Algebraic Property Testing: The Role of Invariance

Tali Kaufman* Madhu Sudan†

ABSTRACT

We argue that the symmetries of a property being tested play a central role in property testing. We support this assertion in the context of algebraic functions, by examining properties of functions mapping a vector space $\mathbb{K}^n$ over a field $\mathbb{K}$ to a subfield $\mathbb{F}$. We consider ($\mathbb{F}$-)linear properties that are invariant under linear transformations of the domain and prove that an $O(1)$-local "characterization" is a necessary and sufficient condition for $O(1)$-local testability, when $|\mathbb{K}| = O(1)$. (A local characterization of a property is a definition of a property in terms of local constraints satisfied by functions exhibiting a property.) For the subclass of properties that are invariant under *affine* transformations of the domain, we prove that the existence of a *single* $O(1)$-local constraint implies $O(1)$-local testability. These results generalize and extend the class of algebraic properties, most notably linearity and low-degree-ness, that were previously known to be testable. In particular, the extensions include properties satisfied by functions of degree linear in n that turn out to be $O(1)$-locally testable.

Our results are proved by introducing a new notion that we term "formal characterizations". Roughly this corresponds to characterizations that are given by a single local constraint and its permutations under linear transformations of the domain. Our main testing result shows that local formal characterizations essentially imply local testability. We then investigate properties that are linear-invariant and attempt to understand their local formal characterizability. Our results here give coarse upper and lower bounds on the locality of constraints and characterizations for linear-invariant properties in terms of some structural parameters of the property we introduce. The lower bounds rule out any characterization, while the upper bounds give formal characterizations. Combining the two gives a test for all linear-invariant properties with local characterizations.

We believe that invariance of properties is a very interesting notion to study in the context of property testing in general and merits a systematic study. In particular, the class of linear-invariant and affine-invariant properties exhibits a rich variety among algebraic properties and offer better intuition about algebraic properties than the more limited class of low-degree functions.

Categories and Subject Descriptors

F.2.0 [**Theory of Computation**]: Analysis of Algorithms and problem complexityGeneral

General Terms

Theory

Keywords

Error-correcting codes, Locally testable codes, Sublinear time algorithms

1. INTRODUCTION

Property testing considers the task of testing efficiently, by random sampling, if a function mapping a finite domain to a finite range "essentially" satisfies a given property. A property to be tested can be specified by the family of functions $\mathcal{F}$ that possess the property. A property specified by a family $\mathcal{F}$ is *k-locally testable* if there exists a randomized test that queries the value of a function f on k inputs and accepts if $f \in \mathcal{F}$ and rejects $f \notin \mathcal{F}$ with probability lower bounded by a quantity proportional to the distance of f from $\mathcal{F}$. Proximity of functions is measured in terms of its relative Hamming distance $\delta(f, g) = \Pr_x[f(x) \neq g(x)]$ when x is chosen uniformly from the finite domain. A function f is δ-close to $\mathcal{F}$ if there exists a $g \in \mathcal{F}$ such that $\delta(f, g) \leq \delta$ and δ-far otherwise.

The study of property testing emerged in the wake of the linearity test of Blum, Luby, and Rubinfeld [4] and was defined formally in Rubinfeld and Sudan [19]. The first substantial investigation of property testing occurred in Goldreich, Goldwasser, and Ron [10] who focussed on the testing of properties of combinatorial objects, in particular of graphs. Subsequent works have lead to major strides in the testing of graph properties culminating with the works of Alon et al. and Borgs et al. [1, 6]. The testing of algebraic properties has also seen significant progress since [4, 19] including testing of functions satisfying functional equations [18], and testing of various algebraic properties leading to error-correcting codes e.g. testing of Reed-Muller codes [2], generalized Reed-Muller codes [16, 13], dual-BCH codes [15]. On the negative side, the works of Bogdanov, Obata, and Trevisan [5] and Ben-Sasson, Harsha,and Raskhodnikova [3] give properties that are not locally testable.

In the light of this progress it is natural to ask: What are the essential features that make a property testable. In the context of

*IAS, Princeton. kaufmant@mit.edu. Research supported in part by NSF Awards CCF-0514167 and NSF-0729011.

†MIT CSAIL. madhu@mit.edu. Research supported in part by NSF Award CCR 0514915.

STOC'08, May 17–20, 2008, Victoria, British Columbia, Canada.

graph-property testing (in the "dense-graph" model) this question is answered by the works of [1, 6], who show that a certain feature that they term "regularity" is necessary and sufficient for testing graph properties. In the algebraic setting, a similar understanding of properties that lead to local testability is lacking. In this paper we take some steps to remedy this.

1.1 Invariance and Property Testing:

Our approach to (algebraic) property testing is to attribute testability to some "invariance" features exhibited by the property. Invariance features of a family $\mathcal{F}$, especially under permutations of the domain, seems naturally linked to property testing. For example, let us consider the test for "majority" (the property $\mathcal{F}$ consisting of all functions $f : \{1, \ldots, N\} \to \{0, 1\}$ that take the value 1 at least $N/2$ times). This test is considered uninteresting and we propose a formal explanation. This test actually uses the symmetry of the property $\mathcal{F}$, and the symmetry required is the full group of permutations over the domain. Indeed the test easily extends to any other "symmetric" property $\mathcal{F}$ of Boolean functions, which has the feature that if $f \in \mathcal{F}$ and π is a permutation on the domain, the $f \circ \pi(x) = f(\pi(x))$ is also in $\mathcal{F}$. A formal reason to declare the test "obvious" may be that the group of invariances needed in $\mathcal{F}$ is so large (qualitatively).

Graph property testing similarly revolves around symmetries. This setting consider functions $A : \{1, \ldots, n\} \times \{1, \ldots, n\} \to \{0, 1\}$, and properties that are invariant under permutations that permute rows and columns simultaneously. The groups of symmetries thus is somewhat smaller ($(\sqrt{N})!$ as opposed to $N!$, where $N = n^2$ is the domain size). But now one needs some more features (monotonicity/heredity) to get property testers [1, 6]. Despite this natural link between property testing and invariances, this link does not seem to have been explicit in prior literature. We make it explicit here. We remark that in independent work, Goldreich and Sheffet [11], also make this notion explicit, and use it to understand the randomness complexity needs of property testing.

In this paper we explore invariances of an algebraic kind. To do so, we consider functions mapping an n-dimensional vector space over a finite field $\mathbb{K}$ to a subfield $\mathbb{F}$ of $\mathbb{K}$. Among such functions the families $\mathcal{F}$ we consider satisfy two properties:

1. They are $\mathbb{K}$-*linear invariant* (or simply *linear invariant*), i.e., for every function $f \in \mathcal{F}$, and linear map $L : \mathbb{K}^n \to \mathbb{K}^n$ (i.e., a function that satisfies $\alpha L(\mathbf{x}) + \beta L(\mathbf{y}) = L(\alpha\mathbf{x} + \beta\mathbf{y})$ for every $\alpha, \beta \in \mathbb{K}$ and $\mathbf{x}, \mathbf{y} \in \mathbb{K}^n$), it is the case that $f \circ L$, given by $(f \circ L)(\mathbf{x}) = f(L(\mathbf{x}))$, is also in $\mathcal{F}$. If such a closure holds for all affine maps L from $\mathbb{K}^n$ to $\mathbb{K}^n$, then the property $\mathcal{F}$ is said to be *affine-invariant*.

2. They are $\mathbb{F}$-*linear* (or simply *linear*), i.e., for every pair of functions $f, g \in \mathcal{F}$ and $\alpha, \beta \in \mathbb{F}$ it is the case that the function $\alpha f + \beta g$ is also in $\mathcal{F}$. This is the property that typically leads to linear codes over the alphabet $\mathbb{F}$.

In the algebraic context, linear-invariance over the domain seems to be a natural class of invariances (though not necessarily the only class) to consider, and may be viewed as analogous to the choice of working with "graph-properties". The linearity of the family $\mathcal{F}$ (when viewed as a vector space over the range) is an additional property we impose to derive some testability results (analogous to the role played by heredity/monotonicity in graph property testing).

For simplicity we suppress the use of the phrase "$\mathbb{F}$-linear" in this paper, and use the term linear-invariant (affine-invariant) family to reflect families which are both linear-invariant (resp. affine-invariant) and linear. (We stress that this is merely a notational choice. It maybe quite interesting to study non-linear properties that are linear-invariant also, but we don't do so here.)

The resulting collection of families unify most previously considered in algebraic settings. They include the class of linear functions, low-degree polynomials (and thus generalized Reed-Muller codes), as well as the dual-BCH codes. But they also include other families such as homogenous polynomials of any given degree and linearized polynomials. They satisfy nice closure properties e.g., if $\mathcal{F}_1$ and $\mathcal{F}_2$ are linear-invariant, then so are $\mathcal{F}_1 \cap \mathcal{F}_2$ and $\mathcal{F}_1 + \mathcal{F}_2$, the family that consists of the sum of functions from $\mathcal{F}_1$ and $\mathcal{F}_2$. Finally, we remark that the group of symmetries required by linear-invariance is relatively tiny, and only quasipolynomial in the domain size, compared to the exponential sizes relied upon in the symmetric properties as well as in graph properties.

Our principal results are to show necessary and sufficient conditions for testing linear-invariant families mapping $\mathbb{K}^n$ to $\mathbb{F}$. The results hold for all choices of $\mathbb{K}$ and $\mathbb{F}$ as $n \to \infty$, but are specially strong when $|\mathbb{K}| = O(1)$. We describe our results, and approach, below.

1.2 Constraints, Characterizations, Formal Characterizations, Testing:

To understand necessary conditions for local testability, we start by recalling the some basic notions in this context, namely those of "constraints" and "characterizations".

We say that a family $\mathcal{F}$ satisfies a *constraint* $C = (x_1, \ldots, x_k; S)$ where $x_1, \ldots, x_k \in \mathbb{K}^n$ and $S \subsetneq \mathbb{F}^k$ if every member $f \in \mathcal{F}$ satisfies $\langle f(x_1), \ldots, f(x_k) \rangle \in S$. We refer to this constraint as a k-local constraint. In order for a property to be k-locally testable, with one-sided error, it must be the case that functions in the family satisfy some k-local "constraint" (since every rejected function must be rejected with a proof of non-membership in the family). Local constraints also essential for a family of functions to be local-correctible and indeed it turns out that all function families we analyze are locally correctable.

Testable properties where every non-member is rejected with positive probability (as required by our definition of a local test) actually need to show even more structure. Specifically, it must be that there is some set of local constraints that completely *characterize* the family, i.e., $f \in \mathcal{F}$ if and only if it satisfies every one of the given set of k-local constraints. (See Definition 2.1 for a formal definition.) In this paper we will consider all function families that are linear invariant and have a local characterization and show that they are testable.

To derive this result we examine the source of the local characterizability of a family. Local characterizability of a family requires that a family be specified by *several* local constraints. In examining the features that lead to property testing it is natural to ask for an explanation for this abundance of local constraints. One way to explain them is via the invariance features of the family. If a family satisfies one local constraint, then every "permutation" of the domain that preserves membership in the family yields a potentially new local constraint. In our case, thus the abundance of constraints can be explained by the linear invariance of the family. Every linear transformation of a constraint, leads to another valid constraint, and together this set can be quite large. Motivated by this, we introduce the notion of a *formal characterization*, which requires that the family be specified by a *single* constraint and its "orbit", i.e., all the other constraints obtained by linear transformations of the given one, characterize the family. (The actual definition allows a slightly broader class of characterizations, see Definition 2.3.) Modulo the formal definitions of these objects, we can state our first theorem informally as follows:

Main Theorem 1 (Informal): *If a family $\mathcal{F}$ is linear-invariant and has a k-local formal characterization, which satisfies some additional restrictions, then it is k-locally testable.* (See Theorem 2.9 for a formal statement.)

The requirement that a single constraint and its orbit characterize a family may seem overly restrictive, but known characterizations of most algebraic functions including those from [4, 19, 2, 16, 13] are actually formal and satisfy the (thus far unspecified) additional restrictions (see Proposition 2.7). As a result Theorem 2.9 already subsumes many of the algebraic testing results. Moreover, as discussed later in this section, the proof is actually somewhat simpler and unifies the different proofs presented in the literature for the different cases.

Our other main results show that the above theorem actually gives testers for all linear-invariant families provided the family is locally characterizable, a clear necessary condition. For the special case of affine-invariant families, we show that the existence of a *single* local constraint suffices to establish testability. Again we describe these theorems informally below.

Main Theorem 2 (Informal): *If a family $\mathcal{F}$ is affine-invariant and has a k-local constraint, then it has a $k^{\mathrm{poly}(|\mathbb{K}|)}$-local formal characterization which satisfies the additional restrictions mentioned in Main Theorem 1 (Informal). Hence $\mathcal{F}$ is $k^{\mathrm{poly}(|\mathbb{K}|)}$-locally testable.* (See Theorem 2.10 for a formal statement.)

Thus when $|\mathbb{K}| = O(1)$, the above pins down the local testability to with polynomial factors. Moving to the case of linear-invariant families, here we do get local formal characterizations, but they do not satisfy the additional restrictions described in Theorem 2.9. However, we still manage to use the theorem to give a local tester for all such families.

Main Theorem 3 (Informal): *If a family $\mathcal{F}$ is linear-invariant and has a k-local characterization, then it has a $k^{\mathrm{poly}(|\mathbb{K}|)}$-local formal characterization (which need not satisfy the additional restrictions mentioned in Main Theorem 1 (Informal)). Furthermore, $\mathcal{F}$ is $k^{\mathrm{poly}(|\mathbb{K}|)}$-locally testable.* (See Theorem 2.11 for a formal statement.)

1.3 Significance of results:

The significance of the results depend on the "novelty" of the class of properties that are linear-invariant, and have local constraints or characterizations. At first look it may appear that linear-invariance is just a rephrasing of the notion of being low-degree polynomials[1]. Indeed we even prove that when $\mathbb{K} = \mathbb{F} = \mathbb{Z}_p$ is a prime field then the only *affine-invariant* families are polynomials of a given bound on their degree. However each restriction, $\mathbb{K} = \mathbb{F}$, $\mathbb{F} = \mathbb{Z}_p$ and the affine-invariance of $\mathcal{F}$ (as opposed to mere linear-invariance), when relaxed leads to a broader set of properties.

For instance, when $\mathbb{K} = \mathbb{F}$ and $\mathbb{F}$ is not a prime field, then the class of "linearized polynomials" lead to an interesting collection of "high-degree" polynomials that are affine-invariant, but testable with much greater locality than their degree would suggest. (Linearized polynomials over the field $\mathbb{F}$ of cardinality p^s for prime p and $s > 1$ are functions of the form $\sum_{i=0}^{s-1} c_i x^{p^i}$.) In the full version of this paper [17], we give a generalization of this result to multivariate polynomials of p-degree greater than 1, giving a moderately broad class of functions that are very locally testable using

[1]We remark that it is not possible to deny that every property from $\mathbb{K}^n$ to $\mathbb{F}$ is a property of "polynomials", since every function is from $\mathbb{K}^n$ to $\mathbb{F}$ is a polynomial. However this is no more interesting than saying that some property is $|\mathbb{K}|^n$-locally testable! What we claim here, and show later in the paper, is that the class of properties showing linear-invariance is not just polynomials of a given upper bound on the degree.

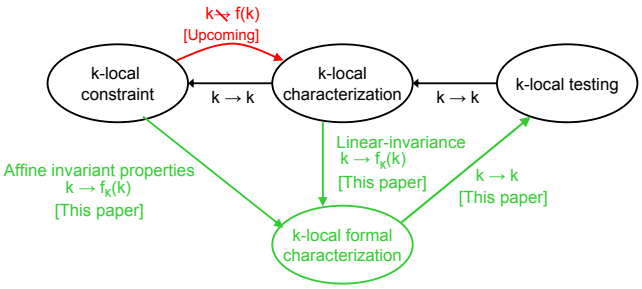

Figure 1: Informal summary of the notions and results in this paper.

Theorem 2.9.

Moving to the case where $\mathbb{K} \neq \mathbb{F}$, a priori it is not even clear that it is good to think of them as polynomials over $\mathbb{K}$ (though as noted earlier, every function from $\mathbb{K}^n$ to $\mathbb{K}$, and hence from $\mathbb{K}^n$ to $\mathbb{F}$, is a polynomial with coefficients from $\mathbb{K}$). Every non-constant function takes on a constant value $1/|\mathbb{F}|$ fraction of the times and so must be a very high degree polynomial over $\mathbb{K}$ (of degree at least $|K|/|F|$). Yet they can be locally testable with $O(1)$ locality, again suggesting that the "degree" of polynomials in the set is not a good way to measure their testability. This class of functions are interesting in that they capture the "dual-BCH" codes studied (in the context of property testing) by Kaufman and Litsyn [15]. In the full version of this paper [17], we give some basic structural results about such functions which allows us to get some weak, but general, results about testing multivariate versions of such functions.

The strongest contrast from low-degree polynomials however comes when studying linear-invariant (as opposed to affine-invariant) families. In the previous cases, it was the structure within the field $\mathbb{K}$ that played a central role in differentiating the properties under consideration from the class of low-degree polynomials. While this distinction led to some nice examples, the "coarseness" of our general results (Informal Theorems 2 and 3 above) is weak to capture this distinction. In the case of linear-invariant families, homogenous polynomials start to play a special role and this role is quantitatively much more significant. For example consider the set of n-variate polynomials over $\mathbb{Z}_3$ supported on monomials of odd degree or monomials of degree at most 10. It can be verified that this a linear-invariant family. On the one hand this set includes polynomials of degree upto $2n-1$, and indeed the supporting set of monomials has cardinality at least 2^n. However, it turns out that this family is testable with $O(1)$-locality independent of n Indeed Lemma 5.11 gives a broad generalization of this example to a rich collection of non-low-degree polynomials that are locally testable.

We remark that linear-invariance also leads to other rich effects. As mentioned above, the class of homogenous polynomials of degree d is linear-invariant and $O(d)$-locally testable. Also if $\mathcal{F}_1$ and $\mathcal{F}_2$ are linear-invariant, then so is $\mathcal{F}_1 + \mathcal{F}_2$. It follows that if both are locally testable then so is $\mathcal{F}_1 + \mathcal{F}_2$ (see the full version [17]).

In summary, we assert that the class of linear-invariant properties mapping $\mathbb{K}^n$ to $\mathbb{F}$ form a rich enhancement of the class of low-degree polynomials and our results here show how to extend some of the property testing results to the enhanced collection of properties.

1.4 Techniques:

Our techniques belong into three different categories.

Unification of previous testing results by Tensor product of codes. Our testing result (Informal Theorem 1) unifies, simplifies and gen-

eralizes the proof of the robustness result from several prior works [4, 19, 2, 16, 13]. The later works in this sequence built on the proof structure developed in [4], but then needed to find new ways to address the many variants of a common technical problem that arose in all the proofs. Our insight in this work is to notice that all these problems were hovering around the concept of "tensor products" of linear spaces (or codes). By extracting this element explicitly (see proofs of Lemmas 3.1 and 3.3) we are able to find a single proof (not much more complicated than the first) that simultaneously solves all the problems. We remark that this proof does not specialize to any of the previous proofs, not even in the case of [4]. Previous proofs were more "efficient" in terms of the tradeoff between the rejection probability of the test and the distance from the family $\mathcal{F}$. By sacrificing this efficiency we are able to unearth some of the underlying reasons for why testing works. Given the central role of linearity and low-degree testing in complexity theory, we hope that the additional understanding will be of technical benefit in the future.

Structural theorems for linear invariant families. Our structural theorems about linear-invariant families (Informal Theorems 2 and 3) are based on a careful analysis of polynomials mapping $\mathbb{K}^n$ to $\mathbb{F}$. Recalling that every function from $\mathbb{K}^n$ to $\mathbb{F}$ can be viewed as a n-variate polynomial over $\mathbb{K}$, we ask questions of the form, what does a linear invariant family $\mathcal{F}$ containing a single function (polynomial) f look like? We present some very simple but broadly useful lemmas in this context, which we describe first for the simple case when $\mathbb{K} = \mathbb{F}$. We give a "monomial extraction lemma", Lemma 4.2, which shows that every monomial appearing in the support of f is also in $\mathcal{F}$ (where we view the monomial also as a function from $\mathbb{F}^n$ to $\mathbb{F}$). For example, any linear-invariant family containing the polynomial $x^2 + xy^2 + y^4$ also contains the function xy^2. This turns our attention to linear invariant families $\mathcal{F}$ that contain some given monomial m. We show a "monomial spreading lemma", Lemma 4.3, which describes many other monomials that should be contained in $\mathcal{F}$ as well. For example a family containing the monomial x^2y^3 over a field of characteristic greater than 5 also contains the monomials x^5 and xy^4 etc. We show a similar (more general) variant for affine-invariant families also. These lemmas, though simple, forge the path for a better understanding of linear-invariant and affine-invariant families. In particular they say that these families are completely characterized by the monomials in the families. In the case of affine-invariant families, the maximum degree of the monomials in the family forms a good, though crude, bound on the locality of the characterizations/tests of the family, and this leads to the Informal Theorem 2 above.

For linear-invariant families however, the degree turns out to be the wrong measure to estimate the locality of characterizations or tests. Instead we introduce a new parameter that we call the *linear-invariance degree* of a family. For example, for the earlier-mentioned example of the family mapping $\mathbb{Z}_3^n$ to $\mathbb{Z}_3$ supported on all monomials of odd degree and on other monomials of degree upto 10, the linear-invariance degree turns out to be 10. We show that this invariance degree bounds, again crudely, the locality of the characterization/tests of any family and this leads to the Informal Theorem 3 above, in the case of $\mathbb{K} = \mathbb{F}$.

Systematic study of functions from a field $\mathbb{K}$ to a subfield $\mathbb{F}$. Finally we extend the results to the case of function families mapping $\mathbb{K}^n$ to some subfield $\mathbb{F}$ of $\mathbb{K}$. Thus, our work provides the *first* systematic study of testability of functions from a field to its subfield. In this case we describe a basis for functions mapping $\mathbb{K}^n$ to $\mathbb{F}$, which itself seems new. This basis generalizes in a common way the well-studied "trace" and "norm" functions, both of which map $\mathbb{K}$ to $\mathbb{F}$. These functions, that we refer to as "Traces of monomials", satisfy similar properties to the monomials in the simpler case of functions from $\mathbb{F}^n$ to $\mathbb{F}$. Viewed as a polynomial over $\mathbb{K}$, if a function f has a support on a monomial m, then the trace of the monomial m is itself a function in any linear-invariant family containing f. Furthermore, the presence of one monomial implies the presence of many others in the family, leading to upper and lower bounds on the characterizations/tests of the family.

Organization of this paper:

In Section 2 we introduce some basic definitions needed to present our main results and we provide formal statements of our main results. In Section 3 we prove our main result (Theorem 2.9) on testing linear-invariant families that admit nice formal characterizations. In Sections 4 and 5 we present necessary and sufficient conditions for affine- and linear-invariant families to admit nice formal characterizations, and give outlines of the proofs, for the case when $\mathbb{K} = \mathbb{F}$. Specifically Section 4 presents some general structural properties of linear-invariant families, which are then turned into bounds on the locality of characterizations in Section 5. In Section 6 we discuss conclusions from our work and some future work.

Due to lack of space, all proofs are omitted from Sections 4 and 5 and may be found in the full version of this paper [17]. The full version also includes the study of functions from general fields $\mathbb{K}$ to subfields $\mathbb{F}$, as also examples of some families that possess non-trivially local formal characterizations.

2. DEFINITIONS AND STATEMENT OF RESULTS

We start with some common notation we use. We use $\mathbb{Z}$ to refer to the integers. We use $[n]$ to denote the set $\{1, \ldots, n\}$. Throughout we work with finite fields $\mathbb{F}$ of cardinality $q = p^s$ and $\mathbb{K}$ of cardinality $Q = q^t$. $\mathbb{F}^*$ and $\mathbb{K}^*$ will denote the non-zero elements of the fields. For an integer vector $\mathbf{d} = \langle d_1, \ldots, d_n \rangle$ with $0 \leq d_i < Q$ and $c \in \mathbb{K}^*$, we let $c \cdot \mathbf{x}^{\mathbf{d}}$ denote the monomial $c \cdot \prod_{i=1}^n x_i^{d_i}$. We use $\mathbb{K}[\mathbf{x}]$ to denote polynomials in $\mathbf{x}$ with coefficients from $\mathbb{K}$. We use $\mathcal{L}$ to denote the space of linear functions from $\mathbb{K}^n \to \mathbb{K}^n$ and $\mathcal{A}$ to denote the set of affine functions.

2.1 Robust local tests

We start with the formal definitions of constraints, characterizations and formal characterizations.

DEFINITION 2.1 (k-LOCAL CONSTRAINT/CHARACTERIZATION). *A k-local constraint C is given by k points $\mathbf{x}_1, \ldots, \mathbf{x}_k \in \mathbb{K}^n$ and a set $S \subsetneq \mathbb{F}^k$. We say that a family $\mathcal{F}$ satisfies a* k-local constraint *$C = (\mathbf{x}_1, \ldots, \mathbf{x}_k; S)$ if $\langle f(\mathbf{x}_1), \ldots, f(\mathbf{x}_k) \rangle \in S$ for every $f \in \mathcal{F}$. We say that a family $\mathcal{F}$ has a* k-local characterization *if there exists a collection $\mathcal{C}$ of k-local constraints such that $f \in \mathcal{F}$ if and only if f satisfies all constraints $C \in \mathcal{C}$.*

When the property being tested is $\mathbb{F}$-linear, it is well-known [3] that the set S might as well be an $\mathbb{F}$-linear proper subspace of $\mathbb{F}^k$. In what follows we often use the letter V to denote such a subspace (instead of S).

We now introduce the notion of a k-local formal characterization. We start with a strong and elegant definition, though we will soon switch to a slightly weaker (but more cumbersome) definition that is easier to work with. The strong definition formalizes characterizations derived from linear, or affine, translations of a *single* k-local constraint.

DEFINITION 2.2 (STRONG FORMAL CHARACTERIZATION). *A family of functions $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ has a* strong *k-local formal*

characterization *it there exists a constraint* $C = (\mathbf{x}_1, \ldots, \mathbf{x}_k; V \subseteq \mathbb{F}^k)$ *such that* $f \in \mathcal{F}$ *if and only if for every linear function* $L : \mathbb{K}^n \to \mathbb{K}^n$ *it is the case that* $\langle f(L(\mathbf{x}_1)), \ldots, f(L(\mathbf{x}_k))\rangle \in V$.

Characterizations such as the above are common in property testing. For instance the class of linear functions from $\mathbb{Z}_p^n$ to $\mathbb{Z}_p$, for prime p and $n \geq 2$ can be described by the constraint $C = (\mathbf{a}, \mathbf{b}, \mathbf{a}+\mathbf{b}; V)$ where $\mathbf{a} = \langle 1, 0, \ldots, 0\rangle$, $\mathbf{b} = \langle 0, 1, 0, \ldots, 0\rangle$, and $V = \{\langle \alpha, \beta, \alpha+\beta\rangle | \alpha, \beta \in \mathbb{Z}_p\}$. Similarly, the class of degree d polynomials mapping $\mathbb{Z}_p^n$ to $\mathbb{Z}_p$, for $d \leq p$ and $n \geq 2$ can be described by the constraint $C = (\mathbf{a}, \mathbf{a}+\mathbf{b}, \mathbf{a}+2\mathbf{b}, \ldots, \mathbf{a}+(d+1)\mathbf{b}; V_d)$ where $V_d = \{\langle \alpha_0, \ldots, \alpha_{d+1}\rangle \in \mathbb{F}^{d+2} | \sum_{i=0}^{d+1} (-1)^i \binom{d+1}{i} \alpha_i = 0\}$. More complex expressions can be found for functions mapping polynomials over any (esp. a non-prime) field to itself. However all these definitions do restrict n to be at least 2, which is somewhat artificial. Also for technical reasons we will use a "dual" (and weaker) notion of a "formal" constraint.

In the above version, a formal characterization may be viewed as being given by a collection of constraints: one for every linear map from $\mathbb{K}^n$ to $\mathbb{K}^n$. In the "dual" version below, we will consider a collection of constraints which are parametrized by a constant number of variables taking values in $\mathbb{K}^n$. The "variables" of a constraint, i.e., locations examined by the constraint, are linear functions of the parameters. As usual the constraint requires that the vector of function values at the specified locations come from the set S.

DEFINITION 2.3 ((WEAK) k-FORMAL CHARACTERIZATION). *A family* $\mathcal{F}$ *has a (weak)* k*-local formal characterization if there exists an integer* m*;* k *linear functions* $\ell_1, \ldots, \ell_k : (\mathbb{K})^m \to \mathbb{K}$*; and a linear subspace* $V \subset \mathbb{F}^k$ *such that* $f \in \mathcal{F}$ *if and only if for every* $y_1, \ldots, y_m \in \mathbb{K}^n$*, we have* $\langle f(x_1), \ldots, f(x_k)\rangle \in V$*, where* $x_i = \ell_i(y_1, \ldots, y_m)$*. (Here we interpret the linear function* ℓ_i *as a map from* $(\mathbb{K}^n)^m \to \mathbb{K}^n$ *in the natural way.)*

The following proposition establishes a fairly close connection between strong and weak formal characterizations.

PROPOSITION 2.4. *A family* $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ *has a weak* k*-local formal characterization if is it has a strong* k*-local formal characterization. If* $n \geq k$ *then the converse also holds.*

PROOF. Let $C = (\mathbf{x}_1, \ldots, \mathbf{x}_k; V)$ give a strong formal characterization of $\mathcal{F}$. Renumber $\mathbf{x}_1, \ldots, \mathbf{x}_k$ so that the vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m$ are linearly independent and $\mathbf{x}_j = \sum_{i=1}^m \lambda_{ij}\mathbf{x}_i$ for $j \in \{m+1, \ldots, k\}$. Now let $\ell_1, \ldots, \ell_k : \mathbb{K}^m \to \mathbb{K}$ be defined as $\ell_j(z_1, \ldots, z_m) = z_j$ if $j \leq m$ and $\ell_j(z_1, \ldots, z_m) = \sum_{i=1}^m \lambda_{ij} z_i$ for $j \in \{m+1, \ldots, k\}$. Then it can be easily seen that $\ell_1, \ldots, \ell_k$ and V give a weak formal characterization of $\mathcal{F}$.

In the other direction, suppose $\ell_1, \ldots, \ell_k : \mathbb{K}^m \to \mathbb{K}$ and V give a weak formal characterization of $\mathcal{F}$. Let $\alpha_1, \ldots, \alpha_m \in \mathbb{K}^n$ be linearly independent vectors in $\mathbb{K}^n$. (Note such a collection exist since $m \leq k \leq n$.) Let $\mathbf{x}_1, \ldots, \mathbf{x}_k$ be given by $\mathbf{x}_j = \ell_j(\alpha_1, \ldots, \alpha_m)$. Then it can be verified that the constraint $(\mathbf{x}_1, \ldots, \mathbf{x}_k; V)$ gives a strong formal characterization of $\mathcal{F}$. ∎

Henceforth whenever we refer to formal characterizations, we mean weak ones. The formal version of the Informal Theorems 1, 2, and 3 rely on some restricted classes of formal characterizations that we specify below.

DEFINITION 2.5 (2-ARY INDEPENDENT). *A* k*-local formal characterization* $(\ell_1, \ldots, \ell_k; V)$ *is* 2-ary independent *if* ℓ_1 *and* ℓ_j *are linearly independent for every* $j \in \{2, \ldots, k\}$*. If all the* ℓ_i*'s are of the form* $y_1 + \tilde{\ell}_i(y_2, \ldots, y_m)$*, where* $\tilde{\ell}_i$*'s are non-zero, then we say that the characterization is an* affine *characterization. (Note that every affine characterization is also 2-ary independent.)*

In the propositions below, we mention some general results on the existence of formal local characterizations. The first gives a general transformation, which may be quite weak for large $\mathbb{K}$, but is quite useful for small $\mathbb{K}$. The second summarizes known (quite strong) characterizations in our terms. Both proofs are omitted.

PROPOSITION 2.6. *For every* $\mathbb{K}$ *there exists a function* $g = g_{\mathbb{K}} : \mathbb{Z} \to \mathbb{Z}$ *such that if* $\mathcal{F}$ *has a* k*-local characterization, then it has a* $g(k)$*-local formal characterization.*

PROPOSITION 2.7 (FOLLOWS FROM [7, 16]). *The set* $\mathcal{F}_{n,d,\mathbb{F}}$ *of* n*-variate polynomials of degree at most* d *over* $\mathbb{F}$ *(so here* $\mathbb{K} = \mathbb{F}$*) of cardinality* $q = p^s$*, have a* $d+2$*-local formal characterization, if* $d \leq q - q/p$*, and a* $q^{\lceil d/(q(1-1/p))\rceil}$*-local formal characterization if* $d \geq d(1-1/p)$*. In both cases, the formal characterizations are affine.*

A much wider class of properties (other than just the class of low-degree polynomials) have local characterizations. We discuss this in detail shortly, but first we describe a natural test for properties with local formal characterizations.

DEFINITION 2.8 (LINEAR-INVARIANT TEST). *For family* $\mathcal{F}$ *that has a formal local characterization given by* $(\ell_1, \ldots, \ell_k; V)$*, the linear-invariant test is defined to be: "Pick* $x_1, \ldots, x_m \in \mathbb{K}^n$ *at random and accept if and only if* $\langle f(y_1), \ldots, f(y_k)\rangle \in V$*, where* $y_i = \ell_i(x_1, \ldots, x_m)$*."*

We can now state our main theorem, which formalizes the Informal Theorem 1 of Section 1, for testing linear-invariant families with local formal characterization.

THEOREM 2.9. *If* $\mathcal{F}$ *is a (linear invariant) family of functions mapping* $\mathbb{K}^n$ *to* $\mathbb{F}$*, with a 2-ary independent* k*-local formal characterization, then it is* k*-locally testable. Specifically, the linear-invariant test accepts all members of* $\mathcal{F}$*, while a function* f *that is* δ*-far from* $\mathcal{F}$ *is rejected with probability* $\min\left\{\frac{\delta}{2}, \frac{1}{(2k+1)(k-1)}\right\}$.

We prove the local testing part of this Theorem in Section 3. In particular, note that in all cases the rejection probability is independent of n and $\mathbb{K}$. So if $k = O(1)$, then the rejection probability is $\Omega(\delta)$.

For well-known linear-invariant families such as linear functions [4], and Reed-Muller codes [19, 2, 16, 13], the theorem above produces local tests with the same locality as in the previous works, though the rejection probability may be slightly smaller in our case. The rest of this section describes property tests that we can derive that are not already captured by previous results.

To do so we study invariance properties of functions mapping $\mathbb{K}^n$ to $\mathbb{F}$. All functions from $\mathbb{K}^n$ to $\mathbb{F}$ are polynomials. So the principal questions we study here are: "Which subsets of polynomials are linear (or affine) invariant?" and "Which of these families have k-local formal characterizations?"

We differentiate our results into two categories: those for affine-invariant families and those for linear-invariant families. In both cases, as argued earlier there is a rich variety of function families that are not "merely" low-degree polynomials. However in the case of affine-invariant families, the maximum degree of functions in the family does give a crude bound on the locality of characterizations and tests for the family. On the one hand families that contain even a single high-degree function cannot satisfy any local constraint; and on the other hand families with only low-degree functions have local formal characterizations (see Lemmas 5.5 and 5.6 for the case when $\mathbb{K} = \mathbb{F}$ and the full version [17] for the general case). For

affine-invariant families, the characterizations can be converted to affine-invariant, and hence 2-ary independent ones, one can now apply Theorem 2.9 to get a testing result as well. This leads us to the following theorem, which formalizes Informal Theorem 2.

THEOREM 2.10. . *For fields $\mathbb{F} \subseteq \mathbb{K}$ with $|\mathbb{F}| = q$ and $|\mathbb{K}| = Q$, let $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ be an affine-invariant family with a k-local constraint. Then $\mathcal{F}$ has a $k' = (Q^2k)^{Q^2}$-local formal affine characterization. Furthermore $\mathcal{F}$ is k'-locally testable, where the test accepts members of $\mathcal{F}$ with probability 1 and rejects functions that are δ-far with probability* $\min\left\{\frac{\delta}{2}, \frac{1}{(2k'+1)(k'+1)}\right\}$.

Theorem 2.10 is proved in the full version [17], though the simpler case where $\mathbb{K} = \mathbb{F}$ is proved in Section 5.

The gap between the upper and lower bounds in the above theorem is quite weak. Partly, this is because the degree of the polynomial in a family is only a weak estimator of the locality of characterizations. In the full version of this paper [17], we give an example of a family mapping $\mathbb{F}^n$ to $\mathbb{F}$ where the degree is larger than the locality of the characterization by a factor of about q/p. This example is interesting in its own right in that it shows some of the ways in which affine-invariant families differ from families of low-degree polynomials.

In the case of linear-invariant families, the degree is no longer even a crude estimator of the locality of characterizations. In Section 5 we introduce the notion of the linear-invariance degree of a family (for the case $\mathbb{K} = \mathbb{F}$) and use this parameter to derive upper bounds on the locality of formal characterizations, while also deriving lower bounds on the locality of (any) characterization (see Lemmas 5.4 and 5.7). Extensions of the notion of linear-invariance degree and the bounds on characterizations for the case of general $\mathbb{K}$ and $\mathbb{F}$ are presented in the full version of this paper [17].

The characterizations in the upper bound, unfortunately, are not 2-ary independent. However we manage to reduce the testing of linear-invariant families to some related families that do have 2-ary independent characterizations. This allows us to use Theorem 2.9, in a slightly more involved way, to get local tests for linear-invariant families as well. The following theorem, which formalizes Informal Theorem 3, summarizes this investigation.

THEOREM 2.11. . *For fields $\mathbb{F} \subseteq \mathbb{K}$ with $|\mathbb{F}| = q$ and $|\mathbb{K}| = Q$, let $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ be an linear-invariant family with a k-local characterization. Then $\mathcal{F}$ has a $k' = (Q^2k)^{Q^2}$-local formal characterization. Furthermore $\mathcal{F}$ is k_0-locally testable, for $k_0 = 2Qk'$ where the test accepts members of $\mathcal{F}$ with probability 1 and rejects functions that are δ-far with probability* $\min\left\{\frac{\delta}{2}, \frac{Q^2}{(2k_0+Q)(k_0+Q)}\right\}$.

Again, the full version of Theorem 2.11 is proved in the full version, though the simpler case where $\mathbb{K} = \mathbb{F}$ is proved in Section 5.

3. LOCAL TESTING FROM LOCAL FORMAL CHARACTERIZATIONS

In this section we prove Theorem 2.9 which asserts that a linear-invariant family $\mathcal{F}$ with a 2-ary independent k-local formal characterization is k-locally testable, by the linear-invariant test for $\mathcal{F}$.

In particular, the theorem implies that every affine-invariant family $\mathcal{F}$ with a k-local formal characterization is testable.

Recall the linear-invariant test picks $x_1, \ldots, x_m \in \mathbb{K}^n$ at random and accepts if and only if $\langle f(y_1), \ldots, f(y_k)\rangle \in V$, where $y_i = \ell_i(x_1, \ldots, x_m)$ for $i \in [k]$.

Let $\epsilon(f)$ denote the probability that the linear-invariant test rejects a function f. It is clear that if $f \in \mathcal{F}$ then $\epsilon(f) = 0$. So to prove Theorem 2.9 for the case of 2-ary independent formal characterizations, it suffices to show that if $\epsilon(f) < \frac{1}{(2k+1)(k-1)}$, then $\delta(f, \mathcal{F}) \leq 2\epsilon(f)$.

We start by making some notational simplifications. For $i \in [k]$ and $j \in [m]$, let $c_{ij} \in \mathbb{K}$ be such that $\ell_i(x_1, \ldots, x_m) = \sum_{j=1}^m c_{ij}x_j$. Without loss of generality, we assume that the first m linear functions simply project on to the first m coordinates; i.e., $\ell_i(x_1, \ldots, x_m) = x_i$ for $i \in [m]$. (This can be achieved by a linear transformation of the variable $x_1, \ldots, x_m$ and by permuting the ℓ_i's.) Furthermore, we assume the remaining coordinates are linearly independent of x_1 and so for every $i \neq 1$, the vector $\langle c_{i2}, \ldots, c_{im}\rangle \neq 0$.

Fix a function f with $\epsilon(f) < 1/((2k+1)(k-1))$. As in [4], we now describe a function $g : \mathbb{K}^n \to \mathbb{F}$ that is close to f, that will turn out to be a member of $\mathcal{F}$. For any choice of values $\alpha_2, \ldots, \alpha_k \in \mathbb{F}$ notice that there is at most one $\alpha \in \mathbb{F}$ such that $\langle \alpha, \alpha_2, \ldots, \alpha_k\rangle \in V$. Define $\text{DECODE}(\alpha_2, \ldots, \alpha_k)$ to be this α if it exists (and a special symbol $\perp$ denoting error otherwise). For $x \in \mathbb{K}^n$ and let $\text{Sc}^f(x; x_2, \ldots, x_m) = \text{DECODE}(f(y_2), \ldots, f(y_k))$ where $y_i = \ell_i(x, x_2, \ldots, x_m)$. Note that $\epsilon(f)$ equals the probability that $f(x) \neq \text{Sc}^f(x; x_2, \ldots, x_m)$, when $x, x_2, \ldots, x_m$ are chosen uniformly and independently from $\mathbb{K}^n$. In particular $f(x) = \text{Sc}^f(x; x_2, \ldots, x_m)$ for every $x, x_2, \ldots, x_m$ if and only if $f \in \mathcal{F}$.

Finally, we are ready to define the function g, which we claim to be the function close to f that is in $\mathcal{F}$. For $x \in \mathbb{K}^n$, let $g(x) = \text{plurality}_{\alpha \in (\mathbb{K}^n)^{m-1}} \text{Sc}^f(x, \alpha)$.

We now follow the same sequence of steps as in [4]. It is straightforward to show that f is close to g and we do so in Lemma 3.2. But before we do so, we move to the crucial step, which is to prove that the plurality above is really an overwhelming majority for every x. We show this first in Lemma 3.1. Finally, a proof similar to that of Lemma 3.1 shows that g must be a member of $\mathcal{F}$ and we do so in Lemma 3.3. Theorem 2.9 follows easily from these lemmas.

LEMMA 3.1. *For every $x \in \mathbb{K}^n$, $\Pr_{\mathbf{y},\mathbf{z}}[(\text{Sc}^f(x, \mathbf{y}) \neq \text{Sc}^f(x, \mathbf{z}))] \leq 2(k-1)\epsilon(f)$. Hence, for every $x \in \mathbb{K}^n$, $\Pr_{\mathbf{y}}[g(x) \neq \text{Sc}^f(x, \mathbf{y})] \leq 2(k-1)\epsilon(f)$.*

PROOF. Let $\epsilon = \epsilon(f)$. We build two $k \times k$ matrices M, N with $M_{ij} \in \mathbb{K}^n$ and $N_{ij} \in \mathbb{F}$ and use properties of these matrices to prove the lemma.

For $i, j \in [m]$ pick $\gamma_{ij} \in \mathbb{K}^n$ as follows. Let $\gamma_{11} = x, \gamma_{1j} = y_j$, $\gamma_{i1} = z_i$, and γ_{ij} be chosen independently and uniformly at random from $\mathbb{K}^n$ otherwise. (Note every γ_{ij} except γ_{11} is thus drawn uniformly at random from $\mathbb{K}^n$.) Now for $i \in [k]$ and $j \in [m]$, let $M_{ij} = \ell_i(\gamma_{1j}, \ldots, \gamma_{mj})$. (In particular, we have $M_{ij} = \gamma_{ij}$ for $i, j \in [m]$.) Finally for $i \in [k]$ and $j \in [k]$, let $M_{ij} = \ell_j(M_{i1}, \ldots, M_{im})$. The second matrix N_{ij} is defined to be $f(M_{ij})$ except when $i = j = 1$, in which case we define $N_{11} = \text{Sc}^f(x, \mathbf{y})$.

Below we show that all the rows of N are codewords of V (with high probability), and that all the columns except possibly the first are also codewords of V. This allows us to conclude that the first column is also a codeword of V and this in turn yields the lemma.

We start by examining the properties of M and N. We claim that every row and every column of M corresponds to the queries of a potential test by our tester. We start with the rows. Fix $i \in [k]$ and note that the entries of the ith row correspond to queries of the test with randomness $M_{i1}, \ldots, M_{im}$ (corresponding to queries of the test "Does $f(M_{i1}) = \text{Sc}^f(M_{i1}; M_{i2}, \ldots, M_{im})$?"). Notice further that for $i \neq 1$ the values $M_{i1}, \ldots, M_{im}$ are drawn uniformly and independently at random from $\mathbb{K}^n$ (independent of x). To see this, suppose $c_{ij} \neq 0$ for some $j \in \{2, \ldots, m\}$. Then note that there is a one to one correspondence between $\langle \gamma_{j1}, \ldots, \gamma_{jm}\rangle$ and $\langle M_{i1}, \ldots, M_{im}\rangle$ for any fixed choice of $\{\gamma_{ik}\}_{i \neq j,k}$. Thus choos-

ing $\langle \gamma_{j1}, \ldots, \gamma_{jm} \rangle$ uniformly at random makes $\langle M_{i1}, \ldots, M_{im} \rangle$ uniform over $(\mathbb{K}^n)^m$ independent of $\gamma_{11} = x$. We conclude that the probability that $f(M_{i1}) \neq \mathrm{Sc}^f(M_{i1}; M_{i2}, \ldots, M_{im})$ is at most ϵ. In other words, the probability that the ith row of N is *not* a codeword of V is at most ϵ for $i \neq 1$.

Next we move to the columns of M and N. Note that the construction of M was asymmetric in that every row was defined to form a "query" pattern of our test. However, we note that the same matrix could have been defined by constructing the first m rows first, and then defining each column to be a "query pattern" of the test. To see this recall that $\ell_i(x_1, \ldots, x_m) = \sum_{j=1}^m c_{ij} x_j$. Thus we have

$$\begin{aligned} M_{ij} &= \ell_j(M_{i1}, \ldots, M_{im}) \\ &= \sum_{j'=1}^m c_{jj'} M_{ij'} \\ &= \sum_{j'=1}^m c_{jj'} \sum_{i'=1}^m c_{ii'} M_{i'j'} \\ &= \sum_{i'=1}^m c_{ii'} \sum_{j'=1}^m c_{jj'} M_{i'j'} \\ &= \sum_{i'=1}^m c_{ii'} M_{i'j} \\ &= \ell_i(M_{1j}, \ldots, M_{mj}). \end{aligned}$$

By a similar argument to the previous paragraph we now have that the probability that the jth column of N is not a codeword is at most ϵ for $j \neq 1$.

Thus, by the union bound, we have that with probability at most $2(k-1)\epsilon$ there exists a row (other than the first) or a column (other than the first) such that N restricted to the row or the column is not a codeword of V. We now use this to show that the first row of N and the first column of N are also codewords of V. Here we use the properties of tensor products of codes. Recall that the tensor product of V with itself, denoted $V \otimes V$ is the code consisting of all $k \times k$ matrices over $\mathbb{F}$ all of whose rows are codewords of V and all of whose columns are codewords of V. It is well known that if V has distance d then its tensor product with itself has the following "erasure-correcting" property: Given the projection of any matrix $B = A|_{S \times T}$ to a subset S of the rows and a subset T of the columns with $|S|, |T| \geq k - d + 1$, B can be extended to a (unique) codeword A of $V \otimes V$ if and only if for every row $s \in S$, the sth row of B is consistent with (the projection to T of) some codeword of V, and for every column $t \in T$, the tth column of B is consistent with (the projection to S of) some codeword of V.

In our case, the code V has distance at least 2 and we know the projection of N onto all columns except the first and all rows except the first are consistent with V. Thus the extension to N to a codeword of $V \otimes V$ is unique and this is the unique value which satisfies $N_{11} = \textsc{Decode}(N_{12}, \ldots, N_{1k}) = \textsc{Decode}(N_{21}, \ldots, N_{k1})$. We conclude that with probability at least $1 - 2(k-1)\epsilon$, we have $\Pr_{\mathbf{y},\mathbf{z}}[\mathrm{Sc}^f(x, \mathbf{y}) \neq \mathrm{Sc}^f(x, \mathbf{z})] \leq 2(k-1)\epsilon(f)$.

The consequence to g follows from the fact when drawing samples from a distribution, the probability of a collision is no more than the probability of the most likely element. ∎

We now revert to the task of proving that f is close to g and that g is a member of the family $\mathcal{F}$. We start with the former task which we show in exactly the same way as in [4, 19].

LEMMA 3.2. *$\delta(f, g) \leq 2\epsilon(f)$.*

PROOF. Let $B = \{x \in \mathbb{K}^n | \Pr_\alpha[f(x) \neq \mathrm{Sc}^f(x, \alpha)] \geq \frac{1}{2}\}$. Notice that $\epsilon(f) \geq \frac{1}{2} \Pr_x[x \in B]$. On the other hand, if $x \notin B$, then $f(x) = \mathrm{plurality}_\alpha[\mathrm{Sc}^f(x, \alpha)]$. The lemma follows. ∎

Next we show that the proof technique of Lemma 3.1 can be adapted to prove also that $g \in \mathcal{F}$. This modification is similar to those in the early papers [4, 19].

LEMMA 3.3. *Let f be a function with $\epsilon(f) < \frac{1}{(2k+1)(k-1)}$ and let g be its self-corrected version. Then $g \in \mathcal{F}$.*

PROOF. It suffices to show that for every $x_1, \ldots, x_m \in \mathbb{K}^n$ the vector $\langle g(y_1), \ldots, g(y_k) \rangle \in V$, where $y_i = \ell_i(x_1, \ldots, x_m)$. Fix such a sequence $x_1, \ldots, x_m \in \mathbb{K}^n$ and let $y_i = \ell_i(x_1, \ldots, x_m)$. for $i \in [k]$. As in the proof of Lemma 3.1, we will construct a matrix $M \in (\mathbb{K}^n)^{k \times k}$ whose first row will be $y_1, \ldots, y_k$. We will then define a related matrix N and show that all rows of N, except possibly the first, and all columns are codewords of V. We will then conclude that its first row must be a codeword of V and this will imply the lemma.

For $i, j \in [m]$, pick γ_{ij} as follows. $\gamma_{1j} = x_j$ and γ_{ij} is drawn uniformly and independently from $\mathbb{K}^n$ for all other i, j pairs. For $i' \in [k]$ and $j \in [m]$, define $M_{i'j} = \ell_{i'}(\gamma_{1j}, \ldots, \gamma_{mj})$. Finally, for $i', j' \in [k]$, define $M_{i'j'} = \ell_{j'}(M_{i'1}, \ldots, M_{i'm})$. Now let $N_{ij} = g(M_{ij})$ if $i = 1$ and $f(M_{ij})$ otherwise.

As in the proof of Lemma 3.1 we have that all the rows of M except the first represent the queries of a random test, and in particular the queried points are independent of $y_1, \ldots, y_k$. Thus we have that the probability that the i'th row of N is not a codeword of V is at most ϵ, for $i' \neq 1$.

Next we turn to the columns of N. Note that once again we have $M_{ij} = \ell_i(M_{1j}, \ldots, M_{mj})$. Now for every j, the jth column of M represents the queries of a random test through y_j. Thus we have that the probability that the jth column of N is not a codeword of V is given by the probability of the event $g(y_j) \neq \mathrm{Sc}^f(y_j; M_{2j}, \ldots, M_{mj})$ and by Lemma 3.1 the probability of this event is at most $2(k-1)\epsilon$.

Taking the union of all the "bad events" and deducting them, we have that with probability at least $1 - (2k+1)(k-1)\epsilon$ we have that all the rows of N except the first, and all the columns of N are codewords of V. We conclude (as in the proof of Lemma 3.1) that the first row of N, i.e., the vector $\langle g(y_1), \ldots, g(y_k) \rangle$ is a codeword of V. Since $1 - (2k+1)(k-1)\epsilon(f) > 0$, we have with positive probability $\langle g(y_1), \ldots, g(y_k) \rangle \in V$. But $y_1, \ldots, y_k$ were chosen deterministically and so the probability of this event is either zero or one, yielding that this event must happen with probability one. ∎

Finally, we can prove our main testing theorem, namely that locally (formally) characterized function families are locally testable.

PROOF OF THEOREM 2.9. >From Lemma 3.2, we have $\delta(f, g) \leq 2\epsilon(f)$. and by Lemma 3.3, we have $g \in \mathcal{F}$ and so $\delta(f) \leq 2\epsilon(f)$. ∎

4. STRUCTURE OF AFFINE-/LINEAR -INVARIANT FAMILIES

In this section we study structural properties of linear-invariant and affine-invariant families of functions mapping $\mathbb{F}^n$ to $\mathbb{F}$. (We extend this study to functions from $\mathbb{K}^n$ to $\mathbb{F}$ in the full version [17].) Before launching into the section we first introduce some notation and definitions that apply generally to functions mapping $\mathbb{K}^n \to \mathbb{F}$.

We use $\{\mathbb{K}^n \to \mathbb{F}\}$ to denote the set of all functions mapping $\mathbb{K}^n$ to $\mathbb{F}$. The central object of our attention is the minimal set of functions containing a specified family of functions that is affine/linear invariant.

DEFINITION 4.1. *For a set of functions $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$, $\text{SPAN}_{\mathbb{F}}(\mathcal{F}) = \{\sum_{i=1}^{\ell} \alpha_i \cdot f_i | \ell \in \mathbb{Z}^+, \alpha_i \in \mathbb{F}, f_i \in \mathcal{F}\}$ denotes the linear span (over $\mathbb{F}$) of $\mathcal{F}$. For a family of functions $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$ we let the linear span of $\mathcal{F}$, denoted $\text{L-SPAN}_{\mathbb{F}}(\mathcal{F})$, be the smallest linear-invariant family of functions containing $\mathcal{F}$. Finally, the affine span of $\mathcal{F}$, denoted $\text{A-SPAN}_{\mathbb{F}}(\mathcal{F})$ is the smallest affine-invariant family containing $\mathcal{F}$.*

When the range $\mathbb{F}$ is clear from the context we suppress the subscript and refer to $\text{SPAN}_{\mathbb{F}}(\mathcal{F})$ as simply $\text{SPAN}(\mathcal{F})$. Note that $\text{L-SPAN}(\mathcal{F})$ can be written as $\text{SPAN}(\{f(L(\mathbf{x}))|f \in \mathcal{F} \text{ and } L : \mathbb{K}^n \to \mathbb{K}^n \text{ is a linear function}\})$. Similarly, $\text{A-SPAN}(\mathcal{F})$ can be written as $\text{SPAN}(\{f(A(\mathbf{x}))|f \in \mathcal{F} \text{ and } A : \mathbb{K}^n \to \mathbb{K}^n \text{ is an affine function}\})$.

Extracting Monomials in Linear-Invariant Families For a polynomial $f = \sum_{\mathbf{d}} c_{\mathbf{d}} \mathbf{x}^{\mathbf{d}}$, we refer to the support of f to be the set of monomials $c_{\mathbf{d}}\mathbf{x}^{\mathbf{d}}$ with $c_d \neq 0$. For a monomial $m = \mathbf{x}^{\mathbf{d}}$, we denote the degree of the monomial by $deg(m) = \sum_{i=1}^{n} d_i$. Our first lemma asserts that in a linear-invariant family mapping $\mathbb{F}^n$ to $\mathbb{F}$, every monomial in the support of a function in the family also belongs to the family. The following lemma shows that linear-invariant families are generated linearly by the pure monomial functions contained in them.

LEMMA 4.2. *[Monomial extraction lemma] For every function $f : \mathbb{F}^n \to \mathbb{F}$, every monomial in the support of f is contained in $\text{L-SPAN}(f)$.*

The spread of monomials in linear-/affine-invariant families Next we present a general lemma that asserts that the presence of a single monomial in a family implies the presence of other monomials, with "smaller" degrees in a somewhat technical sense. We follow the lemma up with a corollary that describes some of the ways in which the lemma will be used later. To motivate the (somewhat technical) lemma, we first give an example. Consider the linear span of the monomial $x^5 \in \mathbb{F}[x, y]$. If the characteristic p of $\mathbb{F}$ is greater that 5 (or if $p = 3$), then $\text{L-SPAN}(x^5) = \text{SPAN}(\{x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5\})$. On the other hand, if $\mathbb{F}$ is of characteristic 5, the $\text{L-SPAN}(x^5) = \text{SPAN}(\{x^5, y^5\})$. If $\mathbb{F}$ is of characteristic 2, then $\text{L-SPAN}(x^5) = \text{SPAN}(\{x^5, x^4y, xy^4, y^5\})$. The lemma below attempts to capture some of this diversity.

LEMMA 4.3 (MONOMIAL SPREAD LEMMA). *Let $\mathbf{d} = \langle d_1, \ldots, d_n \rangle \in \{0, \ldots, q-1\}^n$ and $\mathbf{e} = \langle e_1, \ldots, e_n \rangle \in \{0, \ldots, q-1\}^n$. For $i \in [n]$ and $j \in \{0, \ldots, s-1\}$ let d_{ij} and e_{ij} be the unique integers from $\{0, \ldots, p-1\}$ such that $d_i = \sum_{j=0}^{s-1} d_{ij}p^j$ and $e_i = \sum_{j=0}^{s-1} e_{ij}p^j$. Let m be the monomial $\mathbf{x}^{\mathbf{d}}$ and let $m' = \mathbf{x}^{\mathbf{e}}$. If for every $j \in \{0, \ldots, s-1\}$ it is the case that $\sum_{i=1}^{n} e_{ij} \leq \sum_{i=1}^{n} d_{ij}$, then the following hold:*

1. *$m' \in \text{A-SPAN}(m)$.*
2. *$y^{f-\deg(m')+\deg(m)} \cdot m' \in \text{L-SPAN}(y^f \cdot m)$ for every non-negative f.*

The following corollary describes some of the many ways in which this lemma is used in the rest of this paper (and the full version [17]).

COROLLARY 4.4. *The following statements are true:*

1. *If $e_1, \ldots, e_n$ are non-negative integers such that $e_{n-1} + e_n < p$ then the monomial $x_1^{e_1} \cdots x_n^{e_n}$ is in the linear span of the monomial $x_1^{e_1} \cdots x_{n-2}^{e_{n-2}} \cdot x_{n-1}^{e_{n-1}+e_n}$.*
2. *If $q/p \leq d < q$ and f is an arbitrary integer then the monomial $x^{q/p}y^{f+d-q/p}$ is in the linear span of $x^d y^f$. and $x^{q/p}$ is in the affine span of x^d.*
3. *If $d_1 + \cdots + d_n \geq q/p$ and $f \geq 0$, then the monomial $y^{e+f}x_1^{q/p}$ is in the linear span of $y^f x_1^{d_1} \cdots x_n^{d_n}$ for $e = d_1 + \cdots d_n - q/p$, and $x_1^{q/p}$ is in the affine span of $x_1^{d_1} \cdots x_n^{d_n}$.*

Finally we present a lemma that gives a simple, but powerful consequence of the monomial extraction lemmas above.

LEMMA 4.5. *Let $m \in \mathbb{F}[\mathbf{x}, y]$ be a monomial of degree d. Let $\ell = \lfloor d/q \rfloor$. Then $\prod_{i=1}^{\ell} x_i^{q/p}$ is contained in $\text{A-SPAN}(m)$, Furthermore, $\{y^{d_1} \cdot m' | m' \in \text{A-SPAN}(\prod_{i=1}^{\ell} x_i^{q/p}), d_1 + \deg(m') \equiv d \mod (q-1)\}$ is contained in $\text{L-SPAN}(m)$.*

5. BOUNDING THE LOCALITY OF CHARACTERIZATIONS

In this section we outline the proof of Theorems 2.10 and 2.11 for the special case when $\mathbb{K} = \mathbb{F}$. In the process we present upper and lower bounds on the locality of formal characterizations of affine-invariant and linear-invariant families, in terms of the degree patterns of the monomials in their support.

Our (upper bounds on) characterizations are obtained by considering the values of a given function on some small dimensional subspace and verifying that these values agree with the values of some function in the family. Keeping this in mind, we define the restriction of a function family to a smaller dimension.

DEFINITION 5.1 (PROJECTIONS OF FUNCTION FAMILIES). *For positive integers ℓ and n, and for a linear-invariant family of functions $\mathcal{F} \subseteq \{\mathbb{K}^n \to \mathbb{F}\}$, the ℓ-dimensional restriction (extension) of $\mathcal{F}$, denoted $\mathcal{F}|_\ell$ is the family $\mathcal{F}|_\ell = \{f \circ L | f \in \mathcal{F}, L : \mathbb{K}^\ell \to \mathbb{K}^n \text{ linear }\}$.*

Note that we don't insist that $\ell \leq n$ and indeed the definition above makes sense also in this case. However in all our usage below, we think of $\ell \leq n$.

For affine-invariant families our characterizations depend simply on the maximum degree of functions in the family. For linear invariant functions this is no longer true. For instance, the family of functions supported on all monomials in $x_1, \ldots, x_n$ of degree 3 $\mod 4$ over $\mathbb{F}_5$ has a 2-local characterization even though it contains polynomials of degree $\Omega(n)$. For linear-invariant families, the characterizations depend on a more refined parameter that we define next.

DEFINITION 5.2. *For a linear invariant family $\mathcal{F}$ properly contained in $\{\mathbb{F}^n \to \mathbb{F}\}$, let $d_{\text{lin}}(\mathcal{F})$, the* linear-invariance degree *of $\mathcal{F}$, be the largest integer d such that $\mathcal{F}$ contains a monomial m_1 of degree d, while there also exists a monomial $m_2 \notin \mathcal{F}$ of degree d' for some $d' > 0$ with $d' \equiv d(\mod q-1)$.*

5.1 Upper/Lower bounds on locality of characterizations

The next lemma is the crux of our characterizations for linear-invariant as well as affine-invariant families.

LEMMA 5.3. . *Let $\mathcal{F} \subseteq \{\mathbb{F}^n \to \mathbb{F}\}$ be a linear-invariant family of linear-invariance degree $d_{\text{lin}}(\mathcal{F}) = d$. Suppose $f : \mathbb{F}^n \to \mathbb{F}$ is not in $\mathcal{F}$. Then, if $n \geq 1 + \left(\frac{2}{p} \cdot (d+q)\right)$, then there exists a linear function $L : \mathbb{F}^{n-1} \to \mathbb{F}^n$ such that $f \circ L \notin \mathcal{F}|_{n-1}$.*

We can now give a characterization for linear-invariant families.

LEMMA 5.4. *Let $\mathcal{F}$ be a linear invariant family, properly contained in $\{\mathbb{F}^n \to \mathbb{F}\}$, of linear-invariance degree $d_{\max}$. Then $\mathcal{F}$ has a q^ℓ-local formal characterization for $\ell = \frac{2(d+q)}{p}$.*

Immediately, we also get a characterization for affine-invariant families (since every affine invariant family with polynomials of degree at most $d_{\max}$ is also a linear-invariant family of linear-invariance degree at most $d_{\max}$).

LEMMA 5.5. *Let $\mathcal{F}$ be a proper subset of $\{\mathbb{F}^n \to \mathbb{F}\}$ and let $d_{\max}$ denote the maximum degree of any function in $\mathcal{F}$. Then $\mathcal{F}$ has a q^ℓ-local formal characterization for $\ell \leq \frac{2(d+q)}{p}$.*

We now describe lower bounds on the locality of constraints (and thus characterizations) in affine-invariant families. The lower bound is eventually derived from the study of Generalized Reed-Muller codes where it is known that the family of polynomials of degree d has no $q^{\lfloor d/q \rfloor}$-local characterizations [14, 8].

LEMMA 5.6. *Let $\mathcal{F}$ be an affine invariant family properly contained in $\{\mathbb{F}^n \to \mathbb{F}\}$ containing a polynomial of degree d. Then $\mathcal{F}$ has no q^ℓ-local constraints for $\ell \leq (d - q^2)/q^2$.*

In this section we provide lower bounds on the locality of characterizations of linear-invariant families, based on their "linear-invariance degree" (see Definition 5.2). As shown in Section 5.1, this parameter also yields upper bounds and thus together we find that this parameter governs (in some weak sense, since the bounds are far apart) the locality of characterizations for linear-invariant families.

LEMMA 5.7. *Let $\mathcal{F} \subsetneq \{\mathbb{F}^{n+1} \to \mathbb{F}\}$ be a family of linear invariance degree d. Then $\mathcal{F}$ has no characterizations of locality $q^{(d-q^2)/q^2}$.*

5.2 Testing Linear Invariant Families

The formal characterization described in Section 5.1 can immediately be turned into an affine invariant characterization for affine-invariant families. Coupled with Theorem 2.9 this leads immediately to a tester for affine-invariant families. However the characterization does not immediately lead to a tester for linear-invariant families, since these characterizations are not necessarily 2-ary independent. In this section we fix this gap.

We start with a definition that isolates a seemingly problematic subclass of linear-invariant families, where the characterizations are necessarily not 2-ary independent.

DEFINITION 5.8. *A linear invariant family $\mathcal{F} \subseteq \{\mathbb{F}^n \to \mathbb{F}\}$ is said to be* projective *if, for every pair of monomials $\mathbf{x}^{\mathbf{d}}$ and $\mathbf{x}^{\mathbf{e}}$ with $\sum_{i=1}^n d_i \equiv \sum_{i=1}^n e_i \mod (q-1)$, it is the case that $\mathbf{x}^{\mathbf{d}}$ is in the support of $\mathcal{F}$ if and only if $\mathbf{x}^{\mathbf{e}}$ is in the support of $\mathcal{F}$.*

Projective families have a very simple local formal characterization, which is unfortunately not 2-ary independent.

Even though projective families do not have a 2-ary independent linear characterization, they turn out to have a simple local test: Namely pick a random line $L : \mathbb{F} \to \mathbb{F}^n$ and verify $f \circ L$ has its support in S. We won't prove the correctness of this test right now (it will follow from the general case). Instead we turn to showing that every linear invariant family can be written as the sum of a nice family (with a 2-ary independent formal characterization) and a projective family and this ends up leading to a test.

LEMMA 5.9. *Let $\mathcal{F}$ be a linear-invariant family of linear invariance degree d. Then there exists a linear-invariant family $\mathcal{F}_1$ containing polynomials of degree at most d, and a projective family $\mathcal{F}_2$ such that $\mathcal{F} = \mathcal{F}_1 + \mathcal{F}_2$. Furthermore given an oracle to a function $f : \mathbb{F}^n \to \mathbb{F}$ one can construct an oracle for a function $g : \mathbb{F}^n \to \mathbb{F}$ where the oracle for g makes q oracle calls to f, such that $g \in \mathcal{F}_1$ if $f \in \mathcal{F}$ and $\delta(f, \mathcal{F}) \leq \delta(g, \mathcal{F}_1)$.*

Finally we use a simple proposition that can be used to give 2-ary independent localy characterizations for family $\mathcal{F}_1$ above.

PROPOSITION 5.10. *Let $\mathcal{F} \subseteq \mathcal{F}'$ have a k_1-local formal characterization. Furthermore suppose $\mathcal{F}'$ has a 2-ary independent k_2-local formal characterization. Then $\mathcal{F}$ has a $k_1 + k_2$-local 2-ary independent formal characterization.*

Putting all the ingredients together we get:

LEMMA 5.11. *Let $\mathcal{F} \subseteq \{\mathbb{F}^n \to \mathbb{F}\}$ be a linear-invariant family of linear-invariance degree d. Then it is $k' = 2q \cdot q^{2(d+q)/p}$-locally testable. Specifically, there is k'-query local test that accepts members of $\mathcal{F}$ with probability 1 and rejects functions that are δ-far from $\mathcal{F}$ with probability $\min\left\{\frac{\delta}{2}, \frac{q^2}{(2k'+q)(k'+q)}\right\}$.*

Combining the lemmas proved in this section (in particular, Lemmas 5.5, 5.7, 5.4, and 5.11) with Theorem 2.9 we get Theorems 2.10 and Theorems 2.11 for the special case when $\mathbb{K} = \mathbb{F}$.

6. CONCLUSIONS: THE ALON ET AL. CONJECTURE AND FUTURE WORK:

Our work attempts to highlight on the role of invariance in property testing. We remark that despite the obvious relationship of this notion to property testing, it has not been highlighted before. The only prior mentions seem to be in the works of Alon et al. [2], and in Goldreich and Sheffet [11].

Our work highlights linear-invariance as a central theme in algebraic property testing. Our results show that this notion yields a wide class of properties that have local property tests. These results are strong when the underlying field $\mathbb{K}$ is small. However when $\mathbb{K}$ is large, the characterization results (in particular, Theorem 2.10) becomes quite weak, even for affine-invariant families. In particular, in the case of the dual-BCH codes (which consider functions mapping $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$), our characterizations are completely trivial, while these codes do have very efficient tests [15]. One way to improve our results would be if Theorem 2.10 could be improved to have no dependence on t. This however is not possible, as shown in upcoming joint work with Grigorescu [12]. Specifically they exhibit a family of affine-invariant functions mapping $\mathbb{F}_{2^t}$ to $\mathbb{F}_2$ that have 8-local constraints, but no $o(t)$-local characterizations. Thus some dependence on $\mathbb{K}$ is necessary in translating constraints to characterizations.

Our work provides the first systematic study of testing functions from a field to its subfield. This setting is different than the well studied case of functions from a field to itself. This difference is best illustrated by the following example

- For affine invariant function family of the form $\mathbb{F}_2^n \to \mathbb{F}_2$ we have : a local constraint imply local characterization and local testability.

- For affine invariant function family of the form $\mathbb{F}_{2^n} \to \mathbb{F}_2$ we might have (by the work of [12]) a local constraint, but *no* local characterization! , and hence *no* local testing!

Moreover, our work suggests a method to construct new locally testable codes by picking the dual code to be a code spanned by an orbit of a short local constraint (orbit under the group of linear transformations).

In general, we feel that the class of linear-invariant functions offer a rich variety of properties, sufficiently wide to test out conjectures about the nature of testable properties. For instance, Alon et al. [2] had conjectured that linear codes of large distance, that have a small weight codeword in the dual, and have a "2-transitive invariant group" are locally testable. When applied to codes derived from affine-invariant function families, their conjecture implies that every affine-invariant family from $\mathbb{K}^n \to \mathbb{F}$ with a k-local constraint, must have an $f_{\mathbb{F}}(k)$-local test and in particular, an $f_{\mathbb{F}}(k)$-local characterization. The aforementioned result [12] refutes this conjecture of [2] by considering affine-invariant families. However, our work (Theorem 2.10) shows that a weak version of the [2] conjecture does hold, within the class of linear-invariant codes, by giving an $f_{\mathbb{K}}(k)$-local algebraic characterization and test.

This leaves the possibility that every locally characterized code with a "2-transitive invariant group" may be locally testable. Again we feel that this question can and should be examined in the context of affine-invariant families. In general, we feel that for every missing arrow, or qualitatively weak one, in Figure 1.3 poses an interesting open question that we hope will be investigated in future work.

This work put in focus object of the following form: $\mathbb{F}$-linear subspaces that are invariant under permutations of a group G. In this work the group G is the group of linear transformations of the domain. In a future work one may try to understand invariance under different groups in the following sense.

- Does k-local formal characterization imply local-testing also when the group of invariances is different than the group of linear transformations?

- Given a linear subspace that is invariant under permutations of a group G, when it is the case that k-local formal characterization exists (i.e. when there exists one short orbit that span the dual space)?

Acknowledgments

We would like to thank Oded Goldreich, Elena Grigorescu, Swastik Kopparty, Alex Samorodnitsky, and Avi Wigderson for many valuable discussions.

7. REFERENCES

[1] N. Alon, E. Fischer, I. Newman, and A. Shapira. A combinatorial characterization of the testable graph properties: It's all about regularity. *STOC 2006*, pages 251–260.

[2] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron. Testing low-degree polynomials over GF(2). *RANDOM 2003*, pages 188–199.

[3] E. Ben-Sasson, P. Harsha, and S. Raskhodnikova. Some 3CNF properties are hard to test. *STOC 2003* pages 345–354.

[4] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. *JCSS*, 47(3):549–595, 1993.

[5] A. Bogdanov, K. Obata, and L. Trevisan. A lower bound for testing 3-colorability in bounded-degree graphs. *FOCS 2002*, pages 93–102.

[6] C. Borgs, J. T. Chayes, L. Lovász, V. T. Sós, B. Szegedy, and K. Vesztergombi. Graph limits and parameter testing. *STOC 2006*, pages 261–270.

[7] S. D. Cohen. Functions and polynomials in vector spaces. *Archiv der Mathematik*, 48(5):409–419, May 1987.

[8] P. Delsarte, J.M. Goethals, and F.J. MacWilliams. On generalized Reed-Muller codes and their relatives. *Information and Control*, 16(5):403–442, 1970.

[9] A. M. Frieze and R. Kannan. Quick approximation to matrices and applications. *Combinatorica*, 19(2):175–220, 1999.

[10] O. Goldreich, S. Goldwasser, and D. Ron. Property testing and its connection to learning and approximation. *JACM*, 45(4):653–750, 1998.

[11] O. Goldreich and O. Sheffet. On the randomness complexity of property testing. *RANDOM 2007*, pages 509–524.

[12] E. Grigorescu, T. Kaufman, and M. Sudan. 2-transitivity is insufficient for local testability. *CCC 2008* page (to appear).

[13] C. S. Jutla, A. C. Patthak, A. Rudra, and D. Zuckerman. Testing low-degree polynomials over prime fields. *FOCS 2004*, pages 423–432.

[14] T. Kasami, S. Lin, and W. W. Peterson. New generalization of the Reed-Muller codes - Part I: Primitive codes. *IEEE Trans. Inf. Th.*, 14:189–199, 1968.

[15] T. Kaufman and S. Litsyn. Almost orthogonal linear codes are locally testable. *FOCS 2005*, pages 317–326.

[16] T. Kaufman and D. Ron. Testing polynomials over general fields. *FOCS 2004*, pages 413–422.

[17] T. Kaufman and M. Sudan. Algebraic property testing: the role of invariance. *ECCC Technical Report*, TR07-111, 2007.

[18] R. Rubinfeld. Robust functional equations and their applications to program testing. *SICOMP*, 28(6):1972–1997, 1999.

[19] R. Rubinfeld and M. Sudan. Robust characterizations of polynomials with applications to program testing. *SICOMP*, 25(2):252–271, April 1996.