A Unified Framework for Testing Linear-Invariant Properties

Arnab Bhattacharyya*, Elena Grigorescu†, Asaf Shapira‡
* *Computer Science and Artificial Intelligence Laboratory, MIT*
Email: abhatt@mit.edu
† *Computer Science and Artificial Intelligence Laboratory, MIT*
Email: elena_g@mit.edu
‡ *School of Mathematics and School of Computer Science, Georgia Institute of Technology*
Email: asafico@math.gatech.edu

***Abstract*—There has been a sequence of recent papers devoted to understanding the relation between the testability of properties of Boolean functions and the invariance of the properties with respect to transformations of the domain. Invariance with respect to $\mathbb{F}_2$-linear transformations is arguably the most common such symmetry for natural properties of Boolean functions on the hypercube. Hence, it is an important goal to find necessary and sufficient conditions for testability of linear-invariant properties. This is explicitly posed as an open problem in a recent survey of Sudan [1]. We obtain the following results:**

1) **We show that every linear-invariant property that can be characterized by forbidding induced solutions to a (possibly infinite) set of linear equations can be tested with one-sided error.**
2) **We show that every linear-invariant property that can be tested with one-sided error can be characterized by forbidding induced solutions to a (possibly infinite) set of *systems* of linear equations.**

We conjecture that our result from item (1) can be extended to cover systems of linear equations. We further show that the validity of this conjecture would have the following implications:

1) **It would imply that every linear-invariant property that is closed under restrictions to linear subspaces is testable with one-sided error. Such a result would unify several previous results on testing Boolean functions, such as the testability of low-degree polynomials and of Fourier dimensionality.**
2) **It would imply that a linear-invariant property $\mathcal{P}$ is testable with one-sided error if and only if $\mathcal{P}$ is closed under restrictions to linear subspaces, thus resolving Sudan's problem.**

AB: Supported in part by a DOE Computational Science Graduate Fellowship and NSF Awards 0514771, 0728645, and 0732334.
EG: Supported in part by NSF award CCR-0829672.
AS: Supported in part by NSF Grant DMS-0901355.

I. Introduction

Let $\mathcal{P}$ be a property of Boolean functions. A *testing* algorithm for $\mathcal{P}$ is a randomized algorithm that can quickly distinguish between the case that f satisfies $\mathcal{P}$ from the case that f is far from satisfying $\mathcal{P}$. The problem of characterizing the properties of Boolean functions for which such an efficient algorithm exists is considered by many to be the most important open problem in this area. Since a complete characterization seems to be out of reach, several researchers have recently considered the problem of characterizing the testable properties $\mathcal{P}$ that belong to certain "natural" subfamilies of properties. One such family that has been extensively studied is the family of so called *linear-invariant* properties. Our main result is two fold. We first show that every property in a large family of linear-invariant properties is indeed testable. Next, we conjecture that an even more general family of properties can be tested and show that such a result would give a *characterization* of the linear-invariant properties that are testable with one-sided error.

A. Background on property testing

We start with the formal definitions related to testing Boolean functions. Let $\mathcal{P}$ be a property of Boolean functions over the n-dimensional Boolean hypercube. In other words, $\mathcal{P}$ is simply a subset of the set of functions $f : \{0,1\}^n \to \{0,1\}$. Two functions $f, g : \{0,1\}^n \to \{0,1\}$ are ϵ-far if they differ on at least $\epsilon 2^n$ of the inputs. We say that f is ϵ-far from satisfying a property $\mathcal{P}$ if it ϵ-far from any function g satisfying $\mathcal{P}$. A *tester* for the property $\mathcal{P}$ is a randomized algorithm which can quickly distinguish between the case that an input function f satisfies $\mathcal{P}$ from the case that it is ϵ-far from satisfying $\mathcal{P}$. Here we assume that the input function f is given to the tester as an oracle, that is, the tester can ask an oracle for the value of the input functions f on a certain $x \in \{0,1\}^n$. We say that $\mathcal{P}$ is *easily testable* (or simply *testable*) if $\mathcal{P}$ has a tester which makes only a constant number of queries to the oracle, where this constant can

depend on ϵ but should be independent[1] of n. Finally, we say that a testing algorithm has *one-sided* error if it always accepts input functions satisfying $\mathcal{P}$. (We always demand that the tester rejects input functions which are ϵ-far from satisfying $\mathcal{P}$ with probability at least, say, 2/3.)

The study of testing of Boolean functions began with the work of Blum, Luby and Rubinfeld [2] on testing linearity of Boolean functions. This work was further extended by Rubinfeld and Sudan [3]. Around the same time, Babai, Fortnow and Lund [4] also studied similar problems as part of their work on MIP=NEXP. These works are all related to the PCP Theorem, and an important part of it involves tasks which are similar in nature to testing properties of Boolean functions. The work of Goldreich, Goldwasser and Ron [5] extended these results to more combinatorial settings, and initiated the study of similar problems in various areas. More recently, numerous testing questions in the Boolean functions settings have sparked great interest: testing dictators [6], low-degree polynomials [7], [8], juntas [9], [10], concise representations [11], halfspaces [12], codes [13], [14]. These are documented in several surveys [15], [16], [17], [1], and we refer the reader to these surveys for more background and references on property testing.

B. Invariance in testing Boolean functions

What features of a property make it testable? One area in which this question is relatively well understood is testing properties of dense graphs [18], [19]. In sharp contrast, this question is far from being well understood in the case of testing properties of Boolean functions. In an attempt to remedy this, Sudan and several coauthors [20], [21], [22], [23] have recently begun to investigate the role of invariance in property testing. The idea is that in order to be able to test if a combinatorial structure satisfies a property using very few queries to its representation, the property we are trying to test must be closed under certain transformations. For example, when testing properties of dense graphs, we are allowed to ask if two vertices i and j are adjacent in the graph, and the assumption is that the property we are testing is invariant under renaming of the vertices. In other words, if we think of the input as an $\binom{n}{2}$ dimensional 0/1 vector encoding the adjacency matrix of the input, then the property should be closed under transformations (of the edges) which result from permuting the vertices of the graph.

A natural notion of invariance that one can consider when studying Boolean functions over the hypercube is linear-invariance, which is in some sense the analogue for graph properties being closed under renaming of the vertices (we further discuss this analogy in Subsection I-C). Formally, a property of Boolean functions $\mathcal{P}$ is said to be linear-invariant if for every function $f : \mathbb{F}_2^n \to \{0,1\}$ satisfying $\mathcal{P}$ and for any linear transformation $L : \mathbb{F}_2^n \to \mathbb{F}_2^n$ the function $f \circ L$ satisfies $\mathcal{P}$ as well, where we define $(f \circ L)(x) = f(L(x))$. Note that here we identify $\{0,1\}^n$ with $\mathbb{F}_2^n$, and we will use this convention from now on throughout the paper. For a thorough discussion of the importance of linear-invariance, we refer the reader to Sudan's recent survey on the subject [1] and to the paper of Kaufman and Sudan which initiated this line of work [20].

C. The main result

Our main result in this paper (stated in Theorem 3 below) is that a natural family of linear-invariant properties of Boolean functions can all be tested with one-sided error. The statement requires some preparation.

Definition 1 ((M,σ)-free): Given an $m \times k$ matrix M over $\mathbb{F}_2$ and $\sigma \in \{0,1\}^k$, we say that a function $f : \mathbb{F}_2^n \to \{0,1\}$ is (M,σ)-*free* if there is no $x = (x_1, \ldots, x_k) \in (\mathbb{F}_2^n)^k$ such that $Mx = 0$ and for all $1 \le i \le k$ we have $f(x_i) = \sigma_i$.

Let us give some intuition about the above definition. Given a function $f : \mathbb{F}_2^n \to \{0,1\}$, it is natural to consider the set $S_f = \{x \in \mathbb{F}_2^n : f(x) = 1\}$. Suppose for the rest of this paragraph that in the above definition $\sigma = 1^k$. In this case f is (M,σ)-free if and only if S_f contains no solution to the system of equations $Mx = 0$, that is, if there is no $v \in S_f^k$ satisfying $Mv = 0$. Note that when considering graph properties, the notion of $(M,1^k)$-freeness is analogous to the graph property of being H-free[2], where H is some fixed graph. Observe that in both cases the property is *monotone* in the sense that if f is $(M,1^k)$-free, then removing elements from S_f results in a set that contains no solution to $Mx = 0$. Similarly if G is H-free, then removing edges from G results in an H-free graph.

Let us now go back to considering arbitrary $\sigma \in \{0,1\}^k$ in Definition 1, where again the intuition comes from graph properties. Observe that a natural variant of the monotone graph property of being H-free is the property of being induced H-free[3]. Note that being induced H-free is no longer a monotone property since if G is induced H-free then removing an edge can actually create induced copies of H. Getting back to the property

[1] Observe that since we aim for asymptotic results (that is, we think of $n \to \infty$), our property $\mathcal{P}$ can actually be described as $\mathcal{P} = \bigcup_{i=1}^{\infty} \mathcal{P}_n$, where $\mathcal{P}_n$ is the collection of functions over the n-dimensional Boolean hypercube which satisfy $\mathcal{P}$.

[2] If H is a graph on h vertices, then we say that a graph G is H-free if G contains no set of h vertices that contain a copy of H (possibly with some other edges).

[3] If H is a graph on h vertices, then we say that a graph G is induced H-free if G contains no set of h vertices that contain a copy of H and no other edges.

of being (M,σ)-free, observe that we can think of this as requiring S_f to contain no *induced* solution to the system of equations $Mx = 0$. That is, the requirement is that there should be no vector v satisfying $Mv = 0$, where $v_i \in S_f$ if $\sigma_i = 1$ and $v_i \in \mathbb{F}_2^n \setminus S_f$ if $\sigma_i = 0$. So we can think of σ as encoding which elements of a potential solution vector v should belong to S_f and which should belong to its complement. For this reason we will adopt the convention of calling (M,σ) a *forbidden induced system of equations*.

Continuing with the graph analogy, once we have the property of being induced H-free, for some fixed graph H, it is natural to consider the property of being induced $\mathcal{H}$-free where $\mathcal{H}$ is a fixed finite set of graphs. Several natural graph properties can be described as being induced $\mathcal{H}$-free (e.g. being a line-graph), but it is of course natural to further generalize this notion and allow $\mathcal{H}$ to contain an infinite number of forbidden induced graphs. One then gets a very rich family of properties like being Perfect, k-colorable, Interval, Chordal etc. This generalization naturally motivates the following definition which will be key to our main results.

Definition 2 ($\mathcal{F}$-free): Let $\mathcal{F} = \{(M^1,\sigma^1),(M^2,\sigma^2),\dots\}$ be a (possibly infinite) set of induced systems of linear equations. A function f is said to be $\mathcal{F}$-free if it is (M^i,σ^i)-free[4] for all i.

Observe that this definition is an OR-AND type restriction, that is, we require that f will not satisfy *any* of the systems (M^i,σ^i), where f satisfies (M^i,σ^i) if it satisfies all the equations of M^i (in the sense of Definition 1). We are now ready to state our main result.

Theorem 3 (Main Result): Let $\mathcal{F} = \{(M^1,\sigma^1),(M^2,\sigma^2),\dots\}$ be a (possibly infinite) set of induced equations (that is, all the matrices M^i are of rank one). Then the property of being $\mathcal{F}$-free is testable with one-sided error.

We stress that in the above theorem each M^i contains a single equation (rather than a *system* of equations as in Definition 2).

Let us compare this result to some previous works. One work that initiated some of the recent results on testing Boolean functions was obtained by Green [24]. His result can be formulated as saying that for any rank one matrix M, the property of being $(M,1^k)$-free can be tested with one-sided error. Green conjectured that the same result holds for any *system* of linear equations. This conjecture was recently confirmed by Shapira [25] and Král', Serra and Vena [26]. In our language, the results of [25], [26] can be stated as saying that for any matrix M, the property of being $(M,1^k)$-free is testable with one-sided error. The case of arbitrary σ was first explicitly considered in [27] where it was shown that if M is a rank one matrix, then (M,σ)-freeness is equivalent to a finite set of properties, all of which were already known to be testable. Austin (see [25]) conjectured that the result of [25] for an arbitrary matrix M can be extended to show testability of (M,σ)-freeness for every vector σ. Shapira [25] further conjectured that his result can be extended to the case when we forbid an infinite set of systems of linear equations as in Definition 2. So Theorem 3 partially resolves the above conjecture, since it can handle an infinite number of induced equations (but not an infinite number of forbidden *systems* of equations).

Another way to think of Theorem 3 comes (yet again) from the analogy with graph properties. Alon and Shapira [18] have shown that for every set of graphs $\mathcal{F}$, the property of being induced $\mathcal{F}$-free is testable with one-sided error. Since in many ways[5], copies of a fixed graph H in a graph G correspond to finding solutions of a *single* equation in a set $S \subseteq \mathbb{F}_2^n$, Theorem 3 can be considered to be a Boolean functions analog of the result of [18]. Just like the property of being H-free is similar to being (M,σ)-free where M has rank 1, the *hypergraph* property of being H-free is analogous to being (M,σ)-free for an arbitrary M. Now, the result of [18] has been later extended to hypergraphs by Austin and Tao [28] and Rödl and Schacht [29], so it is natural to expect that one could also handle an infinite number of forbidden induced systems of equations in the functional case as well. All the above motivates us to raise the following conjecture.

Conjecture 4: For every (possibly infinite) set of systems of induced equations $\mathcal{F}$, the property of being $\mathcal{F}$-free is testable with one-sided error.

As the reader can easily convince himself, a graph property $\mathcal{P}$ is equivalent to being induced $\mathcal{H}$-free if and only if $\mathcal{P}$ is closed under vertex removal. Such properties are usually called *hereditary*. This motivates us to define the following analogous notion for properties of Boolean functions.

Definition 5 (Subspace-Hereditary Properties): A linear-invariant property $\mathcal{P}$ is said to be *subspace-hereditary* if it is closed under restriction to subspaces. That is, if f is in $\mathcal{P}_n$ and H is a m-dimensional linear subspace of $\mathbb{F}_2^n$, then $f|_H \in \mathcal{P}_m$ also, where[6] $f|_H : \mathbb{F}_2^m \to \{0,1\}$ is the restriction of f to H.

When considering linear-invariant properties, one can also obtain the following (slightly cleaner) view of the properties of Definition 2. This equivalence is analogous to the graph properties mentioned above. We stress

[4] In the sense of Definition 1

[5] This analogy is somewhat hard to formally state, at least in this extended abstract

[6] Note that we are implicitly composing $f|_H$ with a linear transformation so that it is now defined on $\mathbb{F}_2^m$. Here, we are using the fact that $\mathcal{F}$ is linear-invariant.

that this equivalence is a further indication of the "naturalness" of the notion of linear-invariance and its resemblance to the closure of graph properties under vertex renaming.

Proposition 6: A linear-invariant property $\mathcal{P}$ is subspace-hereditary if and only if there is a (possibly infinite) set of systems of induced equations $\mathcal{F}$ such that $\mathcal{P}$ is equivalent to being $\mathcal{F}$-free.

We mention that while the notions of graph properties being hereditary and functions being subspace-hereditary are somewhat more natural than the equivalent notions of being free of induced subgraphs and equations respectively, it is actually easier to think about these properties using the latter notion when proving theorems about them. This was the case in [18], and it will be the case in the present paper as well. Proposition 6 along with Conjecture 4 implies the following:

Corollary 7: If Conjecture 4 holds, then every linear-invariant subspace-hereditary property is testable with one-sided tester.

Observe that if Conjecture 4 holds, then Corollary 7 would give yet another surprising similarity between linear-invariant properties of boolean functions and graph properties, since it is known [18] that every hereditary graph property is testable. Actually, as we discuss in the next subsection, if Conjecture 4 holds, then an even stronger similarity would follow.

Many interesting properties of the hypercube that have been studied for testability are linear-invariant. Important examples include linearity [2], being a polynomial of low degree [7], and low Fourier dimensionality and sparsity [30]. These properties have all been shown to be testable. Moreover, they all turn out to be subspace-hereditary. Thus, if our Conjecture 4 is true, as we strongly believe, then we could explain the testability of all these properties through a unified perspective. Note that our main result already shows (yet again!) that linearity is testable but from a completely different viewpoint than used in previous analysis. Furthermore, to show the testability of low degree polynomials (a.k.a., Reed-Muller codes), we would only need to resolve Conjecture 4 for a *finite* [7] family of forbidden induced systems of equations. Regarding the properties of Fourier dimensionality and sparsity, they are currently only known to have two-sided testers, while Corollary 7 will potentially yield one-sided testers, resolving an issue raised in [1].

D. The proposed characterization of testable linear-invariant properties

We now turn to discuss our second result, which based on Conjecture 4 gives a characterization of the linear-invariant properties of Boolean functions that can be tested with one-sided error using "natural" algorithms. Let us start with formally defining the types of "natural" testing algorithms we consider here.

Definition 8 (Oblivious Tester): An *oblivious tester* for a property $\mathcal{P} = \{\mathcal{P}_n\}_n$ is a (possibly 2-sided error) non-adaptive, probabilistic algorithm, which, given a distance parameter ϵ, and oracle access to an input function $f : \mathbb{F}_2^n \to \{0,1\}$, performs the following steps:

1) Computes an integer $d = d(\epsilon)$. If $d(\epsilon) > n$, let $H = \mathbb{F}_2^n$. Otherwise, let $H \leq \mathbb{F}_2^n$ be a subspace of dimension $d(\epsilon)$ chosen uniformly at random.
2) Queries f on all elements $x \in H$.
3) Accepts or rejects based only on the outcomes of the received answers, the value of ϵ, and its internal randomness.

We now discuss the motivation for considering the above type of algorithms. The fact that the tester is non-adaptive and queries a random linear subspace is without loss of generality (details in the full version); this is analogous to the fact [31], [32] that one can assume a graph property tester makes its decision only by inspecting a randomly chosen induced subgraph. The only essential restriction we place on oblivious testers is that their behavior cannot depend on the value of n, the domain size of the input function. If we allow the testing algorithm to make its decisions based on n, then it can do very strange and unnatural things. For example, we can now consider properties that depend on the parity of n. As was shown in [33], the algorithm can use the size of the input in order to compute the optimal query complexity. All these abnormalities will not allow us to give any meaningful characterization. As observed in [18] by restricting the algorithm to make its decisions while not considering the size of the input we can still test any (natural) property while at the same time avoid annoying technicalities. We finally note that all the testing algorithms for testable properties of Boolean functions in prior works were indeed oblivious, and that furthermore many of them implicitly consider only oblivious testers. In particular, these types of testers were considered in [1].

As it turns out, oblivious testers can potentially[8] test properties which are slightly more general than subspace-hereditary properties. These are defined as follows.

Definition 9 (Semi Subspace-Hereditary Property): A property $\mathcal{P} = \{\mathcal{P}_n\}_n$ is *semi subspace-hereditary* if there exists a subspace-hereditary property $\mathcal{H}$ such that

1) Any function f satisfying $\mathcal{P}$ also satisfies $\mathcal{H}$.
2) There exists a function $M : (0,1) \to \mathbb{N}$ such that if $f : \mathbb{F}_2^n \to \{0,1\}$ is ϵ-far from satisfying $\mathcal{P}$ and

[7] The characterization of polynomials of degree d using forbidden induced equations is described in the full version.

[8] The potential relies on the validity of Conjecture 4.

$n \geq M(\epsilon)$, then there exists a subspace $V \subseteq \mathbb{F}_2^n$ such that $f|_V$ does not satisfy $\mathcal{H}$.

The intuition behind the above definition is that a semi subspace-hereditary property can only deviate from being "truly" subspace-hereditary on functions over a finite domain, where the finiteness is controlled by the function M in the definition. Our next theorem connects the notion of oblivious testing and semi subspace-hereditary properties. Assuming Conjecture 4, it essentially characterizes the linear-invariant properties that are testable with one-sided error, thus resolving Sudan's problem raised in [1].

Theorem 10: If Conjecture 4 holds, then a linear-invariant property $\mathcal{P}$ is testable by a one-sided error oblivious tester **if and only if** $\mathcal{P}$ is semi subspace-hereditary.

Getting back to the similarity to graph properties, we note that [18] obtained a similar characterization for the graph properties that are testable with one-sided error. Let us close by mentioning two points. The first is that most linear-invariant properties are known to be testable with one-sided error, and hence the question of characterizing these properties is well motivated. In fact, for the subclass of linear-invariant properties which also themselves form a linear subspace, [34] showed that the optimal tester is always one-sided and non-adaptive. Our second point is that it is natural to ask if there are linear-invariant properties which are not efficiently testable. A linear-invariant property with query complexity $\Omega(2^n)$ arises implicitly from the arguments of [5]; see Section IV for a brief sketch. A second, more natural, example comes from Reed-Muller codes. [35] shows that for any $1 \ll q(n) \ll n$ the linear-invariant property of being a $\log_2(q(n))$-Reed-Muller code cannot be tested with $o(q(n))$ queries. We also conjecture that the property of two functions being isomorphic upto linear transformations of the variables is not a testable property. Lower bounds for isomorphism testing have been studied both in the Boolean function model [9], [36] and in the dense graph model [37], but our problem specifically does not seem to have been examined in a property testing setting.

E. Paper overview

The rest of the paper is organized as follows. In Section II we discuss the regularity lemma of Green [24]. Just as the graph regularity lemma of Szemerédi [38] guarantees that every graph can be partitioned into a bounded number of pseudorandom graphs, Green's regularity lemma guarantees a similar partition for Boolean functions. This lemma, whose proof relies on Fourier analysis over $\mathbb{F}_2^n$, was used in [24] to show that properties defined by forbidding a single (non-induced) equation are testable. This basic approach falls short of being able to handle an infinite number of forbidden non-induced equations or even a single forbidden induced equation. We thus need to develop a variant of Green's regularity lemma that is strong enough to allow such applications. This new variant is described in Section II. The overall approach is motivated by that taken by Alon et al. [19] in their formulation of the functional graph regularity lemma. However, the proof here is somewhat more involved since we need to develop several tools in order to make the approach work. One of them is a certain Ramsey type result for $\mathbb{F}_2^n$ which is key to our proof and that may be useful in other settings (see Theorem 16). The approach of [19] only allows one to handle a *finite* number of forbidden subgraphs, which translates in our setting to being able to handle a finite number of forbidden equations. So, one last technique we employ is motivated by the ideas from [18] on how to handle an infinite number of forbidden subgraphs. This (somewhat complicated) technique is described in Section III. We believe that these set of ideas will prove to be instrumental in resolving Conjecture 4. Section IV is devoted to some concluding remarks and open problems.

Due to space limitations, many of the proofs are omitted from this extended abstract. The reader may consult the full version of this paper for more details.

II. Pseudorandom Partitions of the Hypercube

The *support* of a Boolean function f refers to the subset of the domain on which f evaluates to 1. If H is a subspace of $\mathbb{F}_2^n$ and given function $f : H \to \{0,1\}$, let $\rho(f)$, the *density* of f, denote $\frac{\sum_{x \in H} f(x)}{|H|}$. Recall that the Fourier coefficients of f, defined for each $\alpha \in H^*$, are:

$$\widehat{f}(\alpha) = \mathop{\mathbb{E}}_{x \in H}\left[f(x) \cdot (-1)^{\langle x, \alpha \rangle}\right]$$

For a parameter $\epsilon \in (0,1)$, we say f is *ϵ-uniform* if $\max_{\alpha \neq 0} |\widehat{f}(\alpha)| < \epsilon$. This definition captures the notion of correlation with a linear function on H, and it will serve as our definition of pseudorandomness.

Given a function $f : \mathbb{F}_2^n \to \{0,1\}$, a subspace $H \leq \mathbb{F}_2^n$ and an element $g \in \mathbb{F}_2^n$, define the function $f_H^{+g} : H \to \{0,1\}$ to be $f_H^{+g}(x) = f(x+g)$ for $x \in H$. The support of f_H^{+g} represents the intersection of the support of f with the coset $g + H$. The following lemma shows that if a uniform function is restricted to a coset of a subspace of low codimension, then the restriction does not become too non-uniform and its density stays roughly the same.

Lemma 11: Let $f : \mathbb{F}_2^n \to \{0,1\}$ be an ϵ-uniform function of density ρ, and let $H \leq \mathbb{F}_2^n$ be a subspace of codimension k. Then for any $c \in \mathbb{F}_2^n$, the function $f_H^{+c} : H \to \{0,1\}$ is $(2^k\epsilon)$-uniform and of density ρ_c satisfying $|\rho_c - \rho| < 2^k\epsilon$.

For a subspace $H \leq \mathbb{F}_2^n$, the *H-based partition* refers to the partitioning of $\mathbb{F}_2^n$ into the cosets in $\mathbb{F}_2^n/H$. If $H' \leq H$, then the H'-based partition is called a *refinement* of the H-based partition. The *order* of the H-based partition is defined to be $[G : H]$, i.e., the index of H as a subgroup or the dimension of the quotient space $\mathbb{F}_2^n/H$. Using this notation, Green's regularity lemma can be stated as follows.

Lemma 12 (Green's Regularity Lemma [24]): For every m and $\epsilon > 0$, there exists $T = T_{12}(m, \epsilon)$ such that the following is true. Given function $f : \mathbb{F}_2^n \to \{0, 1\}$ with $n > T$ and H-based partition of $\mathbb{F}_2^n$ with order at most m, there exists a refined H'-based partition of order k, with $m \leq k \leq T$, for which $f_{H'}^{+g}$ is not ϵ-uniform for at most $\epsilon 2^n$ many $g \in \mathbb{F}_2^n$.

Our main tool in this work is a functional variant of Green's regularity lemma, in which the uniformity parameter ϵ is not a constant but rather an arbitrary function of the order of the partition. It is quite analogous to a similar lemma, first proved in [31], in the graph property testing setting. The recent work [39] shows a (very strong) functional regularity lemma in the arithmetic setting but it applies over the integers and not $\mathbb{F}_2$.

Lemma 13 (Functional regularity lemma): For integer m and function $\mathcal{E} : \mathbb{Z}^+ \to (0, 1)$, there exists $T = T_{13}(m, \mathcal{E})$ such that the following is true. Given function $f : \mathbb{F}_2^n \to \{0, 1\}$ with $n \geq T$, there exist subspaces $H' \leq H \leq \mathbb{F}_2^n$ that satisfy:

- Order of H-based partition is $k \geq m$, and order of H'-based partition is $\ell \leq T$.
- There are at most $\mathcal{E}(0) \cdot 2^n$ many $g \in \mathbb{F}_2^n$ such that f_H^{+g} is not $\mathcal{E}(0)$-uniform.
- For every $g \in \mathbb{F}_2^n$, there are at most $\mathcal{E}(k) \cdot 2^{n-k}$ many $h \in H$ such that $f_{H'}^{+g+h}$ is not $\mathcal{E}(k)$-uniform.
- There are at most $\mathcal{E}(0) \cdot 2^n$ many $g \in \mathbb{F}_2^n$ for which there are more than $\mathcal{E}(0) \cdot 2^{n-k}$ many $h \in H$ such that $|\rho(f_H^{+g}) - \rho(f_{H'}^{+g+h})| > \mathcal{E}(0)$.

We use Lemma 13 in two main ways. For one of them, we use the lemma directly. For the other, we use the following simple but extremely useful corollary which allows us to say that there are many cosets in a partitioning which, on the one hand, are *all* uniform, and on the other hand, are arranged in an algebraically nice structure.

Corollary 14: For every m and $\mathcal{E} : \mathbb{Z}^+ \to (0, 1)$, there exist $T = T_{14}(m, \mathcal{E})$ and $\delta = \delta_{14}(m, \mathcal{E})$ such that the following is true. Given function $f : \mathbb{F}_2^n \to \{0, 1\}$ with $n \geq T$, there exist subspaces $H' \leq H \leq \mathbb{F}_2^n$ and an injective linear map $I : \mathbb{F}_2^n/H \to \mathbb{F}_2^n/H'$ such that:

- The H-based partition is of order k, where $m \leq k \leq T$. Additionally, $|H'| \geq \delta 2^n$.
- For each $u \in \mathbb{F}_2^n/H$, $I(u) + H'$ lies inside the coset $u + H$. Note that $I(0) = 0$ since I is linear.
- For every nonzero $u \in \mathbb{F}_2^n/H$, the set $f_{H'}^{+I(u)}$ is $\mathcal{E}(k)$-uniform.
- There are at most $\mathcal{E}(0)2^n$ many $g \in \mathbb{F}_2^n$ for which $|\rho(f_H^{+g}) - \rho(f_{H'}^{+I(u)})| > \mathcal{E}(0)$ where $u = g \pmod H$.

The next lemma is in a similar spirit to Corollary 14. It also obtains a set of uniform cosets which are structured algebraically, but in this case, all of them are contained inside the same subspace. We need a different set of tools to prove this lemma. Specifically, we use linear algebraic variants of the classic theorems of Turán and Ramsey. We note that the (classic) Turán and Ramsey Theorems are key tools in many applications of the graph regularity lemma, for example in the well known bound on the Ramsey numbers of bounded degree graphs [40]. Hence, the following variants of these classic results may be useful in other applications of Greens's regularity lemma.

Proposition 15 (Turán theorem for subspaces): For positive integers n, if S is a subset of $\mathbb{F}_2^n$ with density greater than $1 - \frac{1}{2^{d-1}}$, then there exists a subspace $H \leq \mathbb{F}_2^n$ of dimension d such that $H - \{0\}$ is contained in S. Moreover, there is a subset of $\mathbb{F}_2^n$ with density $\left(1 - \frac{1}{2^{d-1}}\right)$ which does not contain $H - \{0\}$ for any subspace $H \leq \mathbb{F}_2^n$.

Theorem 16 (Ramsey theorem for subspaces): For every positive integer d, there exists $N = N_{16}(d)$ such that for any subset $S \subseteq \mathbb{F}_2^N$, there exists a subspace $H \leq \mathbb{F}_2^N$ of dimension d such that $H - \{0\}$ is contained either in S or in $\bar{S}$.

Given these results, the lemma below follows fairly readily.

Lemma 17: For every positive integer d and $\gamma \in (0, 1)$, there exists $\delta = \delta_{17}(d, \gamma)$ such that the following is true. Given $f : \mathbb{F}_2^n \to \{0, 1\}$, there exists a subspace $H \leq \mathbb{F}_2^n$ and a subspace K of dimension d in the quotient space $\mathbb{F}_2^n/H$ with the following properties:

- $|H| \geq \delta 2^n$.
- For every nonzero $u \in K$, f_H^{+u} is γ-uniform.
- Either $\rho(f_H^{+u}) \geq \frac{1}{2}$ for every nonzero $u \in K$ or $\rho(f_H^{+u}) < \frac{1}{2}$ for every nonzero $u \in K$.

III. Forbidding Infinitely Many Induced Equations

To begin, let us fix some notation. Given a matrix M over $\mathbb{F}_2$ of size m-by-k, a string $\sigma \in \{0, 1\}^k$, and a function $f : \mathbb{F}_2^n \to \{0, 1\}$, if there exists $x = (x_1, \ldots, x_k) \in (\mathbb{F}_2^n)^k$ such that $Mx = 0$ and $f(x_i) = \sigma_i$ for all $i \in [k]$, we say that f *induces* (M, σ) *at* x and denote this by $(M, \sigma) \mapsto f$.

In this section, we prove our main result (Theorem 3) that properties characterized by infinitely many forbidden induced equations are testable. The following theorem is the key to the argument.

Theorem 18: For every infinite family of equations $\mathcal{F} = \{(E^1, \sigma^1), (E^2, \sigma^2), \ldots, (E^i, \sigma^i), \ldots\}$ with each E^i being a row vector $[1\ 1\ \cdots\ 1]$ of size k_i and $\sigma^i \in \{0,1\}^{k_i}$ a k_i-tuple, there are functions $N_{\mathcal{F}}(\cdot)$, $k_{\mathcal{F}}(\cdot)$ and $\delta_{\mathcal{F}}(\cdot)$ such that the following is true for any $\epsilon \in (0,1)$. If a function $f : \mathbb{F}_2^n \to \{0,1\}$ with $n > N_{\mathcal{F}}(\epsilon)$ is ϵ-far from being $\mathcal{F}$-free, then f induces $\delta \cdot 2^{n(k_i-1)}$ many copies of some (E^i, σ^i), where $k_i \leq k_{\mathcal{F}}(\epsilon)$ and $\delta \geq \delta_{\mathcal{F}}(\epsilon)$.

Theorem 3 follows, because the above Theorem 18 allows us to devise the following tester T for $\mathcal{F}$-freeness. T, given input $f : \mathbb{F}_2^n \to \{0,1\}$, first checks if $n \leq N_{\mathcal{F}}(\epsilon)$, and in this case, it queries f on the entire domain and decides accordingly. Otherwise, T repeats the following test $O(1/\delta_{\mathcal{F}}(\epsilon))$ many times: for every i such that $k_i \leq k_{\mathcal{F}}(\epsilon)$, independently and uniformly at random choose elements $x_1, \ldots, x_{k_i-1} \in \mathbb{F}_2^n$, set $x_{k_i} = x_1 + x_2 + \cdots x_{k_i-1}$ and reject immediately if $f(x_j) = \sigma^i_j$ for every $j \in [k_i]$. T accepts if it never rejects in any of the iterations. It's clear that the query complexity of T is constant and that T always accepts if the input is $\mathcal{F}$-free. It rejects inputs ϵ-far from $\mathcal{F}$-free because Theorem 18 guarantees that there will be an equation of size at most $k_{\mathcal{F}}(\epsilon)$ for which T will detect solutions to, with constant probability.

To start the proof (sketch) of Theorem 18, let us relate pseudorandomness (uniformity) of a function to the number of solutions to a single equation induced by it. Similar and more general statements have been shown previously, but we need only the following claim for what follows.

Lemma 19 (Counting Lemma): For every $\eta \in (0,1)$ and integer $k > 2$, there exist $\gamma = \gamma_{19}(\eta, k)$ and $\delta = \delta_{19}(\eta, k)$ such that the following is true. Suppose E is the row vector $[1\ 1 \cdots 1]$ of size k, $\sigma \in \{0,1\}^k$ is a tuple, H is a subspace of $\mathbb{F}_2^n$, and $f : \mathbb{F}_2^n \to \{0,1\}$ is a function. Furthermore, suppose there are k not necessarily distinct elements $u_1, \ldots, u_k \in \mathbb{F}_2^n/H$ such that $Mu = 0$ where $u = (u_1, \ldots, u_k)$, $f_H^{+u_i} : H \to \{0,1\}$ is γ-uniform for all $i \in [k]$, and $\rho(f_H^{+u_i})$ is at least η if $\sigma(i) = 1$ and at most $1 - \eta$ if $\sigma(i) = 0$ for all $i \in [k]$. Then, there are at least $\delta |H|^{k-1}$ many k-tuples $x = (x_1, x_2, \ldots, x_k)$, with each $x_i \in u_i + H$, such that f induces (E, σ) at x.

In light of this lemma, our strategy to prove Theorem 18 will be to partition the domain into uniform cosets, using Green's regularity lemma (Lemma 12) in some fashion, and then to use the above counting lemma to count the number of induced solutions to some equation in $\mathcal{F}$. But one issue that immediately arises is that, because $\mathcal{F}$ is an infinite family of equations, we do not know the size of the equation we would want the input function to induce. Since Lemma 19 needs different uniformity parameters to count equations of different lengths, it is not *a priori* clear how to set the uniformity parameter in applying the regularity lemma. (If $\mathcal{F}$ was finite, one could set the uniformity parameter to correspond to the size of the largest equation in $\mathcal{F}$.)

To handle the infinite case, our basic approach will be to classify the input function into one of a finite set of classes. For each such class c, there will be an associated number k_c such that it is guaranteed that any function classified as c must induce an equation in $\mathcal{F}$ of size at most k_c. If there is such a classification scheme, then we know that *any* input function must induce an equation of size at most $\max_c k_c$. How do we perform this classification? We use the regularity lemma. Consider the following idealized situation. Fix an integer r. Suppose we could modify the input $f : \mathbb{F}_2^n \to \{0,1\}$ at a small fraction of the domain to get a function $F : \mathbb{F}_2^n \to \{0,1\}$ and then could apply Lemma 12 to get a partition of order r so that the restrictions of F to each coset was exactly 0-uniform. F is then a constant function (either 0 or 1) on each of the 2^r cosets, and so, we can classify F by a Boolean function $\mu : \mathbb{F}_2^r \to \{0,1\}$ where $\mu(x)$ is the value of F on the coset corresponding to x. Notice that there are only finitely many such μ's. Since F differs from f at only a small fraction of the domain and since f is far from $\mathcal{F}$-free, F must also induce some equation in $\mathcal{F}$. Then, for every such μ and corresponding F, there is a smallest equation in $\mathcal{F}$ that is induced by F. We can let $\Psi_{\mathcal{F}}(r)$ be the maximum over all such μ of the size of the smallest equation in $\mathcal{F}$ that is induced by the F corresponding to μ. We then might hope that this function $\Psi_{\mathcal{F}}(\cdot)$ can be used to tune the uniformity parameter by using the functional variant of the regularity lemma (Lemma 13).

There are a couple of caveats. First, we will not be able to get the restrictions to every coset to look perfectly uniform. Second, if F induces solutions to an equation, it does not necessarily follow that f also does. To get around the first problem, we use the fact that Lemma 19 is not very restrictive on the density conditions. We think of the uniform cosets which have density neither too close to 0 nor 1 as "wildcard" cosets at which both the restriction of f and its complement behave pseudorandomly and have non-negligible density. Thus, the μ in the above paragraph will map into $\{0, 1, *\}^r$, where a '$*$' denotes a wildcard coset. For the second problem, note that it is not really a problem if $\mathcal{F}$-freeness is known to be monotone. In this case, F inducing an equation automatically means f also induces an equation, if we obtained F by removing elements from the support of f. For induced freeness properties, though, this is not the case. Using ideas from [31] and the tools from Section II, we structure the modifications from f to F in such a way so as to force f to induce solutions of an equation if F induces a solution to the same equation. The reader is encouraged to look at the full version for details.

IV. Concluding Remarks and Open Problems

Obviously, the main open problem we would like to see resolved is Conjecture 4. One appealing way to prove the conjecture would be to proceed as we have but to obtain a stronger notion of pseudorandomness in the regularity lemma. The notion of ϵ-uniformity obtained from Green's regularity lemma corresponds to the Gowers U^2 norm, whereas in order to be able to prove Conjecture 4 in its full generality, we would presumably need a similar regularity lemma with respect to the Gowers U^k norm [41] for any fixed k. Such a higher order regularity lemma has been very recently obtained by Green and Tao [39] over the integers. However, it is not yet available over $\mathbb{F}_2$, as the inverse conjectures for the Gowers norms over $\mathbb{F}_2$ have not yet been completely clarified [42].

Let us mention some other observations and open problems related to this work.

- As we have mentioned in Subsection I-D, it is not too hard to construct linear-invariant properties which are not testable. Actually, there are properties of this type that cannot be tested with $o(2^n)$ queries[9]. One example can be obtained from a variant of an argument used in [5] as follows; it is shown in [5] (see Proposition 4.1) that for every n there exists a property of Boolean functions that contains $2^{\frac{1}{10}2^n}$ of the Boolean functions over $\mathbb{F}_2^n$ and cannot be tested with less than $\frac{1}{20}2^n$ queries. This family of functions is not necessarily linear invariant, so we just "close" it under linear transformation, by adding to the property all the linear-transformed such functions. Since the number of these linear transformation is bounded by 2^{n^2} (corresponding to all possible $n \times n$ matrices over $\mathbb{F}_2$) we get that the new property contains at most $2^{n^2}2^{\frac{1}{10}2^n} \leq 2^{\frac{1}{5}2^n}$ Boolean functions. One can verify that since this new family contains a small fraction of all possible functions the argument of [5] caries over, and the new property cannot be tested with $o(2^n)$ queries.
- Our proof techniques actually show testability for a class of properties slightly larger than that specified in Theorem 3. We can use Lemma 2.7 from [27] to show that whenever the linear system of equations described by the matrix M is of complexity 1 (see [43] or [27] for definition), then our Lemma 19 still holds while the rest of the proof machinery is unaffected. For linear systems of larger complexity, bounds on higher-order Gowers norms are needed to control the terms in the counting lemma.
- The upper bound one obtains from the general result given in Theorem 3 is huge. A natural open problem would be to find a characterization of these properties that can be tested with a number of queries that depends polynomially on ϵ. This, however, seems to be a very hard problem. Even if the only forbidden equation is $x + y = z$ it is not known if such an efficient test exists. This question was raised by Green [24]; see [44] for current best bounds.
- Our result here gives a (conjectured) characterization of the linear-invariant properties of Boolean functions that can be tested with one-sided error. It is of course natural to try to extend our framework to other families of properties, characterized by other or more general invariances. For instance, can we carry out a full characterization for testable affine invariant properties of Boolean functions on the hypercube?
- It would be valuable to understand formally why the technology developed for handling graph properties can be extended so naturally to linear-invariant properties. This "coincidence" seems part of a larger trend in mathematics where claims about subsets find analogs in claims about vector subspaces. See [45] for an interesting attempt to shed light on this puzzle.

[9]Note that any property can be tested with 2^n by simply querying f on all $x \in \mathbb{F}_2^n$.

Acknowledgements: Arnab would like to thank Eldar Fischer for some initial stimulating discussions during a visit to the Technion and Alex Samorodnitsky for constant encouragement and advice.

References

[1] M. Sudan, "Invariance in property testing," *Electronic Colloquium in Computational Complexity*, vol. TR10-051, March 2010.

[2] M. Blum, M. Luby, and R. Rubinfeld, "Self-testing/correcting with applications to numerical problems," *J. Comp. Sys. Sci.*, vol. 47, pp. 549–595, 1993, earlier version in STOC'90.

[3] R. Rubinfeld and M. Sudan, "Robust characterizations of polynomials with applications to program testing," *SIAM J. on Comput.*, vol. 25, pp. 252–271, 1996.

[4] L. Babai, L. Fortnow, and C. Lund, "Non-deterministic exponential time has two-prover interactive protocols," *Computational Complexity*, vol. 1, no. 1, pp. 3–40, 1991.

[5] O. Goldreich, S. Goldwasser, and D. Ron, "Property testing and its connection to learning and approximation," *Journal of the ACM*, vol. 45, pp. 653–750, 1998.

[6] M. Parnas, D. Ron, and A. Samorodnitsky, "Testing basic boolean formulae," *SIAM J. Discrete Math.*, vol. 16, no. 1, pp. 20–46, 2002.

[7] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron, "Testing Reed-Muller codes," *IEEE Transactions on Information Theory*, vol. 51, no. 11, pp. 4032–4039, 2005.

[8] A. Samorodnitsky, "Low-degree tests at large distances," in *STOC*, 2007, pp. 506–515.

[9] E. Fischer, G. Kindler, D. Ron, S. Safra, and A. Samorodnitsky, "Testing juntas," *J. Comp. Sys. Sci.*, vol. 68, no. 4, pp. 753–787, 2004.

[10] E. Blais, "Testing juntas nearly optimally," in *STOC*, 2009, pp. 151–158.

[11] I. Diakonikolas, H. K. Lee, K. Matulef, K. Onak, R. Rubinfeld, R. A. Servedio, and A. Wan, "Testing for concise representations," in *FOCS*, 2007, pp. 549–558.

[12] K. Matulef, R. O'Donnell, R. Rubinfeld, and R. A. Servedio, "Testing halfspaces," in *SODA*, 2009, pp. 256–264.

[13] T. Kaufman and M. Sudan, "Sparse random linear codes are locally decodable and testable," in *FOCS*, 2007, pp. 590–600.

[14] S. Kopparty and S. Saraf, "Tolerant linearity testing and locally testable codes," in *APPROX-RANDOM*, 2009, pp. 601–614.

[15] E. Fischer, "The art of uninformed decisions: A primer to property testing," in *Current Trends in Theoretical Computer Science: The Challenge of the New Century*, G. Paun, G. Rozenberg, and A. Salomaa, Eds. World Scientific Publishing, 2004, vol. 1, pp. 229–264.

[16] R. Rubinfeld, "Sublinear time algorithms," in *Proceedings of International Congress of Mathematicians 2006*, vol. 3, 2006, pp. 1095–1110.

[17] D. Ron, "Property Testing: A Learning Theory Perspective," in *Foundations and Trends in Machine Learning*, 2008, vol. 1, no. 3, pp. 307–402.

[18] N. Alon and A. Shapira, "A characterization of the (natural) graph properties testable with one-sided error," *SIAM J. on Comput.*, vol. 37, no. 6, pp. 1703–1727, 2008.

[19] N. Alon, E. Fischer, I. Newman, and A. Shapira, "A combinatorial characterization of the testable graph properties: it's all about regularity," in *STOC'06: Proceedings of the 38th Annual ACM Symposium on Theory of Computing*, 2006, pp. 251–260.

[20] T. Kaufman and M. Sudan, "Algebraic property testing: the role of invariance," in *Proc. 40th Annual ACM Symposium on the Theory of Computing*. New York, NY, USA: ACM, 2008, pp. 403–412.

[21] E. Grigorescu, T. Kaufman, and M. Sudan, "2-transitivity is insufficient for local testability," in *IEEE Conference on Computational Complexity*, 2008, pp. 259–267.

[22] ——, "Succinct representation of codes with applications to testing," in *APPROX-RANDOM*, 2009, pp. 534–547.

[23] E. Ben-Sasson and M. Sudan, "Limits on the rate of locally testable affine-invariant codes," November 2009, manuscript.

[24] B. Green, "A Szemerédi-type regularity lemma in abelian groups," *Geometric and Functional Analysis*, vol. 15, no. 2, pp. 340–376, 2005.

[25] A. Shapira, "Green's conjecture and testing linear-invariant properties," in *Proc. 41st Annual ACM Symposium on the Theory of Computing*, 2009, pp. 159–166.

[26] D. Král', O. Serra, and L. Vena, "A removal lemma for systems of linear equations over finite fields," *Israel Journal of Mathematics (to appear)*, 2008, preprint available at http://arxiv.org/abs/0809.1846.

[27] A. Bhattacharyya, V. Chen, M. Sudan, and N. Xie, "Testing linear-invariant non-linear properties," in *STACS*, 2009, pp. 135–146, full version at http://www.eccc.uni-trier.de/report/2008/088/.

[28] T. Austin and T. Tao, "On the testability and repair of hereditary hypergraph properties," *Random Structures and Algorithms (to appear)*, 2008, preprint available at http://arxiv.org/abs/0801.2179.

[29] V. Rödl and M. Schacht, "Generalizations of the removal lemma," *Combinatorica*, vol. 29, no. 4, pp. 467–502, 2009.

[30] P. Gopalan, R. O'Donnell, R. A. Servedio, A. Shpilka, and K. Wimmer, "Testing Fourier dimensionality and sparsity," in *ICALP (1)*, 2009, pp. 500–512.

[31] N. Alon, E. Fischer, M. Krivelevich, and M. Szegedy, "Efficient testing of large graphs," *Combinatorica*, vol. 20, no. 4, pp. 451–476, 2000.

[32] O. Goldreich and L. Trevisan, "Three theorems regarding testing graph properties," *Random Structures and Algorithms*, vol. 23, no. 1, pp. 23–57, 2003.

[33] N. Alon and A. Shapira, "A separation theorem in property testing," *Combinatorica*, vol. 28, pp. 261–281, 2008.

[34] E. Ben-Sasson, P. Harsha, and S. Raskhodnikova, "Some 3cnf properties are hard to test," *SIAM J. on Comput.*, vol. 35, no. 1, pp. 1–21, 2005.

[35] A. Bhattacharyya, S. Kopparty, G. Schoenebeck, M. Sudan, and D. Zuckerman, "Optimal testing of Reed-Muller codes," *Electronic Colloquium in Computational Complexity*, vol. TR09-086, October 2009.

[36] E. Blais and R. O'Donnell, "Lower bounds for testing function isomorphism," in *Proc. 25th Annual IEEE Conference on Computational Complexity (to appear)*, 2010.

[37] E. Fischer, "The difficulty of testing for isomorphism against a graph that is given in advance," *SIAM J. on Comput.*, vol. 34, no. 5, pp. 1147–1158, 2005.

[38] E. Szemerédi, "Regular partitions of graphs," in *Proc. Colloque Internationaux CNRS 260 -âĂŤ Problèmes Combinatoires et Théorie des Graphes*, J. Bremond, J. Fournier, M. L. Vergnas, and D. Sotteau, Eds., 1978, pp. 399–401.

[39] B. Green and T. Tao, "An arithmetic regularity lemma, associated counting lemma, and applications," February 2010, preprint available at http://arxiv.org/abs/1002.2028.

[40] C. Chvatál, V. Rödl, E. Szemerédi, and W. T. Trotter Jr., "The Ramsey number of a graph with bounded maximum degree," *Journal of Combinatorial Theory, Series B*, vol. 34, no. 3, pp. 239–243, 1983.

[41] W. T. Gowers, "A new proof of Szeméredi's theorem," *Geometric Functional Analysis*, vol. 11, no. 3, pp. 465–588, 2001.

[42] B. Green, Personal communication, February 2010.

[43] B. Green and T. Tao, "Linear equations in primes," April 2008, preprint available at http://arxiv.org/abs/math/0606088v2.

[44] A. Bhattacharyya and N. Xie, "Lower bounds for testing triangle-freeness in boolean functions," in *Proc. 21st ACM-SIAM Symposium on Discrete Algorithms*. Philadelphia, PA, USA: Society for Industrial and Applied Mathematics, 2010, pp. 87–98.

[45] H. Cohn, "Projective geometry over $\mathbb{F}_1$ and the Gaussian binomial coefficients," *American Mathematical Monthly*, vol. 111, pp. 487–495, 2004.