrast, only requires $O(t)$ bits to describe giving a somewhat more uniform, and yet local, description of the property and the tester for the property.

Moving on, affine-invariant properties offer a clean generalization of "low-degree" polynomials, while being significantly richer, rich enough to counter some natural conjectures about reasons for local testability in codes/algebraic properties. Furthermore, the class still offers the possibility of some

locally testable codes of constant distance that may outperform Reed-Muller codes (codes derived from low-degree polynomials) in terms of their rate. To investigate this possibility one needs a significantly better understanding of the relationship between the locality of characterizations and the degree sets of affine-invariant properties. In the case of univariate functions, no non-trivial upper bounds are known for general degree sets (the trivial one being the size of the degree set), and till recently no general lower bounds were known either. A recent result with Ben-Sasson gives the first general lower bound on the locality of constraints for a general degree set, in terms of the notion of the p-weight of elements in the degree set. We define this notion next, and give their main theorem afterwards.

Definition 3.16 *For integer d and prime p, the p-weight of d, denoted $wt_p(d)$, is defined to be the sum of the non-zero elements in the p-ary expansion of d, i.e., $wt_p(d) = \sum_i d_i$ where $d_0, \ldots, d_i, \ldots, \in \{0, \ldots, p-1\}$ s.t. $d = \sum_i d_i p^i$.*

Theorem 3.17 ([15]) *Let $\mathcal{P} \subseteq \{\mathbb{F}_{p^t} \to \mathbb{F}_p\}$ be an affine-invariant property with degree set $\mathcal{D}$. Let k be the maximum p-weight of elements of $\mathcal{D}$. Then every constraint on $\mathcal{P}$ has locality at least $k+1$. Conversely, $\mathcal{P}$ does have a constraint of locality p^{k+1}.*

When the range p is a constant, the above theorem thus pins down a necessary and sufficient condition for an affine-invariant family to have a $O(1)$-local constraint. Of course, it does not say anything about characterizations and this remains an open question. Indeed the following question remains open.

Question 3.18 *Let $\mathcal{P} \subseteq \{\mathbb{K} \to \mathbb{F}\}$ be an affine-invariant property with a k-local characterization. Let k' be the smallest integer such that $\mathcal{P}$ has a k'-single orbit characterization. Give the best possible upper bound on k' as a function of k, q and Q. Can we get a bound independent of Q? Can it be independent of q?*

To understand such questions a significantly better understanding of the relationship between local characterizations and degree sets is needed. The following question is an example of some very basic questions about this relationship which is still not understood.

Question 3.19 *Let $\mathcal{P} \subseteq \{\mathbb{F}_{2^t} \to \mathbb{F}_2\}$ be an affine-invariant property with degree set $\mathcal{D} \subsetneq \{x^{2^i+2^j} | i, j \in \{0, \ldots, t-1\}\} \cup \{1, x, x^2, \ldots, x^{2^{t-1}}\}$. Further, suppose t is prime. Then does the locality of the characterization of $\mathcal{P}$ grow with $|\mathcal{D}|$? (I.e., is the following statement true? For every k, there exists a prime t and a $(2, 2^t)$-modular, 2-shadow closed set $\mathcal{D} \subsetneq \{x^{2^i+2^j} | i, j \in \{0, \ldots, t-1\}\} \cup \{1, x, x^2, \ldots, x^{2^{t-1}}\}$ such that the affine invariant property $\mathcal{P}$ with degree set $\mathcal{D}$ has no k-local characterization.)*

We remark that if t is not a prime, then the question above does have negative answers; and understanding the exact reson for such negative answers also appears important to understanding affine-invariant properties.

4 Non-linear affine-invariant properties

Finally, we remark briefly on the setting where the properties of interest are invariant under affine/linear transformations, but are not necessarily linear. Examples of such testable non-linear properties that are affine-invariant can be generated easily by taking the union of two (or more) affine-invariant (linear) properties. (Thanks to Noga Alon for this class of examples). More interesting cases, motivated by learning theory and additive number theory, have also been explored in the literature and we mention these results briefly below.

Locally characterized properties: A broad class of affine-invariant properties that seem potentially testable can be obtained by generalizing the notion of constraints and characterizations to the non-linear setting as follows: Let $\mathbb{K}$ be a finite field and Σ be an arbitrary finite set. A k-local constraint C is given by $C = (\alpha_1, \ldots, \alpha_k; S)$ where $\alpha_1, \ldots, \alpha_k \in \mathbb{K}^n$ and $S \subsetneq \Sigma^k$. We say a function $f : \mathbb{K}^n \to \Sigma$ satisfies the constraint C if $\langle f(\alpha_1), \ldots, f(\alpha_k)\rangle \in S$. A collection of constraints $C_1, \ldots, C_m$ characterizes a property $\mathcal{P} \subseteq \{\mathbb{K}^n \to \Sigma\}$ if $f \in \mathcal{P}$ if and only if f satisfies C_j for every $j \in [m]$. Of course, our interest here is in affine-invariant property that are k-locally characterized.

A very simple example of an affine invariant property considered in Green [35] (we note that this is merely an example of property considered there, not the broadest class considered there) is the following: Let $\mathbb{K} = \mathbb{F}_2$ and $\Sigma = \{0, 1\}$. Let $C = \{\alpha, \beta, \alpha + \beta; \{0, 1\}^3 - \{111\}\})$, where $\alpha, \beta \in \mathbb{K}^n$ are an arbitrary pair of linearly independent elements. Now consider the property $\mathcal{P}$ characterized by $\{C \circ \pi | \pi : \mathbb{K}^n \to \mathbb{K}^n$ is an affine map$\}$. This is a 3-locally characterized affine-invariant property from $\mathbb{K}^n \to \Sigma$ consisting of all functions f that are "triangle-free", i.e., $f^{-1}(1)$ does not contain a triple of the form $x, y, x + y$. Green showed that the natural test (pick a random affine map $\pi : \mathbb{K}^n \to \mathbb{K}^n$ and verify that f satisfies $C \circ \pi$) does reject functions that are ϵ-far with positive probability. Somewhat intriguingly the analysis of this test, is quite different from the analyses in the linear cases and more reminiscent of the analyses in graph property testing.

This result was then generalized in various works [16, 44, 43, 54]) with perhaps the strongest result being due to [43, 54] who considers any constant number of "freeness" constraints $C_1, \ldots, C_\ell$, and their affine shifts and shows that any such property is locally testable. (A constraint $C = (\alpha_1, \ldots, \alpha_k; S)$ is said to be a freeness constraint if $\Sigma = \{0, 1\}$ and $S = \Sigma^k - \{1^k\}$.) In the process, these works also tighten the connection to graph property testing, by deriving their main results as a corollary of a new hypergraph removal lemma (a typical ingredient in hypergraph property testing).

Of course, despite all this progress, this area abounds with questions with some basic ones being: Which subclass of locally characterizaed affine-invariant properties are locally testable? When can the rejection probability of the test be lower bounded by a polynomial in the distance to the property? Some progress in this direction is reported in Bhattacharyya and Xing [17].

Sparse linear functions As part of their investigations of properties of Boolean functions Gopalan et al. [34] investigate functions that are represented as sparse functions (e.g., k-juntas) of linear functions of their input. (Formally, their properties are given by some collection of functions $\mathcal{G} \subseteq \{\mathbb{F}_2^\ell \to \mathbb{F}_2\}$ and the property of functions $\mathcal{P} \subseteq \{\mathbb{F}_2^n \to \mathbb{F}_2\}$ is given by $\mathcal{P} = \{g \circ L | g \in \mathcal{G}$ and $L : \mathbb{F}_2^n \to \mathbb{F}_2^\ell$ is linear $\}$. For a broad collection of "sparse" functions (i.e., classes of sets $\mathcal{G}$),

they show that the associated property $\mathcal{P}$ is testable. Since these classes of functions are naturally closed under linear transforms, it follows that this is yet another broad class of properties that is linear-invariant. Typically, these properties (e.g., being representable as a k-junta, or as a k-sparse polynomial) are not closed under addition, and so these properties are non-linear. Also interestingly, these properties are testable, at least to within current knowledge, only with two-sided error.

5 Conclusions

We summarize with the main message: Testing of natural properties is often intimately related to the invariances shown by the property. When the class of invariances is the full symmetric group of permutations, testing ends up representing the classical problems of statistics (though even here some improvements are feasible). But modern property testing highlights the ability to do much better when the underlying class of invariances is no the full set, and often exponentially smaller than the full set. Among the rich variety of such symmetries that can be explored, we emphasize the role of the affine-invariance (or linear-invariance) as a natural way to unify many known results. Understanding affine-invariance further might be one way of making progress on the design of locally testable codes.

We stress that we don't believe that invariance is necessary for local testability, hence the appeal to the weakening clause of "natural properties". We are aware of a wide class of properties that are known to be testable, where we are not aware of a nice invariance class. For example, a typical PCP verifier tends to accept encodings of any satisfying assignment of a SAT formula (this is actually a requirement for PCPP verifier [13] or assignment testers [22]) with local tests. Depending on the SAT formula being checked for satisfiability, the property "tested" by such a verifier is unlikely to have rich invariances. Even in the algebraic setting, we have the example of functional equations that are known to be testable [51], but where the invariance class is not known or has not been determined explicitly. In contrast to the above, we highlight the work of Goldreich and Kaufman [29] who give examples of properties that are testable, but provably have no non-trivial invariances, and also exhibit testable properties which do not have a "local single-orbit characterization".

Our point is not that such exceptions may not exist, but rather that *when invariances exist* clean rules may be found explaining when a property is testable. For graph properties properties the characterization of testability in terms of regularity instances [2] gives such a rule. For affine-invariant linear properties, the existence of local characterizations may be necessary as well as sufficient (both directions being open). The results in [40] show this to be the case, when the field size in the domain is of constant size. More importantly, the invariance class cleanly separates the many different contexts in which property testing results have been found; and gives a general approach to extracting general techniques.

We hope that in future work, the invariance classes may help further the understanding of property testing, while also help in the design of novel classes of testable codes. (A promising result here is that of Kaufman and Wigderson [41] that have given some novel codes that exhibit symmetries.) At the moment, we lack a broad understanding of group theoretic properties that help analyze testability of properties; and indeed the collection of groups for which we are able to derive testing results still remains quite limited. We hope this is remedied in future work.

Acknowledgments

Thanks to Tali Kaufman, Elena Grigorescu, and Ben-Sasson for their collaboration and comments. Thanks to Oded Goldreich and Dana Ron for advice and discussions, and to Arnab Bhattacharyya for valuable suggestions.

References

[1] Noga Alon, Alexandr Andoni, Tali Kaufman, Kevin Matulef, Ronitt Rubinfeld, and Ning Xie. Testing k-wise and almost k-wise independence. In David S. Johnson and Uriel Feige, editors, *STOC*, pages 496–505. ACM, 2007.

[2] Noga Alon, Eldar Fischer, Ilan Newman, and Asaf Shapira. A combinatorial characterization of the testable graph properties: it's all about regularity. In Kleinberg [42], pages 251–260.

[3] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing reed-muller codes. *IEEE Transactions on Information Theory*, 51(11):4032–4039, 2005.

[4] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, May 1998.

[5] László Babai, Lance Fortnow, Leonid A. Levin, and Mario Szegedy. Checking computations in polylogarithmic time. In *Proceedings of the 23rd ACM Symposium on the Theory of Computing*, pages 21–32, New York, 1991. ACM Press.

[6] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[7] László Babai, Amir Shpilka, and Daniel Stefankovic. Locally testable cyclic codes. *IEEE Transactions on Information Theory*, 51(8):2849–2858, 2005.

[8] Tugkan Batu, Sanjoy Dasgupta, Ravi Kumar, and Ronitt Rubinfeld. The complexity of approximating the entropy. *SIAM J. Comput.*, 35(1):132–150, 2005.

[9] Tugkan Batu, Lance Fortnow, Eldar Fischer, Ravi Kumar, Ronitt Rubinfeld, and Patrick White. Testing random variables for independence and identity. In *FOCS*, pages 442–451, 2001.

[10] Tugkan Batu, Lance Fortnow, Ronitt Rubinfeld, Warren D. Smith, and Patrick White. Testing that distributions are close. In *FOCS*, pages 259–269, 2000.

[11] Tugkan Batu, Ravi Kumar, and Ronitt Rubinfeld. Sublinear algorithms for testing monotone and unimodal distributions. In László Babai, editor, *STOC*, pages 381–390. ACM, 2004.

[12] Mihir Bellare, Oded Goldreich, and Madhu Sudan. Free bits, PCP's and non-approximability — towards tight results. *SIAM Journal on Computing*, 27(3):804–915, 1998.

[13] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil P. Vadhan. Robust pcps of proximity, shorter pcps, and applications to coding. *SIAM Journal on Computing*, 36(4):889–974, 2006.

[14] Eli Ben-Sasson, Prahladh Harsha, and Sofya Raskhodnikova. Some 3CNF properties are hard to test. *SIAM Journal on Computing*, 35(1):1–21, September 2005. Preliminary version in *Proc. STOC 2003*.

[15] Eli Ben-Sasson and Madhu Sudan. Limits on the rate of locally testable affine-invariant codes. Manuscript, November 2009.

[16] Arnab Bhattacharyya, Victor Chen, Madhu Sudan, and Ning Xie. Testing linear-invariant non-linear properties. In Susanne Albers and Jean-Yves Marion, editors, *STACS*, volume 3 of *LIPIcs*, pages 135–146. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, Germany, 2009.

[17] Arnab Bhattacharyya and Ning Xie. Lower bounds for testing triangle-freeness in boolean functions. In *SODA '10: Proceedings of the twenty-first Annual ACM-SIAM Symposium on Discrete Algorithms*, pages 87–98, Philadelphia, PA, USA, 2010. Society for Industrial and Applied Mathematics.

[18] Eric Blais. Testing juntas nearly optimally. In Mitzenmacher [47], pages 151–158.

[19] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *Journal of Computer and System Sciences*, 47(3):549–595, 1993.

[20] Christian Borgs, Jennifer T. Chayes, László Lovász, Vera T. Sós, Balázs Szegedy, and Katalin Vesztergombi. Graph limits and parameter testing. In Kleinberg [42], pages 261–270.

[21] Ilias Diakonikolas, Homin K. Lee, Kevin Matulef, Krzysztof Onak, Ronitt Rubinfeld, Rocco A. Servedio, and Andrew Wan. Testing for concise representations. In *FOCS*, pages 549–558. IEEE Computer Society, 2007.

[22] Irit Dinur and Omer Reingold. Assignment testers: Towards a combinatorial proof of the PCP-theorem. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 155–164, Loc Alamitos, CA, USA, 2004. IEEE Press.

[23] Yevgeniy Dodis, Oded Goldreich, Eric Lehman, Sofya Raskhodnikova, Dana Ron, and Alex Samorodnitsky. Improved testing algorithms for monotonicity. In Dorit S. Hochbaum, Klaus Jansen, José D. P. Rolim, and Alistair Sinclair, editors, *RANDOM-APPROX*, volume 1671 of *Lecture Notes in Computer Science*, pages 97–108. Springer, 1999.

[24] Funda Ergün, Sampath Kannan, Ravi Kumar, Ronitt Rubinfeld, and Mahesh Viswanathan. Spot-checkers. *J. Comput. Syst. Sci.*, 60(3):717–751, 2000.

[25] Eldar Fischer, Guy Kindler, Dana Ron, Shmuel Safra, and Alex Samorodnitsky. Testing juntas. *J. Comput. Syst. Sci.*, 68(4):753–787, 2004.

[26] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. In *Proceedings of the 3rd Annual Israel Symposium on Theory of Computing and Systems*, pages 190–198, Washington, DC, USA, 4-6 January 1995. IEEE Computer Society. Corrected version available online at `http://people.csail.mit.edu/madhu/papers/friedl.ps`.

[27] Oded Goldreich, Shafi Goldwasser, Eric Lehman, Dana Ron, and Alex Samorodnitsky. Testing monotonicity. *Combinatorica*, 20(3):301–337, 2000.

[28] Oded Goldreich, Shafi Goldwasser, and Dana Ron. Property testing and its connection to learning and approximation. *JACM*, 45(4):653–750, 1998.

[29] Oded Goldreich and Tali Kaufman. Proximity oblivious testing and the role of invariances. Manuscript, March 2010.

[30] Oded Goldreich and Dana Ron. On testing expansion in bounded-degree graphs. *Electronic Colloquium on Computational Complexity (ECCC)*, 7(20), 2000.

[31] Oded Goldreich and Dana Ron. Property testing in bounded degree graphs. *Algorithmica*, 32(2):302–343, 2002.

[32] Oded Goldreich and Dana Ron. On proximity oblivious testing. In Mitzenmacher [47], pages 141–150.

[33] Oded Goldreich and Or Sheffet. On the randomness complexity of property testing. In Moses Charikar, Klaus Jansen, Omer Reingold, and José D. P. Rolim, editors, *APPROX-RANDOM*, volume 4627 of *Lecture Notes in Computer Science*, pages 509–524. Springer, 2007.

[34] Parikshit Gopalan, Ryan O'Donnell, Rocco A. Servedio, Amir Shpilka, and Karl Wimmer. Testing fourier dimensionality and sparsity. In Susanne Albers, Alberto Marchetti-Spaccamela, Yossi Matias, Sotiris E. Nikoletseas, and Wolfgang Thomas, editors, *ICALP (1)*, volume 5555 of *Lecture Notes in Computer Science*, pages 500–512. Springer, 2009.

[35] Ben Green. A Szemerédi-type regularity lemma in abelian groups, with applications. *Geometric and Functional Analysis*, 15(2):340–376, 2005.

[36] Elena Grigorescu, Tali Kaufman, and Madhu Sudan. 2-transitivity is insufficient for local testability. In *CCC 2008: Proceedings of the 23rd IEEE Conference on Computational Complexity*, page (to appear). IEEE Computer Society, June 23-26th 2008.

[37] Elena Grigorescu, Tali Kaufman, and Madhu Sudan. Succinct representation of codes with applications to testing. In Irit Dinur, Klaus Jansen, Joseph Naor, and José D. P. Rolim, editors, *APPROX-RANDOM*, volume 5687 of *Lecture Notes in Computer Science*, pages 534–547. Springer, 2009.

[38] Charanjit S. Jutla, Anindya C. Patthak, Atri Rudra, and David Zuckerman. Testing low-degree polynomials over prime fields. In *FOCS '04: Proceedings of the Forty-Fifth Annual IEEE Symposium on Foundations of Computer Science*, pages 423–432. IEEE Computer Society, 2004.

[39] Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM J. Comput.*, 36(3):779–802, 2006.

[40] Tali Kaufman and Madhu Sudan. Algebraic property testing: The role of invariance. Technical Report TR07-111, Electronic Colloquium on Computational Complexity, 2 November 2007. Extended abstract in *Proc. 40th STOC*, 2008.

[41] Tali Kaufman and Avi Wigderson. Symmetric LDPC codes and local testing. In *Proceedings of ICS 2010*, January 2010.

[42] Jon M. Kleinberg, editor. *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*. ACM, 2006.

[43] Daniel Král', Oriol Serra, and Lluis Vena. A removal lemma for systems of linear equations over finite fields. `arxiv.org:0809.1846v1 [math.CO]`.

[44] Daniel Král', Oriol Serra, and Lluis Vena. A combinatorial proof of the removal lemma for groups. *Journal of Combinatorial Theory, Series A*, 116(4):971–978, 2009.

[45] Richard E. Ladner and Cynthia Dwork, editors. *Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, British Columbia, Canada, May 17-20, 2008*. ACM, 2008.

[46] Kevin Matulef, Ryan O'Donnell, Ronitt Rubinfeld, and Rocco A. Servedio. Testing halfspaces. In Claire Mathieu, editor, *SODA*, pages 256–264. SIAM, 2009.

[47] Michael Mitzenmacher, editor. *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*. ACM, 2009.

[48] Krzysztof Onak and Madhu Sudan. Learnability of general discrete distributions. Manuscript, March 2010.

[49] Michal Parnas, Dana Ron, and Alex Samorodnitsky. Testing basic boolean formulae. *SIAM J. Discrete Math.*, 16(1):20–46, 2002.

[50] Sofya Raskhodnikova, Dana Ron, Amir Shpilka, and Adam Smith. Strong lower bounds for approximating distribution support size and the distinct elements problem. *SIAM J. Comput.*, 39(3):813–842, 2009.

[51] Ronitt Rubinfeld. Robust functional equations and their applications to program testing. *SIAM Journal on Computing*, 28(6):1972–1997, 1999.

[52] Ronitt Rubinfeld and Rocco A. Servedio. Testing monotone high-dimensional distributions. *Random Struct. Algorithms*, 34(1):24–44, 2009.

[53] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, 1996.

[54] Asaf Shapira. Green's conjecture and testing linear-invariant properties. In Mitzenmacher [47], pages 159–166.

[55] Paul Valiant. Testing symmetric properties of distributions. In Ladner and Dwork [45], pages 383–392.