Robust testing of lifted codes with applications to low-degree testing

Alan Guo Elad Haramaty Madhu Sudan

Abstract

A local tester for a code probabilistically views a small set of coordinates of a given word and based on this local view accepts codewords with probability one while rejecting words far from the code with constant probability. A local tester for a code is said to be "robust" if the local views of the tester are far from acceptable views when the word being tested is far from the code. Robust testability of codes play a fundamental role in constructions of probabilistically checkable proofs where robustness is a critical element in composition. In this work we consider a broad class of codes, called lifted codes, that include codes formed by low-degree polynomials, and show that an almost natural test, extending a low-degree test proposed by Raz and Safra (STOC 1997), is robust. Our result is clean and general — the robustness of the test depends only on the distance of the code being lifted, and is positive whenever the distance is positive.

We use our result to get the first robust low-degree test that works when the degree of the polynomial being tested is more than half the field size. Our results also show that the high-rate codes of Guo et al. (ITCS 2013) are robustly locally testable with sublinear query complexity. Guo et al. also show several other interesting classes of locally testable codes that can be derived from lifting and our result shows all such codes have robust testers, at the cost of a quadratic blowup in the query complexity of the tester. Of technical interest is an intriguing relationship between tensor product codes and lifted codes that we explore and exploit.

Keywords: Error-correcting codes, Locally testable codes, low-degree testing, Affine-invariance.

I. Introduction

In this we work prove that a natural class of "testers" for a broad class of codes called "lifted codes" are "robust". We explain these terms below.

Let $\mathbb{F}_q$ denote the finite field of cardinality q. In this work we consider codes $\mathcal{C} \subseteq \mathbb{F}_q^n$ that are *linear* (i.e., $\mathcal{C}$ forms a vector space over $\mathbb{F}_q$). Rather than thinking of words in $\mathbb{F}_q^n$ as sequences of length n, we will view them as functions from some fixed set S of cardinality n to the range $\mathbb{F}_q$. (The structure of the set S and symmetries will play a role later in the paper.) We use $\{S \to \mathbb{F}_q\}$ to denote the set of all such functions. The rate of a code is the ratio $\dim(\mathcal{C})/n$ and (relative) distance is the quantity $\min_{f \neq g \in \mathcal{C}}\{\delta(f,g)\}$ where $\delta(f,g) = \frac{1}{n} \cdot |\{x \in S | f(x) \neq g(x)\}|$ is the distance between f and g. We say f is τ-far from $\mathcal{C}$ if $\delta(f,\mathcal{C}) \triangleq \min_{g \in \mathcal{C}}\{\delta(f,g)\} \geq \tau$.

Given a code $\mathcal{C} \subseteq \{S \to \mathbb{F}_q\}$ and integer ℓ, an *ℓ-local tester* $\mathcal{T}$ is a distribution $\mathcal{D}$ on $S^\ell \times \mathcal{P}(\mathbb{F}_q^\ell)$[1] with the semantics as follows: Given oracle access to $f : S \to \mathbb{F}_q$, the tester $\mathcal{T}$ samples $(\pi, V) \leftarrow \mathcal{D}$, where $\pi = (\pi_1, \ldots, \pi_\ell) \in S^\ell$ and $V \subseteq \mathbb{F}_q^\ell$, and accepts f if and only if $f|_\pi \triangleq (f(a_1), \ldots, f(a_\ell)) \in V$. The tester is said to be *ϵ-sound* if $\mathcal{T}$ accepts $f \in \mathcal{C}$ with probability one, while rejecting f that is δ-far from $\mathcal{C}$ with probability at least $\epsilon \cdot \delta$.

In this work we are interested in a stronger property of testers known as their robustness, formally defined by Ben-Sasson and Sudan [BSS06] based on analogous notions in complexity theory due to Ben-Sasson et al. [BSGH$^+$04] and Dinur and Reingold [DR04]. The hope with a robust tester is that, while it may make a few more queries than the minimum possible, the rejection is "more emphatic"

[1]For a finite set U, $\mathcal{P}(U)$ denotes the set of all subsets of U.

in that functions that are far from $\mathcal{C}$ typically yield far from acceptable views, i.e., if $\delta(f,\mathcal{C})$ is large then so is $\delta(f|_\pi, V)$ for typical choices of $(\pi, V) \leftarrow \mathcal{D}$. Formally, we say that a tester $\mathcal{T}$ is α-robust if $\mathbb{E}_{(\pi,V)\leftarrow\mathcal{D}}[\delta(f|_\pi, V)] \geq \alpha \cdot \delta(f,\mathcal{C})$. In this work we will be interested in tests for infinite families of codes $\{\mathcal{C}_n \subseteq \mathbb{F}_q^n\}_n$ with *sublinear locality*, i.e., $\ell(n) = o(n)$, and *constant robustness* $\alpha(n) \geq \alpha > 0$.

From the definitions, and the fact that $\delta(f|_\pi, V) \leq 1$ for every (π, V), it follows that an α-robust tester is also α-sound. On the other hand an α-sound ℓ-local tester is at least (α/ℓ)-robust. But robustness can be a much stronger property than mere soundness since it allows for composition with other local testers. In particular, if there is an α-robust tester for f with distribution $\mathcal{D}$ and if for every (π, V) in the support of $\mathcal{D}$, the property of being in V has an ℓ'-local tester that is ϵ-sound, then $\mathcal{C}$ has an ℓ'-local tester that is $\alpha \cdot \epsilon$-sound. The hope that membership in V has a nice local test for *every* V in the support of $\mathcal{D}$ may seem overly optimistic, but for many symmetric codes (as the ones considered in this work) all the V's are isomorphic — so the many different "hopes" combine to a single one. We illustrate the concept of robustness in the context of low-degree testing and describe the role it has played in applications.

A. Low-degree testing

One of the classical problems for which testers have been explored extensively and many applications found is the task of low-degree testing. This task corresponds to the case where $\mathcal{C} = \mathcal{C}_{m,d,q}$ has as its domain $S = \mathbb{F}_q^m$ and $\mathcal{C}$ consists of all m-variate functions that are polynomials of degree at most d. Low-degree testing was studied first in the work of Rubinfeld and Sudan [RS96] and many variations have been analyzed in many subsequent works — a partial list includes [ALM$^+$98], [FS95], [AS03], [RS97], [MR06], [AKK$^+$05], [KR06], [JPRZ09], [BKS$^+$10], [HSS11]. When $d \ll q$ low-degree tests making as few as $d+2$ queries are known, that have $1/\operatorname{poly}(d)$-soundness (see, for instance, Friedl-Sudan [FS95]). However, tests that make $O(d)$ queries achieve constant soundness (a universal constant independent of m, d, q provided q is sufficiently larger than d), and even constant robustness. This constant robustness is central to the PCP construction of Arora et al.[ALM$^+$98]. In all cases with $d \ll q$, low-degree tests operate by considering the restriction of a function to a random line, or "plane" (namely a 2-dimensional affine subspace), in the domain, and accepting a function if it is a polynomial of degree at most d on the restricted subspaces. Thus, the different restrictions π are different affine subspaces of low-dimension (one or two) and the acceptable pattern V is the same for all π. In particular the robust analysis of the low-degree test allows for low-query tests, or even proofs, of membership in V in constant dimensional spaces to be composed with the low-degree test in high-dimensions to yield low-query PCPs. Robustness turns out to be much more significant as a parameter to analyze in these results than the query complexity of the outer test. Indeed subsequent strengthenings of the PCP theorem in various senses (e.g., in [AS03], [RS97], [MR06] rely on improving the robustness to a quantity close to 1, and this leads to PCPs of arbitrarily small constant, and then even $o(1)$, error.

B. Lifted Codes and Testing

In this work we consider robust testing of "lifted codes". A family of lifted codes is specified by a *base code* $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$. The family is indexed by positive integer $m \geq t$ and the *m-dimensional lifted* code $\mathcal{C}^{t\nearrow m}$ consists of all functions $f : \mathbb{F}_q^m \to \mathbb{F}_q$ such that for every t-dimensional affine subspace A in $\mathbb{F}_q^m$, the restriction of f to A, denoted $f|_A$, is contained in $\mathcal{C}$. (For the definition to be natural it is best if $\mathcal{C}$ is affine-invariant, i.e., $f \in \mathcal{C} \Leftrightarrow f \circ T \in \mathcal{C}$ for every affine bijection $T : \mathbb{F}_q^m \to \mathbb{F}_q^m$.)

Lifted codes were first defined by Ben-Sasson et al. [BSMSS11] and subsequently explored systematically by Guo et al. [GKS13]. Lifted codes naturally generalize the notion of low-degree polynomials. Indeed the characterization that for $d < q/2$ the family of degree d m-variate polynomials is the lift of univariate degree polynomials, is the basis of the low-degree test in [RS96], [FS95]; and extensions to settings where $d > q/2$ in [KR06] forms the basis of their low-degree test. But lifted codes give other

families of codes as well. They form a natural subclass of "affine-invariant" codes that have been studied in the context of local testing by Kaufman and Sudan [KS08] and many subsequent works (e.g., [GKS08], [GKS09], [KL10], [BGM+11]): A code $\mathcal{C} \subseteq \{\mathbb{F}_{q^t}^m \to \mathbb{F}_q\}$ is *affine-invariant* if for every affine bijection (permutation) $A : \mathbb{F}_{q^t}^m \to \mathbb{F}_{q^t}^m$ we have $f \in \mathcal{C} \Leftrightarrow f \circ A \in \mathcal{C}$. They satisfy a property termed the "single-orbit" property in [KS08] that makes them locally testable, and indeed with some fairly strong analysis as shown by Haramaty et al. [HRS13]. In particular, they give codes of rate arbitrarily close to 1 and positive distance that have n^α-local testers on codes of length n for arbitrarily small α [GKS13]. Lifted codes have essentially the same distance as base code, and they are locally correctible as well, making them general and sometimes powerful extensions of low-degree polynomials.

Lifted codes have a natural test - to test $\mathcal{C}^{t\nearrow m}$, pick a random t-dimensional subspace A in $\mathbb{F}_q^m$ and verify that $f|_A \in \mathcal{C}$. Such a test is known to be q^{-2t}-sound [KS08] and even ϵ_q-sound (independent of t) [HRS13]. These analyses however are not robust, or more accurately, the soundness as well as robustness of these tests degrades with q. In this work we analyze a slightly less natural test and show that it has good robustness if the underlying code has good distance, with the robustness depending only on the distance.

C. Our results

In this work we propose and analyze the following test for $\mathcal{C}^{t\nearrow m}$: Pick a random $2t$-dimensional subspace A in $\mathbb{F}_q^m$ and accept if $f|_A \in \mathcal{C}^{t\nearrow 2t}$. Our main theorem relates the robustness of this test to the distance of the code $\mathcal{C}$.

Theorem I.1. *$\forall \delta > 0$ $\exists \alpha > 0$ such that the following holds: For every finite field $\mathbb{F}_q$, for every pair of positive integers t and m and for every affine-invariant code $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ satisfying $\delta(\mathcal{C}) \geq \delta$, the code $\mathcal{C}^{t\nearrow m}$ has a q^{2t}-local test that is α-robust.*

The special case of Theorem I.1 for $t = 1$ is proved in Section V. The general case is proved in the full version of this paper [GHS15]. As we elaborate below, Theorem I.1 immediately implies a robust analysis for low-degree tests. Whereas almost all previous robust analyses of low-degree tests had more complex conditions on the relationship betwen the robustness, the degree, and the field size - our relationship is extremely clean. The dependence α on δ that we prove is polynomial but of fairly high degree $\alpha = \Omega(\delta^{74})$. We do not attempt to improve this relationship in this paper and choose instead to keep the intermediate statements simple and general. We note that a significant portion of this complexity arises due to our desire to lift t-dimensional codes for general t, and here the fact that the robustness lower-bound is independent of t is itself significant.

Comparing with other testing results for lifted codes, there are only two prior works to compare with: Kaufman and Sudan [KS08] analyze a tester for a broader family of codes that they call "single-orbit" codes. Their result would yield a robustness of $\Theta(q^{-3t})$. (See Corollary II.8.) Haramaty et al. [HRS13] also give a tester for lifted codes. They don't state their results in terms of robustness but their techniques would turn into a robustness of $\epsilon_q \cdot \delta$, where the ϵ_q is a positive constant for constant q but goes to zero extremely quickly as $q \to \infty$. Thus for growing q (and even slowly shrinking δ) our results are much stronger.

Turning to consequences of our main theorem, a direct corollary obtained by applying Theorem I.1 to codes developed by Guo et al. [GKS13] are codes of rate close to 1 that have n^ϵ-local $\Omega(1)$-robust local testers.

Corollary I.2. *$\forall \epsilon, \beta > 0$, $\exists \alpha > 0$ such that for infinitely many n there exists $q = q(n) = O(n^\epsilon)$ and a linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of rate $1 - \beta$ that has an α-robust n^ϵ-local tester.*

The only other prior construction of codes that achieve such properties were the tensor product codes of Viderman [Vid12].

Even applied to the classical task of low-degree testing our results are new. An almost direct corollary of our main theorem is a q^4-local robust low-degree test for the setting $d \leq (1-\delta)q$. To see why we get q^4 queries, note that when $d > q/2$ then the set of m-variate degree d polynomials are not equal to the m-dimensional lift of the set of degree d univariate polynomials. But they do turn out to be the m-dimensional lifts of the set of degree d bivariate polynomials. Applying our testing result to this lifted family yields a robust test making q^4 queries. But with some slight extra work we can get a better tester that makes only q^2 queries and this yields the following theorem.

Theorem I.3. *$\forall \delta > 0$ $\exists \alpha > 0$ such that the following holds: For every finite field $\mathbb{F}_q$, for every integer $d \leq (1-\delta)q$ and every positive integer m, there is a q^2-query α-robust low-degree test for the class of m-variate polynomials of degree at most d over $\mathbb{F}_q$.*

We note that previous works on low-degree testing worked only when $d < q/2$. This ratio seems to be achieved by Friedl and Sudan (see [FS95, Theorem 13]). Other works [RS96], [ALM+98], [RS97], [AS03], [MR06] seem to achieve weaker ratios for a variety of reasons that we discuss below.

D. Proof approach and some technical contributions

In order to describe our test and analysis techniques, we briefly review the two main tests proposed in the literature for "low-degree testing", when the field size is much larger than the degree. The most natural test for this task is the one that picks a random line in $\mathbb{F}_q^m$ and computes the proximity of the function restricted to this line to the space of univariate degree d polynomials. This is the test proposed by Rubinfeld and Sudan [RS96] and analyzed in [RS96], [ALM+98], [AS03]. A second low-degree test is somewhat less efficient in its query complexity (quadratically so) but turns out to have a much simpler analysis — this test would pick a random two-dimensional (affine) subspace in $\mathbb{F}_q^m$ and verify that the function is a bivariate polynomial of degree at most d on this subspace. This is the test proposed by Raz and Safra [RS97] and analyzed in [RS97], [MR06]. Both tests can be analyzed by first reducing the testing problem to that of testing constant variate functions (at most four variate functions) and then analyzing the constant dimensional problem as a second step.

The first step is completely generic or at least it was sensed to be so. However there was no prior formalization of the fact that it is generic. The only class of functions to which it has been applied are the class of low-degree polynomials and a priori it is not clear how to even justify the claim of genericity. Here we show that the first step applies to all lifted codes and thus giving the first justification of the presumed genericity of this step, which we consider to be a conceptual contribution.

For the second step, the robust analyses in [ALM+98], [AS03] are quite algebraic and there seems to be no hope to use them on general lifted codes. The test and analysis of Raz and Safra [RS97] on the other hand feels much more generic. In this work we use their test, and extend it to general lifted codes and show that it is robust. Even the extension of the test is not completely obvious. In particular, to test low-degree polynomials they look at restrictions of the given function to 2-dimensional "planes". When lifting t-dimensional properties, it is not immediate what would be the dimension of the restrictions the test should look at: Should it be $t+1$? or $2t$ or maybe $3t-1$ (each of which does make logical sense)? We show that the $2t$ dimensional tests are robust, with robustness being independent of t.

Next we turn to our analysis. In showing robustness of their test, applied to generic lifted codes there is a major barrier: Almost all analyses of low-degree tests, for polynomials of degree at most d, attempt to show first that a function passing the test with high probability is close to a polynomial of degree *twice* the degree, i.e., at most $2d$, with some additional features. They then use the distance of the space of

polynomials of degree $2d$ and the additional features to establish that the function being tested is really close to a degree d polynomial. In extending such analyses to our setting we face two obstacles: In the completely generic setting, there is no nice notion corresponding to the set of degree $2d$ polynomials. One approach might be to consider the linear space spanned by products of functions in our basic space and work with them, but the algebra gets hairy to understand and analyze. Even if we abandon the complete genericity and stick to the space of polynomials of degree d, but now allow $d > q/2$ we hit a second obstacle: The space of polynomials of degree $2d$ have negligible relative distance compared to the space of polynomials of degree d.

Thus we need to search for a new proof technique and we find one by unearthing a new connection between "lifted codes" and "tensor product" codes. The tensor product is a natural operation in linear algebra and when applied to two linear codes, it produces a new linear code in a natural way. Tensor products of codes are well-studied in the literature on coding theory. The testing of tensor product codes was initiated by Ben-Sasson and Sudan [BSS06] and subsequently has been well-studied [DSW06], [Val05], [BSV09b], [BSV09a], [GGR09]. Specifically, a recent result of Viderman [Vid12] gives a powerful analysis which we are able to reproduce in a slightly different setting to get our results. In particular this is the ingredient that allows us to work with base codes whose distance is less than $1/2$. Also, for the sake of the exposition we pretend that this test can test two-dimensional tensor products of one dimensional codes, with one-dimensional tests. (Actually, the test works with three dimensional tensors and tests them by looking at two-dimensional planes, but by suppressing this difference, our exposition becomes a little simpler.)

To explain the connection between lifted codes and tensor product codes, and the idea that we introduce to test the former, we turn to the simple case of testing a bivariate lift of a univariate Reed-Solomon code. Specifically, let $\mathcal{C}$ be the family of univariate polynomials of degree at most d mapping $\mathbb{F}_q$ to $\mathbb{F}_q$. Let $\mathcal{C}_2$ be the family of bivariate polynomials that become a univariate polynomial of degree at most d on every restriction to a line. The tensor product of the $\mathcal{C}$ with itself, which we denote $\mathcal{C}^{\otimes 2}$ corresponds to the set of bivariate polynomials of degree at most d in each variable. Clearly $\mathcal{C}_2 \subseteq \mathcal{C}^{\otimes 2}$ but such subset relationships are not of immediate use in testing a code. (Indeed locally testable codes contain many non-LTCs.) To get a tighter relationship, now fix two "directions"[2] d_1 and d_2 and let $\mathcal{C}_{d_1,d_2}$ be the code containing all bivariate polynomials over $\mathbb{F}_q$ that on every restriction to lines in directions d_1 and d_2 form univariate degree d polynomials. On the one hand the code $\mathcal{C}_{d_1,d_2}$ is just isomorphic to the tensor product code $\mathcal{C}^{\otimes 2}$ which is testable by the natural test, by our assumption. On the other hand, we now have $\mathcal{C}_2 = \cap_{d_1,d_2}\mathcal{C}_{d_1,d_2}$ so we now have a characterization of the lifted codes in terms of the tensor product. One might hope that one could use this characterization to get a (robust) analysis of the lifted test since it tests membership in $\mathcal{C}_{d_1,d_2}$ for random choices of d_1 and d_2, but unfortunately we do not see a simple way to implement this hope.

Our key idea is look instead at a more complex family of codes $\mathcal{C}_{d_1,d_2,d_3}$ that consists of functions of degree d in directions d_1, d_2 and d_3. (Of course now d_1, d_2, d_3 are linearly dependent and so $\mathcal{C}_{d_1,d_2,d_3}$ is not a tensor product code. We will return to this issue later.) We still have $\mathcal{C}_2 = \cap_{d_1,d_2,d_3}\mathcal{C}_{d_1,d_2,d_3}$. Indeed we can even fix d_1, d_2 arbitrarily (only requiring them to be linearly independent) and we have $\mathcal{C}_2 = \cap_{d_3}\mathcal{C}_{d_1,d_2,d_3}$. This view turns out to be more advantageous since we now have that for any d_3 and d_3' we have $\mathcal{C}_{d_1,d_2,d_3} \cup \mathcal{C}_{d_1,d_2,d_3'} \subseteq \mathcal{C}_{d_1,d_2}$ which is a code of decent distance. This allows us to show that if the function being tested is close to $\mathcal{C}_{d_1,d_2,d_3}$ for many choices of d_3 then the nearest codewords for all these choices of d_3 are *the same*. An algebraic analysis of lifted codes tells us that a codeword of $\mathcal{C}_{d_1,d_2}$ can not be in $\mathcal{C}_{d_1,d_2,d_3}$ for many choices of d_3 without being a codeword of the lifted code and this lends

[2]Informally a direction refers to the slope of the line. This may be formalized by considering all non-zero pairs $(a, b) \in \mathbb{F}_q^2$ under the equivalence $(a, b) \sim (c, d)$ if $ad = bc$.

promise to our idea. But we are not done, since we still need to test the given function for proximity to $\mathcal{C}_{d_1,d_2,d_3}$ and this is no longer a tensor product code so Viderman's result does not apply directly. Fortunately, we are able to develop the ideas from Viderman's analysis for tensor product codes [Vid12] and apply them also to our case and this yields our test and analysis. We note that this extension is not immediate — indeed one of the central properties of tensor product codes is that they are decodable from some clean erasure patterns and this feature is missing in our codes. Nevertheless the analysis can be modified to apply to our codes and this suffices to complete the analysis.

In the actual implementation, as noted earlier, we can't work with univariate tests even for the simple case above, and work instead by using a bivariate test for trivariate and 4-variate functions. (This is similar to the reasons why Raz and Safra used a bivariate test.) This complicates the notations a bit, but the idea remains similar to the description above. Our task gets more complicated when the base code being lifted is t-dimensional for $t > 1$. The most natural adaptation of our analysis leads to dependencies involving δ (the distance of the base code) and t. We work somewhat harder in this case to eliminate any dependence on t while working within the framework described above.

Organization: We describe some preliminary background in Section II. The rest of the paper is devoted to the proof of Theorem I.1 for the special case of $t = 1$. In Section III we analyze the robustness $m-1$-dimensional tests of m-dimensional lifts. This analysis reduces to the analysis of a special class of "tensor-like" codes which we perform in Section IV. In Section V we show how to use the analysis from Section III, in particular for the cases $m = 3$ and $m = 4$, to get a robust analysis of 2-dimensional tests of arbitrarily high-dimensional lifts. In the full version of this paper [GHS15] we show how to convert the analysis of lifted-code testers to get a robust low-degree test.

II. Preliminaries

We present some basic background and definitions related to lifted codes and their testing. We describe some previous testers that offer weak robustness (that depends on q and t). We then introduce the notion of tensor product codes which will play a central role in our proofs. Finally, we describe some of the basic geometry of affine subspaces in $\mathbb{F}_q^m$.

We include some very basic terminology here. The full version [GHS15] of this paper contains more detailed background.

A. Affine-invariance and degree sets

Definition II.1. A code $\mathcal{C} \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ is *affine-invariant* if $f \in \mathcal{C}$ if and only if $f \circ A \in \mathcal{C}$ for every affine bijection $A : \mathbb{F}_q^m \to \mathbb{F}_q^m$.

Definition II.2. For prime p and integers $a = \sum_{i\geq 0} a^{(i)} p^i$ and $b = \sum_{i\geq 0} b^{(i)} p^i$ with $0 \leq a^{(i)}, b^{(i)} \leq p-1$ for each $i \geq 0$, *a is in the p-shadow of b*, denoted by $a \leq_p b$, if $a^{(i)} \leq b^{(i)}$ for all $i \geq 0$.

Definition II.3. A code $\mathcal{C} \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ *has a degree set* if there is a set $D \subseteq \{0, 1, \ldots, q-1\}^m$ such that $\mathcal{C} = \{f : \mathbb{F}_q^m \to \mathbb{F}_q \mid \mathrm{supp}(f) \subseteq D\}$, where $\mathrm{supp}(f)$ is the set of all exponents of monomials in the support of the unique polynomial representing f. Denote $\mathrm{Deg}(\mathcal{C}) \triangleq D$. The degree set $\mathrm{Deg}(\mathcal{C})$ is *p-shadow-closed* if, whenever $\mathbf{d} \in \mathrm{Deg}(\mathcal{C})$ and $\mathbf{e} \leq_p \mathbf{d}$, then $\mathbf{e} \in \mathrm{Deg}(\mathcal{C})$.

We now state a basic proposition about the degree sets of affine-invariant codes. This proposition follows immediately from Lemmas 4.2 and 4.3 in [KS08]. Specifically, Lemma 4.2 establishes the existence of a degree set and Lemma 4.3 implies that it is p-shadow closed.

Proposition II.4 ([KS08])**.** *Every linear affine-invariant code over $\mathbb{F}_q$ of characteristic p has a p-shadow-closed degree set.*

B. Lifting

Whenever $f : \mathbb{F}_q^m \to \mathbb{F}_q$ and $A \subseteq \mathbb{F}_q^m$ is a k-dimensional affine subspace, we think of A as being parameterized by some affine function $A : \mathbb{F}_q^k \to \mathbb{F}_q^m$ (abusing notation) and by the restriction $f|_A$ of f to A, we mean the k-variate function $f \circ A$. This definition depends on the parameterization of A, but if $\mathcal{C}$ is affine-invariant, then whether $f|_A \in \mathcal{C}$ does not depend on this parameterization. We define lines and planes to be 1-dimensional and 2-dimensional affine subspaces respectively.

Definition II.5. Let $m \in \mathbb{N}$ and let $\mathcal{C} \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ be affine-invariant. Then the *m-dimensional lift $\mathcal{C}^{\uparrow m}$ of $\mathcal{C}$* is the code

$$\mathcal{C}^{\uparrow m} \triangleq \left\{ f : \mathbb{F}_q^m \to \mathbb{F}_q \;\middle|\; f|_l \in \mathcal{C} \text{ for any line } l \right\}$$

C. Testing and robustness

We now define the robustness of a lifted code, specializing the definition to robustness with respect to subspace testers.

Definition II.6. Let $k \leq m$. The code $\mathcal{C}^{\uparrow m}$ is (α, k)-*robust* if, for every $r : \mathbb{F}_q^m \to \mathbb{F}_q$,

$$\mathbb{E}_A \left[\delta \left(r|_A, \mathcal{C}^{\uparrow k} \right) \right] \geq \alpha \cdot \delta \left(r, \mathcal{C}^{\uparrow m} \right)$$

where the expectation is over uniformly random k-dimensional affine subspaces $A \subseteq \mathbb{F}_q^m$. When k is clear from context, we say the code is α-robust.

In this terminology we wish to show that $\mathcal{C}^{\uparrow m}$ is $(\alpha, 2)$-robust for some α depending only on $\delta(\mathcal{C})$.

Observe that if A is a random k_1-dimensional subspace and B is a random k_2-dimensional subspace, where $k_2 \geq k_1$, then

$$\mathbb{E}_A \left[\delta \left(r|_A, \mathcal{C}^{\uparrow k_1} \right) \right] = \mathbb{E}_B \left[\mathbb{E}_{A \subseteq B} \left[\delta \left(r|_A, \mathcal{C}^{\uparrow k_1} \right) \right] \right] \leq \mathbb{E}_B \left[\delta \left(r|_B, \mathcal{C}^{\uparrow k_2} \right) \right]$$

so if $\mathcal{C}^{\uparrow m}$ is (α, k_1)-robust, then it is also (α, k_2)-robust.

The following theorem follows from Kaufman and Sudan [KS08, Theorem 2.9].

Theorem II.7. *If $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ is linear affine-invariant, then $\mathcal{C}^{\uparrow m}$ has a line test which rejects with probability $\frac{\delta(r, \mathcal{C}^{\uparrow n})}{(2q+1)(q-1)}$.*

As a corollary to Theorem II.7, the k-dimensional test for $\mathcal{C}^{\uparrow m}$ is $O(q^{-3})$-robust.

Corollary II.8. *If $\mathcal{C} \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ is linear affine-invariant, then $\mathcal{C}^{\uparrow m}$ is $(\frac{q^{-3}}{2}, k)$-robust for $k \geq 1$.*

Proof. It suffices to show that $\mathcal{C}^{\uparrow m}$ is $(\frac{q^{-3}}{2}, 1)$-robust. Let $r : \mathbb{F}_q^m \to \mathbb{F}_q$ and l be a random line. Then

$$\begin{aligned}
\mathbb{E}_l \left[\delta \left(r|_l \mathcal{C} \right) \right] &= \mathbb{E}_l \left[\delta \left(r|_l, \mathcal{C} \right) \mid r|_l \notin \mathcal{C} \right] \cdot \Pr_l \left[r|_l \notin \mathcal{C} \right] \\
&\geq q^{-1} \cdot \Pr_u \left[r|_l \notin \mathcal{C} \right] \\
\text{(Theorem II.7)} \quad &\geq q^{-1} \cdot \frac{\delta \left(r, \mathcal{C}^{\uparrow m} \right)}{(2q+1)(q-1)} \\
&\geq \frac{q^{-3}}{2} \cdot \delta \left(r, \mathcal{C}^{\uparrow m} \right).
\end{aligned}$$

□

We will also use the fact that we can compose robustness.

Proposition II.9 (Robustness composes multiplicatively). *Let $k_1 \le k_2 \le m$ and let $\mathcal{C} \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ be linear affine-invariant. If $\mathcal{C}^{\uparrow m}$ is (α_2, k_2)-robust and $\mathcal{C}^{\uparrow k_2}$ is (α_1, k_1)-robust, then $\mathcal{C}^{\uparrow m}$ is $(\alpha_1 \cdot \alpha_2, k_1)$-robust.*

D. Tensor codes

Tensor product codes play an important role in our proof. There are many equivalent ways to define the tensor product of two codes. Since in this work we think of codes as linear subspaces of functions in $\{\mathbb{F}_q^m \to \mathbb{F}_q\}$, we define the tensor product in this context.

Definition II.10. Let $m \ge 2$ and for each $i \in [m]$, let the code $\mathcal{C}_i \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ be linear and let $V_{i,\mathbf{a}} \subseteq \mathbb{F}_q^m$ be the one dimensional subspace consisting of all points where the i-th coordinate is free and all the $[m]\backslash\{i\}$ coordinates are fixed to $\mathbf{a} \in \mathbb{F}_q^{[m]\backslash\{i\}}$. The *tensor product code* $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ is the code

$$\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m \triangleq \left\{ f : \mathbb{F}_q^m \to \mathbb{F}_q \;\middle|\; f|_{V_{i,\mathbf{a}}} \in \mathcal{C}_i \text{ for every } i \in [m] \text{ and } \mathbf{a} \in \mathbb{F}_q^{[m]\backslash\{i\}} \right\}$$

Define $\mathcal{C}^{\otimes m} \triangleq \overbrace{\mathcal{C} \otimes \cdots \otimes \mathcal{C}}^{m}$.

The following characterization of tensor product codes will be helpful.

Proposition II.11. *Let $m \ge 2$ and for each $i \in [m]$ let the code $\mathcal{C}_i \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ be linear. Then*

$$\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_n = \mathrm{span}_{\mathbb{F}_q} \left\{ \prod_{i=1}^{n} f_i(X_i) \;\middle|\; f_i \in \mathcal{C}_i \right\}$$

Corollary II.12. *If $\mathcal{C} \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ has a degree set $\mathrm{Deg}(\mathcal{C})$, and $m \ge 1$, then $\mathcal{C}^{\otimes m}$ has degree set $\mathrm{Deg}(\mathcal{C}^{\otimes m}) = \mathrm{Deg}(\mathcal{C})^m$. In particular, if $\mathcal{C}$ is linear affine-invariant, and $\mathbb{F}_q$ has characteristic p, then $\mathcal{C}^{\otimes m}$ has a p-shadow-closed degree set.*

Proposition II.13. *Let $\mathcal{C}_1, ..., \mathcal{C}_m$ be codes with distance $\delta_1, ..., \delta_m$ respectively. Then $\delta(\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m)$ is at least $\prod_{i=1}^m \delta_i$. In particular, $\delta\left(\mathcal{C}^{\otimes m}\right) \ge \delta(\mathcal{C})^m$.*

The following is a statement about the erasure decoding properties of tensor product codes.

Proposition II.14. *[BSS06, Proposition 3.1] Let $\mathcal{C} = \mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_m \in \left\{\mathbb{F}_q^m \to \mathbb{F}_q\right\}$ and $S \subseteq \mathbb{F}_q^m$ be a subset such that for every $i \in [m]$ and $\mathbf{a} \in F_q^{[m]\backslash\{i\}}$ satisfy $|S \cap V_{i,\mathbf{a}}| \ge (1 - \delta(\mathcal{C}_i))q$. Let $r : S \to \mathbb{F}_q$ be such that for every $i \in [m]$ and $\mathbf{a} \in \mathbb{F}_q^{[m]\backslash\{i\}}$ satisfy that $r|_{S \cap V_{i,\mathbf{a}}}$ can be extended into a codeword of $\mathcal{C}_i$ on $V_{i,\mathbf{a}}$. Then there exists a unique $r' \in \mathcal{C}$ such that $r'|_S = r$.*

E. Geometry over finite fields

For two sets $A, B \subseteq \mathbb{F}_q^m$, define the Minkowski sum

$$A + B \triangleq \{\mathbf{a} + \mathbf{b} \mid \mathbf{a} \in A, \mathbf{b} \in B\}$$

and define

$$\mathrm{span}(A) \triangleq \left\{ \sum_{\mathbf{a} \in A} c_{\mathbf{a}} \cdot \mathbf{a} \;\middle|\; c_{\mathbf{a}} \in \mathbb{F}_q \right\}.$$

For $\mathbf{x} \in \mathbb{F}_q^m$ and $A \subseteq \mathbb{F}_q^m$, define the subspace through $\mathbf{x}$ in directions A to be

$$(\mathbf{x}, A) \triangleq \{\mathbf{x}\} + \mathrm{span}(A).$$

Lemma II.15. *Let $k < m$. Let $l \subseteq \mathbb{F}_q^m$ be a fixed line, and let $v \subseteq \mathbb{F}_q^m$ be a uniformly random affine subspace of dimension k. Then* $\Pr_v[u \cap v \neq \emptyset] < q^{-(m-k-1)}$.

Proof. By affine symmetry, we may assume that v is fixed and l is random. Furthermore, we can assume that $v = \{\mathbf{y} \in \mathbb{F}_q^m \mid y_1 = \cdots = y_{m-k} = 0\}$. We choose l by choosing random $\mathbf{x} \in \mathbb{F}_q^m$, $\mathbf{a} \in \mathbb{F}_q^m \setminus \{\mathbf{0}\}$ and define $l(t) = \mathbf{x} + t\mathbf{a}$. If $a \in v$, then l intersect v only if $\mathbf{x} \in v$, which happens with probability $q^{-(m-k)}$. Else, there is a coordinate $i \in [m-k]$ such that $a_i \neq 0$. In this case for $t = -\frac{b_i}{a_i}$ we have that l intersect v only if for all $j \in [m-k] \setminus \{i\}$ we have that $b_j + ta_j = 0$, which happens with probability $q^{-(m-k-1)}$. □

Lemma II.16. *Let $k < m$ and $\mathbf{a}_1, \ldots, \mathbf{a}_k \in \mathbb{F}_q^m$ be uniformly chosen vectors. Then the probability that $\{\mathbf{a}_i\}_{i=1}^k$ are linearly independent is at least $1 - q^{-(m-k)}$. In particular, the probability that two t-dimensional subspaces through a point $\mathbf{x} \in \mathbb{F}_q^m$ will intersect only on $\mathbf{x}$ is at least $1 - q^{-(m-2t)}$.*

Proof. The probability that $\mathbf{a}_{i+1} \notin \operatorname{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_i\}$ given that the latter are linearly independent is $1 - q^{-(m-i)}$. Therefore the probability that all of them are independent is

$$\prod_{i=0}^{k-1}(1 - q^{-(m-i)}) \geq 1 - \sum_{i=0}^{k-1} q^{-(m-i)} = 1 - q^{-(m-k)} \sum_{i=1}^{k} q^{-i} \geq 1 - q^{-(m-k)} .$$

For the last part, observe that choosing two t-dimensional subspaces through $\mathbf{x}$ is equivalent to choose $2t$ basis vectors, given that each t are linearly independent. So the probability that they intersect only on $\mathbf{x}$, is the same as that those vectors are linearly independent. Hence, by the first part, this probability is at least $1 - q^{-(m-2t)}$. □

III. Robustness for small dimension

In this section, we show that when $m \geq 3$, $\mathcal{C}^{\uparrow m}$ is $(\alpha, m-1)$-robust for $\alpha = \frac{\delta^{2m}}{4\binom{m+1}{m-1}^2}$.

Overview: We observe that picking a random hyperplane can be done by picking m random linearly independent directions, picking an additional random direction $\mathbf{a}$ that is not spanned by any $m-1$ of former, and picking a hyperplane spanned by $m-1$ of these $m+1$ random directions (call such a hyperplane "special"). Now, viewing the first m chosen directions as the standard basis directions, we see that the average distance to the code, when restricted to special hyperplanes, is still small. We then show that, through the main technical lemma (Theorem III.5), that this implies the codeword is close to a special subcode $\mathcal{C}_{\mathbf{a}}$ of the standard tensor code $\mathcal{C}^{\otimes m}$, where in addition we insist that restrictions to lines in direction $\mathbf{a}$ are codewords of $\mathcal{C}$. Therefore, for "most" random directions $\mathbf{a}$, our function r is close to some codeword $c_{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$. Since these $c_{\mathbf{a}}$ are also codewords of $\mathcal{C}^{\otimes m}$ and they are all close to r and therefore to each other, they are actually the same codeword of $\mathcal{C}^{\otimes m}$. In fact, because this codeword is in $\mathcal{C}_{\mathbf{a}}$, we show by Proposition III.1 that it must actually be a codeword of the lift $\mathcal{C}^{\uparrow m}$. The proof of the main lemma, Theorem III.5, follows a strategy similar to that of Viderman. Throughout, we deal with the distance $\delta(\mathcal{C}^{\otimes m}) = \delta(\mathcal{C})^m$ of the tensor code $\mathcal{C}^{\otimes m}$, which degrades with m, which is why the robustness we achieve in this section degrades with m as well. In Section V, we avoid dealing with tensor codes, and use the result in this section for $m = 3$ to boost our way up to general m.

Proposition III.1. *If $f \in \mathcal{C}^{\otimes m} \setminus \mathcal{C}^{\uparrow m}$, then there is a point such that for at least δ^m fraction of lines through the point, the restriction of f to the line is not a codeword of $\mathcal{C}$. More precisely, there exists $\mathbf{b} \in \mathbb{F}_q^m$ such that for at least $\delta^m \cdot q^m$ directions $\mathbf{a} \in \mathbb{F}_q^m$, the univariate polynomial $g_{\mathbf{a},\mathbf{b}}(T) := f(\mathbf{a}T + \mathbf{b})$ is not a codeword of $\mathcal{C}$.*

Proof. Let $D = \mathrm{Deg}(\mathcal{C})$. Write $f(\mathbf{X}) = \sum_{\mathbf{d}\in D^m} f_{\mathbf{d}} \cdot \mathbf{X}^{\mathbf{d}}$. Then

$$\begin{aligned}
g_{\mathbf{a},\mathbf{b}}(T) &:= f(\mathbf{a}T + \mathbf{b}) && (1)\\
&= \sum_{\mathbf{d}\in D^m} f_{\mathbf{d}} \cdot (\mathbf{a}T + \mathbf{b})^{\mathbf{d}} && (2)\\
&= \sum_{\mathbf{d}\in D^m} f_{\mathbf{d}} \cdot \sum_{\mathbf{e}\le_p \mathbf{d}} \binom{\mathbf{d}}{\mathbf{e}} \mathbf{a}^{\mathbf{e}}\mathbf{b}^{\mathbf{d}-\mathbf{e}} T^{\mathbf{e}} && (3)\\
&= \sum_{\mathbf{e}\in\{0,\ldots,q-1\}^m} T^{\|\mathbf{e}\|_1} \cdot \sum_{\substack{\mathbf{d}\in D^m\\ \mathbf{e}\le_p\mathbf{d}}} f_{\mathbf{d}} \binom{\mathbf{d}}{\mathbf{e}} \mathbf{a}^{\mathbf{e}}\mathbf{b}^{\mathbf{d}-\mathbf{e}} && (4)\\
&= \sum_{d=0}^{q-1} T^d \cdot \sum_{\substack{\mathbf{e}\\ \|\mathbf{e}\|_1 \bmod^* q = d\\ \mathbf{d}\in D^m\\ \mathbf{e}\le_p\mathbf{d}}} f_{\mathbf{d}} \binom{\mathbf{d}}{\mathbf{e}} \mathbf{a}^{\mathbf{e}}\mathbf{b}^{\mathbf{d}-\mathbf{e}} && (5)\\
&=: \sum_{d=0}^{q-1} f_{d,\mathbf{b}}(\mathbf{a}) \cdot T^d. && (6)
\end{aligned}$$

Since $\mathcal{C}$ is linear affine-invariant, D is p-shadow closed, so $\mathbf{e} \in D^m$ if $\mathbf{d} \in D^m$ and $\mathbf{e} \le_p \mathbf{d}$. Therefore, each $f_{d,\mathbf{b}} \in \mathcal{C}^{\otimes m}$. By assumption, $f \notin \mathcal{C}^{\uparrow m}$, so there exist $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^m$ such that $g_{\mathbf{a},\mathbf{b}} \notin \mathcal{C}$, so there must be some $d \notin D$ such that $f_{d,\mathbf{b}} \neq 0$. Since $\delta(\mathcal{C}^{\otimes m}) = \delta^m$, for at least δ^m fraction of $\mathbf{a} \in \mathbb{F}_q^m$ we have $f_{d,\mathbf{b}}(\mathbf{a}) \neq 0$ and hence $g_{\mathbf{a},\mathbf{b}} \notin \mathcal{C}$. □

The following is the main technical theorem that will be prove in Section IV.

Definition III.2. For a set $D \subseteq \mathbb{F}_q^m$ of size $|D| \ge m-1$, define V_D^k to be the collection of k-dimensional affine subspaces in $\mathbb{F}_q^m$ spanned by elements in D, i.e. affine subspaces parametrized by $\mathbf{a}_0 + \mathbf{a}_1 T_1 + \cdots + \mathbf{a}_k T_k$ for $\mathbf{a}_0 \in \mathbb{F}_q^m$, $\mathbf{a}_1, \ldots, \mathbf{a}_k \in D$, and $T_1, \ldots, T_k$ take values in $\mathbb{F}_q$. For convenience, define $H_D := V_D^{m-1}$ and define $L_D := V_D^1$.

Definition III.3. Define $\mathcal{C}_D^m$ to be the code of all words $f : \mathbb{F}_q^m \to \mathbb{F}_q$ such that $f|_l \in \mathcal{C}$ for every line $l \in L_D$.

Remark III.4. Observe that $\mathcal{C}^{\uparrow m}$ is a subcode of $\mathcal{C}_D^m$ for every D. Indeed $\mathcal{C}^{\uparrow m} = \cap_{D\subseteq\mathbb{F}_q^m} \mathcal{C}_D^m = \cap_{a\in\mathbb{F}_q^m} \mathcal{C}_{\{a\}}^m$. Furthermore, if D contains the standard basis vectors, then $\mathcal{C}_D^m$ is a subcode of $\mathcal{C}^{\otimes m}$.

Our main technical contribution, captured by the following theorem, shows that $\mathcal{C}_D^m$ is robustly testable with robustness going to zero as $|D|$ grows.

Theorem III.5. *Let $D \subseteq \mathbb{F}_q^m$ be a set of size $|D| \ge m$ such that every m elements of D are linearly independent and let $r : \mathbb{F}_q^m \to \mathbb{F}_q$ be a word with $\rho := \mathbb{E}_{h\in H_D}[\delta(r|_h, \mathcal{C}^{\otimes m-1})]$. If $\rho < \frac{\delta^m}{4\binom{|D|}{m-1}^2}$, then $\delta(r, \mathcal{C}_D^m) \le \rho\binom{|D|}{m-1}$.*

Before we prove Theorem III.5, we show how it (almost immediately) implies the robustness of the $m-1$-dimensional test of the m-dimensional lifted code, where the robustness again decays with m.

Theorem III.6. *Let $m \ge 3$. Then the m-dimensional lift code $\mathcal{C}^{\uparrow m}$ is $\left(\min\left\{\frac{\delta^{2m}}{8\binom{m+1}{m-1}^2}, \frac{\delta^{3m}}{16m^3}\right\}, m-1\right)$-robust.*

Proof. We will assume that $q < 2m\delta^{-m}$, since if $q > 2m\delta^{-m}$ then by Corollary II.8 we are done. Let $r : \mathbb{F}_q^m \to \mathbb{F}_q$ to be some receiving word and let $\rho := \mathbb{E}_h\left[\delta(r|_h, \mathcal{C}^{\uparrow m-1})\right]$. We assume that $\rho < \frac{\delta^{2m}}{8\binom{m+1}{m-1}^2}$ (otherwise the result follows trivially).

$$\rho = \mathbb{E}_{\mathbf{a}_1,\ldots,\mathbf{a}_m}\mathbb{E}_{\mathbf{a}}\mathbb{E}_{h\in H_{\{\mathbf{a}_1,\ldots,\mathbf{a}_m,\mathbf{a}\}}}[\delta(r|_h, \mathcal{C}^{\uparrow m-1})]$$

where $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are random linearly independent directions in $\mathbb{F}_q^m$ and $\mathbf{a}$ is linearly independent of any $m-1$ of them. Fix $\mathbf{a}_1, \ldots, \mathbf{a}_m$ such that

$$\mathbb{E}_{\mathbf{a}}\mathbb{E}_{h\in H_{\{\mathbf{a}_1,\ldots,\mathbf{a}_m,\mathbf{a}\}}}[\delta(r|_h, \mathcal{C}^{\uparrow m-1})] \le \rho.$$

By affine-invariance, assume without loss of generality that $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are the standard basis vectors. Note that the last direction $\mathbf{a}$ is chosen uniformly at random from $(\mathbb{F}_q^*)^m$, the set of vectors with each coordinate nonzero. For $\mathbf{a} \in (\mathbb{F}_q^*)^m$, define $H_{\mathbf{a}} := H_{\{\mathbf{a}_1,\ldots,\mathbf{a}_m,\mathbf{a}\}}$ and $\mathcal{C}_{\mathbf{a}} := \mathcal{C}^m_{\{\mathbf{a}_1,\ldots,\mathbf{a}_m,\mathbf{a}\}}$. Since $\mathcal{C}^{\uparrow m-1} \subseteq \mathcal{C}^{\otimes m-1}$,

$$\mathbb{E}_{\mathbf{a}}\mathbb{E}_{h\in H_{\mathbf{a}}}[\delta(r|_h, \mathcal{C}^{\otimes m-1})] \le \rho.$$

By Markov's inequality,

$$\Pr_{\mathbf{a}}\left[\mathbb{E}_{h\in H_{\mathbf{a}}}[\delta(r|_h, \mathcal{C}^{\otimes m-1})] \ge \frac{\rho}{\frac{1}{2}\delta^m}\right] < \frac{1}{2}\delta^m.$$

In other words, there is a set $A \subseteq (\mathbb{F}_q^*)^m$ of size $|A| \ge (1-\frac{1}{2}\delta^m)\cdot(q-1)^m > (1-\frac{1}{2}\delta^m - \frac{m}{q})\cdot q^m$ such that, for each $\mathbf{a} \in A$, there is a codeword $c_{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$ such that $\rho_{\mathbf{a}} := \mathbb{E}_{h\in H_{\mathbf{a}}}[\delta(r|_h, \mathcal{C}^{\uparrow m-1})] < \frac{2\rho}{\delta^m} < \frac{\delta^m}{4\binom{m+1}{m-1}^2}$. By Theorem III.5, it follows that for each $\mathbf{a} \in A$ there is some codeword $c_{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$ with $\delta(r, c_{\mathbf{a}}) \le \rho_{\mathbf{a}}\binom{m+1}{m-1} < \frac{\delta^m}{2}$.

We proceed by showing that all of these codewords are the same codeword c, and moreover $c \in \mathcal{C}^{\uparrow m}$, which implies $\delta(r, \mathcal{C}^{\uparrow m}) \le \delta(r, c) \le \rho\delta^{-m}\binom{m+1}{m-1}$, as desired. Since $\mathbf{a}_1, \ldots, \mathbf{a}_m$ are the standard basis vectors, each $\mathcal{C}_{\mathbf{a}}$ is a subcode of $\mathcal{C}^{\otimes m}$. Thus, for any two $\mathbf{a}$, $\mathbf{a}' \in A$, the codewords $c_{\mathbf{a}}, c_{\mathbf{a}'} \in \mathcal{C}^{\otimes m}$ and satisfy $\delta(c_{\mathbf{a}}, c_{\mathbf{a}'}) \le \delta(c_{\mathbf{a}}, r) + \delta(r, c_{\mathbf{a}'}) < \delta^m = \delta(\mathcal{C}^{\otimes m})$, and therefore $c_{\mathbf{a}} = c_{\mathbf{a}'}$, i.e. all of these codewords are the same codeword $c \in \mathcal{C}^{\otimes m}$. Moreover, for each $\mathbf{a} \in A$, the codeword c restricted to any line in direction $\mathbf{a}$ is a codeword of $\mathcal{C}$, by definition of $\mathcal{C}_{\mathbf{a}}$. It follows from Proposition III.1 and the assumption that $q > \frac{1}{2}\delta^m$ that $c \in \mathcal{C}^{\uparrow m}$.

□

Corollary III.7. *The 4-dimensional lifted code $\mathcal{C}^{\uparrow 4}$ is $\left(\frac{\delta^{21}}{2\cdot 10^7}, 2\right)$-robust.*

Proof. By Theorem III.6, $\mathcal{C}^{\uparrow 4}$ is $\left(\frac{\delta^{12}}{1024}, 3t\right)$-robust and $\mathcal{C}^{\uparrow 3}$ is $\left(\frac{\delta^9}{432}, 2\right)$-robust. Therefore, by composing, the 2-dimensional robustness of $\mathcal{C}^{\uparrow 4}$ is at least $\frac{\delta^{12}}{1024}\cdot\frac{\delta^9}{432} = \frac{\delta^{21}}{15{,}786{,}368}$ □

IV. Robustness of special tensor code

In this section, we prove the main technical result (Theorem III.5) used in Section III.

Overview of the proof of Theorem theorem:special tensor main.: The analysis of Viderman [Vid12] forms the starting point of ours. We define a function $c : \mathbb{F}_q^m \to \mathbb{F}_q$, which we show is both close to r and a codeword of $\mathcal{C}_D^n$. Following Viderman's analysis, we partition $\mathbb{F}_q^m$ into "good", "fixable", and "bad" points. Each hyperplane $v \in \mathcal{T}_D$ has an associated codeword $c_v \in \mathcal{C}^{\otimes(m-1)}$, the nearest codeword to $r|_v$, and an opinion $c_v(\mathbf{x})$ about $\mathbf{x}$. "Good" points are points for which any hyperplane agrees with r. "Fixable" points are points for which hyperplanes agree with each other, but not with r. "Bad" points are points for which at least two hyperplanes disagree with each other. For good or fixable $\mathbf{x}$, we naturally

define $c(\mathbf{x})$ to be the common opinion $c_v(\mathbf{x})$ of any hyperplane v through $\mathbf{x}$. Claim IV.2 implies that there are not many bad points, which immediately shows that c is close to r.

So far, our proof has been a straightforward adaptation of Viderman's. However, at this point, we are forced to depart from Viderman's proof. A hyperplane is "bad" if it has more than $\frac{1}{2}\delta^{m-1}$ fraction bad points. Claim IV.1 shows that every bad point is in a bad hyperplane, and Claim IV.3 shows that there are less than $\frac{1}{2}\delta q$ bad hyperplanes. In [Vid12], which analyses $\mathcal{C}^{\otimes m}$ and axis-parallel hyperplanes instead of $\mathcal{C}_D^n$ and $\mathcal{T}_D$, this is already enough, since this implies that in each axis-parallel direction, there are less than δq bad hyperplanes, so the remaining points are all good or fixable and with a little bit more work, one can show that c can be extended uniquely to a tensor codeword using the erasure-decoding properties of tensor codes. Unfortunately, we do not have this structure and so we have to work some more.

We say a line is "good" if it is contained in some good hyperplane, otherwise it is bad. We must further partition the bad points into merely bad and "super-bad" points, which are points such that either every hyperplane is bad, or there are two disagreeing good hyperplanes. For merely bad $\mathbf{x}$, we define $c(\mathbf{x})$ to be the common opinion $c_v(\mathbf{x})$ of any good hyperplane v through $\mathbf{x}$. For super-bad $\mathbf{x}$, we pick any line u through $\mathbf{x}$, take the restriction of c to the non-super-bad points on u, and extend it to a codeword $c_u \in \mathcal{C}$, and define $c(\mathbf{x}) \triangleq c_u(\mathbf{x})$. Two non-trivial steps remain: showing that $c(\mathbf{x})$ is well-defined for super-bad $\mathbf{x}$, and showing that $c \in \mathcal{C}_D^n$.

Claim IV.4 shows that, for any special plane, there are less than $\frac{1}{2}\delta q$ lines in each direction that are bad (not contained in any good hyperplane) or contain a super-bad point. This is proved by exhibiting, for each such undesirable line, a bad hyperplane in a fixed direction containing the line. If there were too many undesirable lines, this would result in too many parallel bad hyperplanes, contradicting Claim IV.3. Finally Claim IV.5 shows if u is a line with no super-bad points, then $c|_u \in \mathcal{C}$ is a codeword.

Now, we show that c is well-defined on super-bad $\mathbf{x}$. Let u_1, u_2 be two lines through $\mathbf{x}$. Let P be the plane through $\mathbf{x}$ containing u_1, u_2. On this plane, by Claim IV.4, in each direction we have enough lines u with no super-bad points, for which $c|_u \in \mathcal{C}$ (by Claim IV.5), so that we can uniquely extend c onto the entire plane (by Proposition II.14). This gives a well-defined value for $c(\mathbf{x})$.

Finally, we show that $c \in \mathcal{C}_D^n$. Let u be any line. If u has no super-bad points, then $c|_u \in \mathcal{C}$ follows from Claim IV.5. If c does have a super-bad point $\mathbf{x}$, then $c|_u \in \mathcal{C}$ by the way we defined $c(\mathbf{x})$. This completes our analysis.

Proof of Theorem III.5. For each hyperplane $h \in \mathbb{F}_q^m$, define $c_h \in \mathcal{C}^{\otimes m-1}$ to be the closest codeword to $r|_h$ (break ties arbitrarily). We will partition $\mathbb{F}_q^m$ into three disjoint sets G, F, B (*good*, *fixable*, and *bad points*, respectively) as follows:

$$\begin{aligned} G &:= \left\{\mathbf{x} \in \mathbb{F}_q^m \mid c_h(\mathbf{x}) = r(\mathbf{x}) \text{ for every } h \in H_D\right\} \\ F &:= \left\{\mathbf{x} \in \mathbb{F}_q^m \mid c_h(\mathbf{x}) = c_{h'}(\mathbf{x}) \neq r(\mathbf{x}) \text{ for every } h, h' \in H_D\right\} \\ B &:= \left\{\mathbf{x} \in \mathbb{F}_q^m \mid c_h(\mathbf{x}) \neq c_{h'}(\mathbf{x}) \text{ for some } h, h' \in H_D\right\}. \end{aligned}$$

Call a hyperplane $h \in H_D$ *bad* if at least $\frac{1}{2}\delta^{m-1}$ fraction of its points are in B, and *good* otherwise. A line is *good* if it is contained in some good hyperplane $h \in H_D$, and *bad* otherwise. Further, define the set B' of *super-bad* points

$$B' := \{\mathbf{x} \in B \mid \forall h \in H_D \text{ through } \mathbf{x} \text{ is bad or } \exists h, h' \in H_D \text{ through } \mathbf{x} \text{ such that } c_h(\mathbf{x}) \neq c_{h'}(\mathbf{x})\}.$$

Claim IV.1. *If $h, h' \in H_D$ are good hyperplanes that differ in only one direction, then $c_h|_{h\cap h'} = c_{h'}|_{h\cap h'}$. In particular, every bad point is in a bad hyperplane.*

Proof. Suppose $\mathbf{b} \in h \cap h'$ and $c_h(\mathbf{b}) \neq c_{h'}(\mathbf{b})$. Let h have directions $\mathbf{a}_1, \ldots, \mathbf{a}_{m-2}, \mathbf{a}$ and let h' have directions $\mathbf{a}_1, \ldots, \mathbf{a}_{m-2}, \mathbf{a}'$. Let l be the line through $\mathbf{b}$ in direction $\mathbf{a}_1$. Since $c_h|_l, c_{h'}|_l \in \mathcal{C}$ disagree on $\mathbf{b}$, they are distinct codewords and hence disagree on at least δq points, say $\mathbf{x}_1, \ldots, \mathbf{x}_{\delta q}$. For each $i \in [\delta q]$, let $h_i \in H_D$ be the hyperplane through $\mathbf{x}_i$ in directions $\mathbf{a}_2, \ldots, \mathbf{a}_{m-2}, \mathbf{a}, \mathbf{a}'$. Since $c_h(\mathbf{x}_i) \neq c_{h'}(\mathbf{x}_i)$, that means c_{h_i} disagrees with one of $c_h, c_{h'}$ at $\mathbf{x}_i$. Without loss of generality, suppose c_h disagrees with $c_{h_1}, \ldots, c_{h_{\delta q/2}}$. We will show that h is bad, which proves the first part of the claim.

For each $i \in [\delta q]$, let $v_i = h_i \cap h$, which is the subspace of dimension $m-2$ through $\mathbf{x}_i$ spanned by directions $\mathbf{a}_2, \ldots, \mathbf{a}_{m-2}, \mathbf{a}$. Since $v_i \in V_D^{m-2}$, the restrictions $c_h|_{v_i}, c_{h_i}|_{v_i} \in \mathcal{C}^{\otimes m-2}$ are codewords and are distinct because they disagree on $\mathbf{x}_i$, therefore they disagree on at least $\delta^{m-2}q^{m-2}$ points in v_i, which are therefore bad. Thus, each h_i contributes $\delta^{m-2}q^{m-2}$ bad points to h, for a total of $\frac{1}{2}\delta^{m-1}q^{m-1}$ bad points.

For the second part, suppose $\mathbf{b} \in B$ is a bad point. We will show that $\mathbf{b}$ lies in a bad hyperplane. By definition, there are two hyperplanes $h, h' \in H_D$ such that $c_h(\mathbf{b}) \neq c_{h'}(\mathbf{b})$. Suppose h has directions $\mathbf{a}_1, \ldots, \mathbf{a}_{m-1}$ and h' has directions $\mathbf{a}'_1, \ldots, \mathbf{a}'_{m-1}$. Define $h_0 := h$, and for $i \in [m-1]$, define $h_i \in H_D$ to be the hyperplane through $\mathbf{b}$ in directions $\mathbf{a}'_1, \ldots, \mathbf{a}'_i, \mathbf{a}_{i+1}, \ldots, \mathbf{a}_{m-1}$. Consider the sequence $h_0, h_1, \ldots, h_{m-1}$ of hyperplanes. For each i, the hyperplanes h_i, h_{i+1} differ in at most one direction. Since $c_{h_0}(\mathbf{b}) \neq c_{h_{m-1}}(\mathbf{b})$, there exists some i such that $c_{h_i}(\mathbf{b}) \neq c_{h_{i+1}}(\mathbf{b})$, and by the first part of the claim it follows that one of h_i, h_{i+1} is bad. □

Claim IV.2. $\rho \geq \frac{|F|}{q^m} + \frac{|B|}{q^m \binom{|D|}{m-1}}$

Claim IV.3. *There are less than $\frac{1}{2}\delta^{m-1}q$ bad hyperplanes.*

Proof. By Claim IV.2, there are at most $|B| \leq \rho\binom{|D|}{m-1}q^m$ bad points. Each bad hyperplane has at least $\delta^{m-1}q^{m-1}/2$ bad points by definition. Each bad point has at most $\binom{|D|}{m-1}$ bad hyperplanes through it. Therefore, there are at most

$$\frac{|B|}{\delta^{m-1}q^{m-1}/2} \cdot \binom{|D|}{m-1} \leq \frac{2\rho}{\delta^{m-1}}\binom{|D|}{m-1}^2 q < \frac{1}{2}\delta q$$

bad hyperplanes. □

Now we proceed to prove the lemma. We construct a codeword $c \in \mathcal{C}_D^m$ with $\delta(r, c) \leq \rho\binom{|D|}{m-1}$ in stages, as follows. First, for $\mathbf{x} \in G \cup F$, we define $c(\mathbf{x}) := c_h(\mathbf{x})$ for any hyperplane $h \in H_D$ through $\mathbf{x}$. This is well-defined since, by definition of G and F, all hyperplanes $h \in H_D$ agree on the value $c_h(\mathbf{x})$. Furthermore, since $c(\mathbf{x}) = c_h(\mathbf{x}) = r(\mathbf{x})$ for $\mathbf{x} \in G$, we already guarantee that $\delta(r, c) \leq \frac{|F|+|B|}{q^m} \leq \rho\binom{|D|}{m-1}$.

For $\mathbf{x} \in B \setminus B'$, define $c(\mathbf{x}) := c_h(\mathbf{x})$ for any good hyperplane $h \in H_D$ through $\mathbf{x}$, whose existence is guaranteed by the fact that $x \notin B'$. This is well-defined because if $h, h' \in H_D$ are both good hyperplanes through $\mathbf{x}$, then it follows from the fact that $\mathbf{x} \notin B'$ that $c_h(\mathbf{x}) = c_{h'}(\mathbf{x})$.

Claim IV.4. *Let P be a plane in directions $\mathbf{a}_1, \mathbf{a}_2 \in D$. For each $i \in \{1, 2\}$, there are less than $\frac{1}{2}\delta q$ lines in P in direction $\mathbf{a}_i$ which intersect B' or are bad.*

Proof. By symmetry, it suffices to consider $i = 1$. Let $\mathbf{a}_3, \ldots, \mathbf{a}_m \in D$ be some other directions, so that $\mathbf{a}_1, \ldots, \mathbf{a}_m$ form a basis for $\mathbb{F}_q^m$. Let $l_1, \ldots, l_k$ be lines P in direction $\mathbf{a}_1$ such that, for each $j \in [k]$, l_j intersects B' or is bad. It suffices to exhibit, for each $j \in [k]$, a bad hyperplane $h_j \in H_D$ containing l_j which has direction $\mathbf{a}_1$ but not $\mathbf{a}_2$, for then $h_1, \ldots, h_k$ would be distinct bad hyperplanes, and by Claim IV.3, $k < \frac{1}{2}\delta q$.

Fix $j \in [k]$ and $l := l_j$. If l is bad, then we are done, since any hyperplane containing l, in particular the hyperplane in directions $\mathbf{a}_1, \mathbf{a}_3, \ldots, \mathbf{a}_m$, is bad. Now suppose l has a point $\mathbf{x} \in l \cap B'$. Let $h \in H_D$ be the hyperplane through $\mathbf{x}$ in directions $\mathbf{a}_1, \mathbf{a}_3, \ldots, \mathbf{a}_m$. If h is bad, we are done. Otherwise, since $\mathbf{x} \in B'$, there exists another good hyperplane $h' \in D$, in directions $\mathbf{a}'_1, \mathbf{a}'_3, \ldots, \mathbf{a}'_m$, such that $c_h(\mathbf{x}) \neq c_{h'}(\mathbf{x})$. Without loss of generality, suppose $\mathbf{a}_2 \notin \{\mathbf{a}'_3, \ldots, \mathbf{a}'_m\}$. For each $i \in \{0, \ldots, m-2\}$, define $h_i \in H_D$ to be the hyperplane through $\mathbf{x}$ in directions $\mathbf{a}_1, \mathbf{a}_3, \ldots, \mathbf{a}_{m-i}, \mathbf{a}'_{m-i+1}, \ldots, \mathbf{a}'_m$, and define $h_{m-1} := h'$. For every i, h_i and h_{i+1} differ in at most one direction. Note that for every $i \in \{0, 1, \ldots, m-2\}$, h_i contains the direction $\mathbf{a}_1$ and does not contain the direction $\mathbf{a}_2$. We will show that h_i is bad for some $i \leq m-2$. Since $c_{h_0}(\mathbf{x}) \neq c_{h_{m-1}}(\mathbf{x})$, there exists some $i \leq m-2$ such that $c_{h_i}(\mathbf{x}) \neq c_{h_{i+1}}(\mathbf{x})$, and therefore, by Claim IV.1, one of h_i, h_{i+1} is bad. If $i < m-2$, then $i, i+1 \leq m-2$, and so we are done. If $i = m-2$, then by assumption h' is good, so it must be that h_{m-2} is bad. □

Claim IV.5. *If $l \cap B' = \emptyset$, then for every $\mathbf{x} \in l$ there is a codeword $c_{\mathbf{x}} \in \mathcal{C}$ such that $c_{\mathbf{x}}(\mathbf{x}) = c(\mathbf{x})$ and $\delta(c_{\mathbf{x}}, c|_l) < \frac{\delta}{2}$.*

Proof. Let $\mathbf{a}_1$ be the direction of l. Let h be a good hyperplane through $\mathbf{x}$ and let $\mathbf{a}_2$ be a direction in h, and let $\mathbf{a}_3, \ldots, \mathbf{a}_m \in D$ so that $\mathbf{a}_1, \ldots, \mathbf{a}_m$ is a basis of $\mathbb{F}_q^m$. Consider the plane P through $\mathbf{x}$ in directions $\mathbf{a}_1, \mathbf{a}_2$. By Claim IV.4, in each direction $\mathbf{a}_i$, there are at least $(1 - \frac{\delta}{2})q$ good lines in P in direction $\mathbf{a}_i$. Therefore, c restricted to any of these good lines is a codeword of $\mathcal{C}$, and hence we can extend the restriction of c to these good lines in P to a codeword $c_P \in \mathcal{C}^{\otimes 2}$ on P. Define $c_{\mathbf{x}} := c_P|_l$. Then $c_{\mathbf{x}}(\mathbf{x}) = c(\mathbf{x})$ since the line l' through $\mathbf{x}$ in direction $\mathbf{a}_2$ is a good line (as it lies in h) and so $c_P|_{l'} = c|_{l'}$. Extending this reasoning to the $(1 - \frac{\delta}{2})q$ good lines in P intersecting l, we also see that $\delta(c_{\mathbf{x}}, c|_l) < \frac{\delta}{2}$. □

Claim IV.6. *If l is a line and $l \cap B' = \emptyset$, then $c|_l \in \mathcal{C}$.*

Proof. Fix some $\mathbf{x}_0 \in l$. For each $\mathbf{x} \in l$, let $c_{\mathbf{x}}$ be the codeword guaranteed by Claim IV.5. Then, for every $\mathbf{x} \in l$, $\delta(c_{\mathbf{x}_0}, c_{\mathbf{x}}) \leq \delta(c_{\mathbf{x}_0}, c|_l) + \delta(c|_l, c_{\mathbf{x}}) < \delta$, therefore $c_{\mathbf{x}_0} = c_{\mathbf{x}}$. Moreover, $c_{\mathbf{x}_0}(\mathbf{x}) = c_{\mathbf{x}}(\mathbf{x}) = c(\mathbf{x})$, so $c|_l = c_{\mathbf{x}_0} \in \mathcal{C}$. □

We proceed to define $c(\mathbf{x})$ for $x \in B'$. For such an $\mathbf{x}$, pick any line $l \in L_D$ through $\mathbf{x}$, extend $c|_{l \setminus B'}$ to a codeword $c_l \in \mathcal{C}$, and define $c(\mathbf{x}) := c_l(\mathbf{x})$. The argument that this is well-defined is different from the previous argument. Suppose $l_1, l_2 \in L_D$ are two lines through $\mathbf{x}$, in directions $\mathbf{a}_1, \mathbf{a}_2 \in D$, respectively. Let P be the unique plane containing l_1, l_2. By Claim IV.4, in each direction $\mathbf{a}_1, \mathbf{a}_2$, there are less than $\delta \cdot q$ lines in that direction in P which intersects B'. In particular, this implies that l_1, l_2 each contain less than $\delta \cdot q$ points from B'. The plane P can be parametrized by $\mathbf{x} + \mathbf{a}_1 T_1 + \mathbf{a}_2 T_2$. By what we just showed, there are sets $S_1, S_2 \subseteq \mathbb{F}_q$ of size $|S_1|, |S_2| > (1-\delta) \cdot q$ such that the sub-rectangle $R := \{\mathbf{x} + \mathbf{a}_1 t_1 + \mathbf{a}_2 t_2 \mid t_1 \in S_1, t_2 \in S_2\}$ contains no points from B', and therefore c has already been defined on R. By Claim IV.6, on each line l in R in either direction $\mathbf{a}_1$ or $\mathbf{a}_2$, $c|_l \in \mathcal{C}$. Applying the erasure-decoding properties of tensor codes, we see that $c|_R$ can be uniquely extended to a tensor codeword $c_P \in \mathcal{C}^{\otimes 2}$ on P, and this gives a way to extend $c|_{l_i \setminus B'}$ to the codeword $c_{l_i} = c_P|_{l_i} \in \mathcal{C}$ for $i \in \{1, 2\}$. Therefore, the extensions $c_{l_1}, c|_{l_2}$ agree on $\mathbf{x}$ since $c_{l_1}(\mathbf{x}) = c_P(\mathbf{x}) = c_{l_2}(\mathbf{x})$, and moreover for each line l_i this extension is unique since each line has less than $\delta \cdot q$ points from B'.

Now that we have defined $c : \mathbb{F}_q^m \to \mathbb{F}_q$ and have shown that $\delta(r, c) \leq \rho\binom{|D|}{m-1}$, it only remains to show that $c \in \mathcal{C}_D^m$. Let $l \in L_D$. If l is good, then we are done, since l is contained in some good hyperplane $h \in H_D$, so $c(\mathbf{x}) = c_h(\mathbf{x})$ for every $\mathbf{x} \in l$, and hence $c|_l = c_h|_l \in \mathcal{C}$. If $l \cap B' = \emptyset$, then $c|_l \in \mathcal{C}$ follows from Claim IV.6.

Finally, the remaining case is when l is bad and intersects B'. In this case, by the way we defined $c(\mathbf{x})$ for $\mathbf{x} \in B'$, we showed that for any line l through $\mathbf{x} \in B'$, $c|_l \in \mathcal{C}$ by extending $c|_{l \setminus B'}$ to a codeword.

□

V. Robustness for large dimension

In this section, we prove our main result:

Theorem V.1. *Let $\rho \triangleq \mathbb{E}_p[\delta(r|_p, \mathcal{C}^{\uparrow 2})]$, where p is a random plane (affine subspace of dimension 2). Let α be the 2-dimensional robustness of $\mathcal{C}^{\uparrow 4}$ given by Corollary III.7. If $\rho < \frac{\alpha\delta^3}{400} - 3q^{-1}$, then $\rho \geq \left(1 - \frac{\delta}{4}\right) \cdot \delta(r, \mathcal{C}^{\uparrow m})$. In particular, $\mathcal{C}^{\uparrow m}$ is $(\alpha', 2)$-robust, where $\alpha' \geq \frac{\delta^{72}}{2 \cdot 10^{31}}$.*

Notation: Throughout Section V, fix the received word $r : \mathbb{F}_q^m \to \mathbb{F}_q$ and $\rho \triangleq \mathbb{E}_p[\delta(r|_p, \mathcal{C}^{\uparrow 2})]$, and we will assume that $0 < \rho < \frac{\alpha_1\delta^3}{400} - 3q^{-1}$. The case where $\frac{\alpha_1\delta^3}{400} > 3q^{-1}$ is easily dealt with at the end of the proof by using Corollary II.8. Note that, since $\alpha, \delta \leq 1$, this implies $q^{-1} \leq \frac{\delta}{1200}$. Throughout this section we will assume $m \geq 4$. If $m < 4$ we can pad the function f to get a function $\hat{f} : \mathbb{F}_q^4 \to \mathbb{F}_q$ (by setting $\hat{f}(\mathbf{x}, \mathbf{y}) = f(\mathbf{x})$ for every $\mathbf{x} \in \mathbb{F}_q^m$ and $\mathbf{y} \in \mathbb{F}_q^{4-m}$) and applying our tester to $\hat{f}$. We will typically use l, p, w to denote affine lines, planes and 4 dimensional subspaces respectively. For any affine subspace $A \subseteq \mathbb{F}_q^m$, let $c_A \in \mathcal{C}^{\uparrow \dim(A)}$ be the codeword nearest to $r|_A$, breaking ties arbitrarily. Let $\rho_A \triangleq \mathbb{E}_{p \subseteq A}[\delta(r|_p, \mathcal{C}^{\uparrow 2})]$, where the expectation is taken over uniformly random plane $p \subseteq A$. Fix the following constants:

$$\begin{aligned} \gamma &\triangleq \frac{\alpha\delta^2}{40} - \alpha q^{-1} \\ \epsilon &\triangleq \frac{\rho + 2q^{-1}}{\gamma}. \end{aligned}$$

In particular, these constants are chosen so that the following bounds hold:

$$\begin{aligned} 20\delta^{-1}(\alpha^{-1}\gamma + q^{-1}) &\leq \frac{\delta}{2} \\ \epsilon &\leq \frac{\delta}{10}. \end{aligned}$$

Overview: This proof is a straightforward generalization of "bootstrapping" proofs originating in the work of Rubinfeld and Sudan [RS96] and which also appears in [ALM+98], [AS03], [Aro94]. Our writeup in particular follows [Aro94]. Our approach is to define a function $c : \mathbb{F}_q^m \to \mathbb{F}_q$ and then show that it is both close to r and a codeword of $\mathcal{C}^{\uparrow m}$. The definition of c is simple: for every $\mathbf{x} \in \mathbb{F}_q^m$, consider the opinion $c_l(\mathbf{x})$ for every line l through $\mathbf{x}$, and define $c(\mathbf{x})$ as the majority opinion. We need to show that c is well-defined (the majority is actually a majority). Our main technical lemma (Lemma V.4) of this section shows that most lines agree with each other, so c is well-defined. Lemma V.4 uses Claim V.2, which shows that for a 4-dimensional affine subspace w, if ρ_w is small, then for every $\mathbf{x} \in w$, most lines $l \subseteq w$ satisfy $c_l(\mathbf{x}) = c_w(\mathbf{x})$. To prove Claim V.2 we use the results of Section III, in particular the robustness of the plane test in $m = 4$ dimensions (Corollary III.7). Since the average $\delta(r|_l, c_w|_l)$ over l through $\mathbf{x}$ is about $\delta(r|_w, c_w)$, by robustness this is less than $\alpha_1^{-1}\rho_w$, which is small since ρ_w is small. Therefore, for most l, $\delta(r|_l, c_w|_l)$ is small and so it must be that $c_l = c_w|_l$.

Once we have shown that c is well-defined, showing that c is close to r requires just a bit of calculation. Showing that $c \in \mathcal{C}^{\uparrow m}$ involves more work. For each line l, define $c'_l \in \mathcal{C}$ to be the nearest codeword to $c|_l$. Fix a line l and a point $\mathbf{x} \in l$. We want to show that $c|_l(\mathbf{x}) = c'_l(\mathbf{x})$. The idea is to show the existence of a "good" 4-dimensional $w \supseteq l$ such that ρ_w is small and for more than $1 - \frac{\delta}{2}$ fraction of points $\mathbf{y} \in l$ (including $\mathbf{x}$) are "good" in the sense that $c(\mathbf{y}) = c_{l'}(\mathbf{y})$ for a non-negligible fraction of lines l' through $\mathbf{y}$. Once we have such a w, we show that for every good $\mathbf{y} \in l$, $c(\mathbf{y}) = c_w(\mathbf{y})$. Since l has more than

$1 - \frac{\delta}{2}$ fraction good points, this implies that $\delta(c|_l, c_w|_l) < \frac{\delta}{2}$, hence $c'_l = c|_l$, so $c'_l(\mathbf{x}) = c|_w(\mathbf{x}) = c(\mathbf{x})$, as desired.

Claim V.2. *If $w \subseteq \mathbb{F}_q^m$ be a 4-dimensional affine subspace with $\rho_w \leq \gamma$, then for every $\mathbf{x} \in w$, at least $1 - \frac{\delta}{20}$ fraction of lines $l \subseteq w$ satisfy $c_l(\mathbf{x}) = c_w(\mathbf{x})$.*

Proof. Fix $\mathbf{x} \in w$. Let U be the set of lines l containing $\mathbf{x}$ such that $\delta(r|_l, c_w|_l) < 20\delta^{-1}(\alpha^{-1}\rho_w + q^{-1})$. By Corollary III.7, $\mathbb{E}_{\substack{l \subseteq w \\ l \ni \mathbf{x}}}[\delta(r|_l, c_w|_l)] \leq \delta(r|_w, c_w) + q^{-1} \leq \alpha^{-1}\rho_w + q^{-1}$, so by Markov's inequality, the probability that $\delta(r|_l, c_w|_l) \geq 20\delta^{-1}(\alpha^{-1}\rho_w + q^{-1})$ is at most $\frac{\alpha^{-1}\rho_w + q^{-1}}{20\delta^{-1}(\alpha_1^{-1}\rho_w + q^{-1})} = \frac{\delta}{20}$. For $l \in U$, since $\delta(r|_l, c_w|_l) < 20\delta^{-1}(\alpha^{-1}\rho_w + q^{-1}) \leq \frac{\delta}{2}$ and $c_w|_l \in \mathcal{C}$, we have $c_l = c_w|_l$ and therefore $c_l(\mathbf{x}) = c_w(\mathbf{x})$. □

The following claim says that $\mathbb{E}_w[\rho_w] \approx \rho$, even if we insist that w contains a fixed t-dimensional subspace.

Claim V.3. *For any line $l \subseteq \mathbb{F}_q^m$, $\mathbb{E}_{w \supseteq l}[\rho_w] \leq \rho + 2q^{-1}$, where w is a random 4-dimensional affine subspace containing l. In particular, for any point $\mathbf{x} \in \mathbb{F}_q^m$, $\mathbb{E}_{w \ni \mathbf{x}}[\rho_w] \leq \rho + 2q^{-1}$.*

Proof. Observe that

$$\begin{aligned}
\rho &= \mathbb{E}_p\left[\delta\left(r|_p, \mathcal{C}^{\uparrow 2}\right)\right] \\
&\geq \mathbb{E}_{p: l \cap p = \emptyset}\left[\delta\left(r|_p, \mathcal{C}^{\uparrow 2}\right)\right] \cdot \Pr_p[l \cap p = \emptyset] \\
\text{(Lemma II.15)} \quad &\geq \mathbb{E}_{p: l \cap p = \emptyset}\left[\delta\left(r|_p, \mathcal{C}^{\uparrow 2}\right)\right] \cdot \left(1 - q^{-(m-3)}\right).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathbb{E}_{w \supseteq l}[\rho_w] &= \mathbb{E}_{w \supseteq l}\left[\mathbb{E}_{p \subseteq w}\left[\delta(r|_p, \mathcal{C}^{\uparrow 2})\right]\right] \\
&\leq \mathbb{E}_{w \supseteq l}\left[\mathbb{E}_{p \subseteq w}\left[\delta(r|_p, \mathcal{C}^{\uparrow 2}) \;\middle|\; l \cap p = \emptyset\right] + \Pr_{p \subseteq w}[l \cap p \neq \emptyset]\right] \\
\text{(Lemma II.15)} \quad &\leq \mathbb{E}_{w \supseteq l}\left[\mathbb{E}_{p \subseteq w}\left[\delta(r|_p, \mathcal{C}^{\uparrow 2}) \;\middle|\; l \cap p = \emptyset\right]\right] + q^{-1} \\
&= \mathbb{E}_{v: l \cap p = \emptyset}[\delta(r|_p, \mathcal{C}^{\uparrow 2})] + q^{-1} \\
&\leq \frac{\rho}{1 - q^{-(m-3)}} + q^{-1} \\
&\leq \rho + 2q^{-1}
\end{aligned}$$

□

Lemma V.4 (Main)**.** *For every $\mathbf{x} \in \mathbb{F}_q^m$, there is a collection U_1 of at least $1 - \frac{\delta}{5} - \frac{\delta}{600}$ fraction of the lines through $\mathbf{x}$, such that $c_l(\mathbf{x}) = c_{l'}(\mathbf{x})$ for every $l, l' \in U_1$.*

Proof. Let U be the set of all lines l through $\mathbf{x}$. Partition U into disjoint collections $U_1, \ldots, U_k$ with $|U_1| \geq \cdots \geq |U_k|$ according to the value of $c_l(\mathbf{x})$. We will show that $\Pr_{l \ni x}[l \in U_1] \geq 1 - \frac{\delta}{5} - \frac{\delta}{600}$. For every 4-dimensional subspace w, let U_w be the collection of lines l through $\mathbf{x}$, guaranteed by Claim V.2, satisfying $c_l(\mathbf{x}) = c_w(\mathbf{x})$. Then

$$\begin{aligned}
\Pr_{l \ni \mathbf{x}}[l \in U_1] &\geq \Pr_{l, l' \ni \mathbf{x}}[\exists i \;\; l, l' \in U_i] \\
&= \Pr_{l, l' \ni \mathbf{x}}[c_l(\mathbf{x}) = c_{l'}(\mathbf{x})]
\end{aligned}$$

$$
\begin{aligned}
&\geq \Pr_{l \neq l' \ni \{\mathbf{x}\}}[c_l(\mathbf{x}) = c_{l'}(\mathbf{x})] - q^{-(m-1)} \\
&= \mathbb{E}_{w \ni \mathbf{x}} \left[\Pr_{\substack{l,l' \subseteq w \\ l \neq l' \ni \{\mathbf{x}\}}} [c_l(\mathbf{x}) = c_{l'}(\mathbf{x})] \right] - q^{-(m-1)} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}} \left[\Pr_{\substack{l,l' \subseteq w \\ l,l' \ni \mathbf{x}}} [c_l(\mathbf{x}) = c_{l'}(\mathbf{x}) \right] - q^{-3} - q^{-(m-1)} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}} \left[\Pr_{\substack{l,l' \subseteq w \\ l,l' \ni \mathbf{x}}} [c_l(\mathbf{x}) = c_{l'}(\mathbf{x}) \right] - \frac{\delta}{600} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}} \left[\Pr_{\substack{l,l' \subseteq w \\ l,l' \ni \mathbf{x}}} [c_l(\mathbf{x}) = c_{l'}(\mathbf{x})] \;\middle|\; \rho_w \leq \gamma \right] \cdot \Pr_{w \ni \mathbf{x}} [\rho_w \leq \gamma] - \frac{\delta}{600} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}} \left[\Pr_{\substack{l,l' \subseteq w \\ l,l' \ni \mathbf{x}}} [l, l' \in U_w] \;\middle|\; \rho_w \leq \gamma \right] \cdot \Pr_{w \ni \mathbf{x}} [\rho_w \leq \gamma] - \frac{\delta}{600} \\
\text{(Claim V.2)} \quad &\geq \left(1 - \frac{\delta}{20}\right)^2 \cdot \Pr_{w \ni \mathbf{x}} [\rho_w \leq \gamma] - \frac{\delta}{600} \\
\text{(Markov)} \quad &\geq \left(1 - \frac{\delta}{20}\right)^2 \cdot \left(1 - \frac{\mathbb{E}_{w \ni \mathbf{x}}[\rho_w]}{\gamma}\right) - \frac{\delta}{600} \\
\text{(Claim V.3)} \quad &\geq \left(1 - \frac{\delta}{20}\right)^2 \cdot \left(1 - \frac{\rho + 2q^{-1}}{\gamma}\right) - \frac{\delta}{600} \geq 1 - \frac{\delta}{10} - \frac{\rho + 2q^{-1}}{\gamma} - \frac{\delta}{600} \\
&= 1 - \frac{\delta}{10} - \epsilon - \frac{\delta}{600} \geq 1 - \frac{\delta}{5} - \frac{\delta}{600}
\end{aligned}
$$

□

We are now ready to prove the main theorem.

Proof of Theorem V.1. We will define a function $c : \mathbb{F}_q^m \to \mathbb{F}_q$ and then show that it is close to r and is a codeword of $\mathcal{C}^{\uparrow m}$. For $\mathbf{x} \in \mathbb{F}_q^m$, define $c(\mathbf{x}) \triangleq \text{Majority}_{l \ni \mathbf{x}}\{c_l(\mathbf{x})\}$, where the majority is over lines l through $\mathbf{x}$. Since $\frac{\delta}{5} + \frac{\delta}{600} < \frac{1}{2}$, it follows from Lemma V.4 that c is well-defined.

Next, we show that c is close to r. Indeed,

$$
\begin{aligned}
\rho &= \mathbb{E}_p[\delta(r|_p, c_p)] \\
&\geq \mathbb{E}_l[\delta(r|_l, c_l)] \\
&= \mathbb{E}_l \left[\mathbb{E}_{\mathbf{x} \in l} \left[\mathbb{1}_{c_l(\mathbf{x}) \neq r(\mathbf{x})} \right] \right] \\
&= \mathbb{E}_{\mathbf{x}} \left[\mathbb{E}_{l \ni \mathbf{x}} \left[\mathbb{1}_{c_l(\mathbf{x}) \neq r(\mathbf{x})} \right] \right] \\
&\geq \mathbb{E}_{\mathbf{x}} \left[\mathbb{E}_{l \ni \mathbf{x}} \left[\mathbb{1}_{c_l(\mathbf{x}) \neq r(\mathbf{x})} \right] \;\middle|\; c(\mathbf{x}) \neq r(\mathbf{x}) \right] \cdot \Pr_{\mathbf{x}}[c(\mathbf{x}) \neq r(\mathbf{x})] \\
&\geq \mathbb{E}_{\mathbf{x}} \left[\Pr_{l \ni \mathbf{x}}[c_l(\mathbf{x}) = c(\mathbf{x})] \;\middle|\; c(\mathbf{x}) \neq r(\mathbf{x}) \right] \cdot \delta(r, c) \\
\text{(Lemma V.4)} \quad &\geq \left(1 - \frac{\delta}{4}\right) \cdot \delta(r, c).
\end{aligned}
$$

Finally, we show that $c \in \mathcal{C}^{\uparrow m}$. Let $l \subseteq \mathbb{F}_q^m$ a line. We wish to show that $c|_l \in \mathcal{C}$. Let $c'_l \in \mathcal{C}$ be the codeword of $\mathcal{C}$ nearest to $c|_l$ (not to be confused with c_l, the nearest codeword to $r|_l$). Let $\mathbf{x} \in l$. We will show that $c'_l(\mathbf{x}) = c|_l(\mathbf{x})$. For a 4-dimensional affine subspace $w \subseteq \mathbb{F}_q^m$, we say a point $\mathbf{y} \in w$ is *good for* w if $\Pr_{\substack{l' \subseteq w \\ l' \ni \mathbf{y}}}[c_{l'}(\mathbf{y}) = c(\mathbf{y})] > \frac{\delta}{20}$. We will show, by a union bound, that there exists a 4-dimensional affine subspace $w \supseteq l$ such that

1) $\rho_w \leq \gamma$;
2) $\mathbf{x}$ is good for w;
3) more than $1 - \frac{\delta}{2}$ fraction of points $\mathbf{y} \in l$ are good for w.

Observe that for any $\mathbf{y} \in l$, picking a random 4-dimensional w containing l and then picking a random line $l' \subseteq w$ through $\mathbf{y}$ that intersect l only on y is equivalent to picking a random line l' through $\mathbf{y}$ that intersect l only on y and then picking a random 4-dimensional w containing both l, l'. Therefore, for any fixed $\mathbf{y} \in l$

$$\begin{aligned}
\mathbb{E}_{w \supseteq l}\left[\Pr_{\substack{l' \subseteq w \\ l' \ni \mathbf{y}}}[c_{l'}(\mathbf{y}) \neq c(\mathbf{y})]\right] &= \mathbb{E}_{\substack{w \supseteq l \\ l' \subseteq w, l' \ni \mathbf{y}}}\left[\mathbb{1}_{c_{l'}(\mathbf{y}) \neq c(\mathbf{y})}\right] \\
&\leq \mathbb{E}_{\substack{w \supseteq l \\ l' \subseteq w, l' \ni \mathbf{y}}}\left[\mathbb{1}_{c_{l'}(\mathbf{y}) \neq c(\mathbf{y})} \mid l \cap l' = \{\mathbf{y}\}\right] + \Pr_{\substack{w \supseteq l \\ l' \subseteq w, l' \ni \mathbf{y}}}\left[l \cap l' \neq \{\mathbf{y}\}\right] \\
\text{(Lemma II.16)} \quad &\leq \mathbb{E}_{l' \ni \mathbf{y}}\left[\mathbb{1}_{c_{l'}(\mathbf{y}) \neq c(\mathbf{y})} \mid l \cap l' = \{y\}\right] + q^{-2} \\
\text{(Lemma II.16)} \quad &\leq \mathbb{E}_{l' \ni \mathbf{y}}\left[\mathbb{1}_{c_{l'}(\mathbf{y}) \neq c(\mathbf{y})}\right] + q^{-(m-2)} + q^{-2} \\
\text{(Lemma V.4 and definition of } c) \quad &\leq \frac{\delta}{5} + \frac{\delta}{600} + 2q^{-2} \leq \frac{\delta}{5} + \frac{\delta}{300} \leq \frac{\delta}{4}.
\end{aligned}$$

Therefore, by Markov's inequality, for any fixed $\mathbf{y} \in l$,

$$\begin{aligned}
\Pr_{w \supseteq l}[\mathbf{y} \text{ is not good for } w] &= \Pr_{w \supseteq l}\left[\Pr_{l' \supseteq w, l' \ni \mathbf{y}}[c_{l'}(\mathbf{y}) \neq c(\mathbf{y})] \geq 1 - \frac{\delta}{20}\right] \\
&\leq \frac{\frac{\delta}{4}}{1 - \frac{\delta}{20}} \\
&\leq \frac{5}{19} \cdot \delta.
\end{aligned}$$

In particular, this applies for $\mathbf{y} = \mathbf{x}$. Further applying Markov's inequality, we find that

$$\Pr_{w \supseteq l}\left[\text{fraction of not good } \mathbf{y} \text{ in } l \geq \frac{\delta}{2}\right] \leq \frac{5\delta/19}{\delta/2} = \frac{10}{19}.$$

Finally, since $\mathbb{E}_{w \supseteq l}[\rho_w] \leq \rho + 2q^{-1}$ (by Claim V.3), we have

$$\Pr_{w \supseteq l}[\rho_w > \gamma] \leq \frac{\rho + 2q^{-1}}{\gamma} = \epsilon \leq \frac{\delta}{10}.$$

Since $\delta \leq 1$ and $\frac{5}{19} + \frac{10}{19} + \frac{1}{10} < 1$, by the union bound such a desired w exists.

Now that we have such a subspace w, consider c_w. We claim that it suffices to prove that if $\mathbf{y} \in l$ is good, then $c_w(\mathbf{y}) = c(\mathbf{y})$. Indeed, since more than $1 - \frac{\delta}{2}$ fraction of points in l are good, we have $\delta(c_w|_l, c|_l) < \frac{\delta}{2}$. Therefore $c_w|_l = c'_l$, and since $\mathbf{x}$ is good, we have $c(\mathbf{x}) = c_w(\mathbf{x}) = c'_l(\mathbf{x})$ as desired. It remains to prove that $c_w(\mathbf{y}) = c(\mathbf{y})$ for good $\mathbf{y} \in u$. By Claim V.2, at least $1 - \frac{\delta}{20}$ fraction of lines $l' \subseteq w$ through $\mathbf{y}$ satisfy $c_{l'}(\mathbf{y}) = c_w(\mathbf{y})$. Since $\mathbf{y}$ is good, more than $\frac{\delta}{20}$ fraction of lines $l' \subseteq w$

through $\mathbf{y}$ satisfy $c_{l'}(\mathbf{y}) = c(\mathbf{y})$. Therefore, there must be some line $l' \subseteq w$ through $\mathbf{y}$ which satisfies $c_w(\mathbf{y}) = c_{l'}(\mathbf{y}) = c(\mathbf{y})$.

Finally, for the robustness statement: if $q^{-1} \geq \frac{\delta^{24}}{2.5 \cdot 10^{10}}$, then by Corollary II.8, the robustness is at least $\frac{q^{-3}}{2} \geq \frac{\delta^{72}}{2 \cdot 10^{31}}$. Otherwise, the robustness is at least $\frac{\alpha_1 \delta^3}{57{,}600 \cdot 400} - 3q^{-1} \geq \frac{\delta^{24}}{10^{11}}$. □

REFERENCES

[AKK+05] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing Reed-Muller codes. *IEEE Transactions on Information Theory*, 51(11):4032–4039, 2005.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, May 1998.

[Aro94] Sanjeev Arora. *Probabilistic checking of proofs and the hardness of approximation problems*. PhD thesis, University of California at Berkeley, 1994.

[AS03] Sanjeev Arora and Madhu Sudan. Improved low degree testing and its applications. *Combinatorica*, 23(3):365–426, 2003. Preliminary version in Proceedings of ACM STOC 1997.

[BGM+11] Eli Ben-Sasson, Elena Grigorescu, Ghid Maatouk, Amir Shpilka, and Madhu Sudan. On sums of locally testable affine invariant properties. *Electronic Colloquium on Computational Complexity (ECCC)*, 18:79, 2011.

[BKS+10] Arnab Bhattacharyya, Swastik Kopparty, Grant Schoenebeck, Madhu Sudan, and David Zuckerman. Optimal testing of Reed-Muller codes. In *FOCS*, pages 488–497. IEEE Computer Society, 2010.

[BSGH+04] Eli Ben-Sasson, Oded Goldreich, Prahladh Harsha, Madhu Sudan, and Salil Vadhan. Robust PCPs of proximity, shorter PCPs and applications to coding. In *Proceedings of the 36th Annual ACM Symposium on Theory of Computing*, pages 1–10, New York, 2004. ACM Press.

[BSMSS11] Eli Ben-Sasson, Ghid Maatouk, Amir Shpilka, and Madhu Sudan. Symmetric LDPC codes are not necessarily locally testable. In *IEEE Conference on Computational Complexity*, pages 55–65. IEEE Computer Society, 2011.

[BSS06] Eli Ben-Sasson and Madhu Sudan. Robust locally testable codes and products of codes. *Random Structures and Algorithms*, 28(4):387–402, 2006.

[BSV09a] Eli Ben-Sasson and Michael Viderman. Composition of semi-LTCs by two-wise tensor products. In Dinur et al. [DJNR09], pages 378–391.

[BSV09b] Eli Ben-Sasson and Michael Viderman. Tensor products of weakly smooth codes are robust. *Theory of Computing*, 5(1):239–255, 2009. Preliminary version in Proc. APPROX-RANDOM 2008.

[DJNR09] Irit Dinur, Klaus Jansen, Joseph Naor, and José D. P. Rolim, editors. *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, 12th International Workshop, APPROX 2009, and 13th International Workshop, RANDOM 2009, Berkeley, CA, USA, August 21-23, 2009. Proceedings*, volume 5687 of *Lecture Notes in Computer Science*. Springer, 2009.

[DR04] Irit Dinur and Omer Reingold. Assignment testers: Towards a combinatorial proof of the PCP-theorem. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 155–164, Loc Alamitos, CA, USA, 2004. IEEE Press.

[DSW06] Irit Dinur, Madhu Sudan, and Avi Wigderson. Robust local testability of tensor products of LDPC codes. In Josep Díaz, Klaus Jansen, José D. P. Rolim, and Uri Zwick, editors, *APPROX-RANDOM*, volume 4110 of *Lecture Notes in Computer Science*, pages 304–315. Springer, 2006.

[FS95] Katalin Friedl and Madhu Sudan. Some improvements to total degree tests. In *Proceedings of the 3rd Annual Israel Symposium on Theory of Computing and Systems*, pages 190–198, Washington, DC, USA, 4-6 January 1995. IEEE Computer Society. Corrected version available online at `http://people.csail.mit.edu/madhu/papers/friedl.ps`.

[GGR09] Parikshit Gopalan, Venkatesan Guruswami, and Prasad Raghavendra. List decoding tensor products and interleaved codes. In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 13–22, 2009.

[GHS15] Alan Guo, Elad Haramaty, and Madhu Sudan. Robust testing of lifted codes with applications to low-degree testing. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:34, 2015.

[GKS08] Elena Grigorescu, Tali Kaufman, and Madhu Sudan. 2-transitivity is insufficient for local testability. In *CCC 2008: Proceedings of the 23rd IEEE Conference on Computational Complexity*, page (to appear). IEEE Computer Society, June 23-26th 2008.

[GKS09] Elena Grigorescu, Tali Kaufman, and Madhu Sudan. Succinct representation of codes with applications to testing. In Dinur et al. [DJNR09], pages 534–547.

[GKS13] Alan Guo, Swastik Kopparty, and Madhu Sudan. New affine-invariant codes from lifting. In Robert D. Kleinberg, editor, *Innovations in Theoretical Computer Science, ITCS '13, Berkeley, CA, USA, January 9-12, 2013*, pages 529–540. ACM, 2013.

[HRS13] Elad Haramaty, Noga Ron-Zewi, and Madhu Sudan. Absolutely sound testing of lifted codes. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 16th International Workshop, APPROX 2013, and 17th International Workshop, RANDOM 2013, Berkeley, CA, USA, August 21-23, 2013. Proceedings*, volume 8096 of *Lecture Notes in Computer Science*, pages 671–682. Springer, 2013.

[HSS11] Elad Haramaty, Amir Shpilka, and Madhu Sudan. Optimal testing of multivariate polynomials over small prime fields. In Rafail Ostrovsky, editor, *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 629–637. IEEE, 2011.

[JPRZ09] Charanjit S. Jutla, Anindya C. Patthak, Atri Rudra, and David Zuckerman. Testing low-degree polynomials over prime fields. *Random Struct. Algorithms*, 35(2):163–193, 2009.

[KL10] Tali Kaufman and Shachar Lovett. Testing of exponentially large codes, by a new extension to weil bound for character sums. *Electronic Colloquium on Computational Complexity (ECCC)*, 17:65, 2010.

[KR06] Tali Kaufman and Dana Ron. Testing polynomials over general fields. *SIAM J. Comput.*, 36(3):779–802, 2006.

[KS08] Tali Kaufman and Madhu Sudan. Algebraic property testing: the role of invariance. In *STOC*, pages 403–412, 2008.

[MR06] Dana Moshkovitz and Ran Raz. Sub-constant error low degree test of almost-linear size. In *Proceedings of the 38th Annual ACM Symposium on Theory of Computing, Seattle, WA, USA, May 21-23, 2006*, pages 21–30, 2006.

[RS96] Ronitt Rubinfeld and Madhu Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM Journal on Computing*, 25(2):252–271, April 1996.

[RS97] Ran Raz and Shmuel Safra. A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*, pages 475–484, New York, NY, 1997. ACM Press.

[Val05] Paul Valiant. The tensor product of two codes is not necessarily robustly testable. In Chandra Chekuri, Klaus Jansen, José D. P. Rolim, and Luca Trevisan, editors, *APPROX-RANDOM*, volume 3624 of *Lecture Notes in Computer Science*, pages 472–481. Springer, 2005.

[Vid12] Michael Viderman. A combination of testability and decodability by tensor products. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques - 15th International Workshop, APPROX 2012, and 16th International Workshop, RANDOM 2012, Cambridge, MA, USA, August 15-17, 2012. Proceedings*, pages 651–662, 2012.