Electronic Colloquium on Computational Complexity, Report No. 43 (2015)

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

Alan Guo* Elad Haramaty† Madhu Sudan‡

April 2, 2015

**Abstract**

A local tester for a code probabilistically looks at a given word at a small set of coordinates and based on this local view accepts codewords with probability one while rejecting words far from the code with constant probabilility. 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.

*CSAIL, Massachusetts Institute of Technology, 32 Vassar Street, Cambridge, MA, USA. aguo@mit.edu. Research supported in part by NSF grant CCF-1420956, NSF/Purdue Subaward Number 0939370, and an NSF Graduate Research Fellowship.

†College of Computer and Information Science, Northeastern University, 360 Huntington Ave, Boston, MA eladh@cs.technion.ac.il. Research supported in part by NSF grant CCF-1319206.

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

ISSN 1433-8092

# Contents

# 1 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 $\tau$-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 $\ell$, an *$\ell$-local tester* $\mathcal{T}$ is a distribution $\mathcal{D}$ on $(S^\ell, \mathcal{P}(\mathbb{F}_q^\ell))$[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 *$\epsilon$-sound* if $\mathcal{T}$ accepts $f \in \mathcal{C}$ with probability one, while rejecting $f$ that is $\delta$-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" 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 $\alpha$-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 $(\pi, V)$, it follows that an $\alpha$-robust tester is also $\alpha$-sound. On the other hand an $\alpha$-sound $\ell$-local tester is at least $(\alpha/\ell)$-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 $\alpha$-robust tester for $f$ with distribution $\mathcal{D}$ and if for every $(\pi, V)$ in the support of $\mathcal{D}$, the property of being in $V$ has an $\ell'$-local tester that is $\epsilon$-sound, then $\mathcal{C}$ has an $\ell'$-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 this is really just one hope. We illustrate the concept of robustness in the context of low-degree testing and describe the role it has played in applications.

## 1.1 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 $d \ll q$

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

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 $\pi$ are different affine subspaces of low-dimension (one or two) and the acceptable pattern $V$ is the same for all $\pi$. 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.

### 1.2 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 $n^\alpha$-local testers on codes of length $n$ for arbitrarily small $\alpha$ [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 $\epsilon_q$-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.

### 1.3 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 1.1.** $\forall \delta > 0\ \exists \alpha > 0$ *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* $\alpha$*-robust.*

Theorem 1.1 is proved in Section 3. As we elaborate below, Theorem 1.1 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 $\alpha$ on $\delta$ 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 2.9.) 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 $\epsilon_q$ 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 $\delta$) our results are much stronger.

Turning to consequences of our main theorem, a direct corollary obtained by applying Theorem 1.1 to codes developed by Guo et al. [GKS13] are codes of rate close to 1 that have $n^\epsilon$-local $\Omega(1)$-robust local testers.

**Corollary 1.2.** $\forall \epsilon, \beta > 0,\ \exists \alpha > 0$ *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* $\alpha$*-robust* $n^\epsilon$*-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 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 1.3.** $\forall \delta > 0\ \exists \alpha > 0$ *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* $\alpha$*-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.

### 1.4 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 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

[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 $ad = bc$.

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 $\delta$ (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 2. We analyze the test for lifted codes in Section 3. We then apply the lifted-code tester to get an efficient and robust low-degree test in Section 4. Sections 3 and 4 depend on some algebraic analyses of lifted, tensored and affine-invariant codes which we defer to Section 5.

## 2 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 $\mathbb{F}_q^m$.

### 2.1 Affine-invariance and degree sets

**Definition 2.1.** 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 2.2.** 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 $i \geq 0$. For $m \geq 1$ and vectors $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{N}^m$ and $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{N}^m$, *$\mathbf{a}$ is in the $p$-shadow of $\mathbf{b}$*, denoted $\mathbf{a} \leq_p \mathbf{b}$, if $a_i \leq_p b_i$ for $i \in [m]$.

**Definition 2.3.** 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 $\mathbf{e} \in \mathrm{Deg}(\mathcal{C})$.

**Proposition 2.4.** *Every linear affine-invariant code over $\mathbb{F}_q$ of characteristic $p$ has a $p$-shadow-closed degree set.*

### 2.2 Lifting

Whenever $f : \mathbb{F}_q^m \to \mathbb{F}_q$ and $A \subseteq \mathbb{F}_q^m$ is a $t$-dimensional affine subspace, we think of $A$ as being parameterized by some affine function $A : \mathbb{F}_q^t \to \mathbb{F}_q^m$ (abusing notation) and by the restriction $f|_A$ of $f$ to $A$, we mean the $t$-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.

**Definition 2.5.** Let $t \leq m$ and let $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be affine-invariant. Then the *$m$-dimensional lift $\mathcal{C}^{t \nearrow m}$ of $\mathcal{C}$* is the code

$$\mathcal{C}^{t \nearrow m} \triangleq \left\{ f : \mathbb{F}_q^m \to \mathbb{F}_q \;\middle|\; f|_A \in \mathcal{C} \text{ for any } t\text{-dimensional affine subspace } A \right\}$$

**Proposition 2.6** (**Distance of lifted codes** [GKS13, Theorem 5.1, Part (2)])**.** *Let $t \le m$ and let $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be affine-invariant. Then $\delta(\mathcal{C}^{t\nearrow m}) \ge \delta(\mathcal{C}) - q^{-t}$.*

## 2.3 Testing and robustness

We now define the robustness of a lifted code, specializing the definition to robustness with respect to subspace testers. We include the dimension of the testing subspace as a parameter in the robustness since this will be convenient later.

**Definition 2.7.** Let $t \le k \le m$. The code $\mathcal{C}^{t\nearrow m}$ is $(\alpha, k)$-*robust* if, for every $r : \mathbb{F}_q^m \to \mathbb{F}_q$,

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

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

In this terminology we wish to show that $\mathcal{C}^{t\nearrow m}$ is $(\alpha, 2t)$-robust for some $\alpha$ 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 $k_2 \ge k_1$, then

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

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

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

**Theorem 2.8.** *If $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ is linear affine-invariant, then $\mathcal{C}^{t\nearrow m}$ has a $t$-dimensional subspace test which rejects with probability $\frac{\delta\left(r, \mathcal{C}^{t\nearrow n}\right)}{(2q^t+1)(q^t-1)}$.*

As a corollary to Theorem 2.8, the $k$-dimensional test (for $k \ge t$) for $\mathcal{C}^{t\nearrow m}$ is $O(q^{-3t})$-robust.

**Corollary 2.9.** *If $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ is linear affine-invariant, then $\mathcal{C}^{t\nearrow m}$ is $(\frac{q^{-3t}}{2}, k)$-robust for $k \ge t$.*

*Proof.* It suffices to show that $\mathcal{C}^{t\nearrow m}$ is $(\frac{q^{-3t}}{2}, t)$-robust. Let $r : \mathbb{F}_q^m \to \mathbb{F}_q$ and $u$ be a random $t$-dimensional affine subspace. Then

$$\begin{aligned}
\mathbb{E}_u \left[ \delta\left( r|_u, \mathcal{C} \right) \right] &= \mathbb{E}_u \left[ \delta\left( r|_u, \mathcal{C} \right) \mid r|_u \notin \mathcal{C} \right] \cdot \Pr_u \left[ r|_u \notin \mathcal{C} \right] \\
&\ge q^{-t} \cdot \Pr_u \left[ r|_u \notin \mathcal{C} \right] \\
\text{(Theorem 2.8)} \quad &\ge q^{-t} \cdot \frac{\delta\left( r, \mathcal{C}^{t\nearrow m} \right)}{(2q^t+1)(q^t-1)} \\
&\ge \frac{q^{-3t}}{2} \cdot \delta\left( r, \mathcal{C}^{t\nearrow m} \right).
\end{aligned}$$

□

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

**Proposition 2.10** (**Robustness composes multiplicatively**)**.** *Let $t \le k_1 \le k_2 \le m$ and let $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be linear affine-invariant. If $\mathcal{C}^{t\nearrow m}$ is $(\alpha_2, k_2)$-robust and $\mathcal{C}^{t\nearrow k_2}$ is $(\alpha_1, k_1)$-robust, then $\mathcal{C}^{t\nearrow m}$ is $(\alpha_1 \cdot \alpha_2, k_1)$-robust.*

## 2.4 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 2.11.** Let $n \geq 2$, let $t_1, \ldots, t_n \geq 1$ and $m = \sum_{i=1}^n t_i$, and for each $i \in [n]$, let the code $\mathcal{C}_i \subseteq \{\mathbb{F}_q^{t_i} \to \mathbb{F}_q\}$ be linear and let $V_{i,\mathbf{a}} \subseteq \mathbb{F}_q^m$ be the $t_i$ dimensional subspace consisting of all points where the $i$-th block (of $t_i$ coordinates) is free and all the $[n] \setminus \{i\}$ blocks are fixed to $\mathbf{a} \in \prod_{j \neq i} \mathbb{F}_q^{t_j}$. The *tensor product code* $\mathcal{C}_1 \otimes \cdots \otimes \mathcal{C}_n \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ is the code

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

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

The following characterization of tensor product codes will be helpful.

**Proposition 2.12.** *Let $n \geq 2$, let $t_1, \ldots, t_n \geq 1$ and $m = \sum_{i=1}^n t_i$, and for each $i \in [n]$, let the code $\mathcal{C}_i \subseteq \{\mathbb{F}_q^{t_i} \to \mathbb{F}_q\}$ be linear, and let $\mathbf{X}_i = (X_{i1}, \ldots, X_{it_i})$ be variables. Then*

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

**Corollary 2.13.** *If $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ has a degree set $\mathrm{Deg}(\mathcal{C})$, and $n \geq 1$, then $\mathcal{C}^{\otimes n}$ has degree set $\mathrm{Deg}(\mathcal{C}^{\otimes n}) = \mathrm{Deg}(\mathcal{C})^n$. In particular, if $\mathcal{C}$ is linear affine-invariant, and $\mathbb{F}_q$ has characteristic $p$, then $\mathcal{C}^{\otimes n}$ has a $p$-shadow-closed degree set.*

**Proposition 2.14.** *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be codes with distance $\delta_1$ and $\delta_2$ repectively. Then $\delta(\mathcal{C}_1 \otimes \mathcal{C}_2)$ is at least $\delta_1\delta_2$. In particular, $\delta\left(\mathcal{C}^{\otimes n}\right) \geq \delta(\mathcal{C})^n$.*

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

**Proposition 2.15.** *Let $\mathcal{C} = \mathcal{C}_1 \otimes \ldots \mathcal{C}_n \in \left\{\mathbb{F}_q^m \to \mathbb{F}_q\right\}$ and $S \subseteq \mathbb{F}_q^m$ be a subset such that for every $i \in [n]$ and $\mathbf{a} \in \prod_{j \neq i} \mathbb{F}_q^{t_j}$ satisfy $|S \cap V_{i,\mathbf{a}}| \geq (1 - \delta(\mathcal{C}_i))q^{t_i}$. Let $r : S \to \mathbb{F}_q$ be such that for every $i \in [n]$ and $\mathbf{a} \in \prod_{j \neq i} \mathbb{F}_q^{t_j}$ 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 $r'|_S = r$.*

## 2.5 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 2.16.** *Let $t \le k < m$. Let $u \subseteq \mathbb{F}_q^m$ be a fixed affine subspace of dimension $t$, and let $v \subseteq \mathbb{F}_q^m$ be a uniformly random affine subspace of dimension $k$. Then $\Pr_v[u \cap v \neq \emptyset] < q^{-(m-k-t)}$.*

*Proof.* By affine symmetry, we may assume that $v$ is fixed and $u$ is random. Furthermore, we can assume that $v = (\mathbf{0}, B)$, where $B$ is a basis and hence $|B| = k$. We choose $u$ by choosing random $\mathbf{x} \in \mathbb{F}_q^m$, random basis $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_t\}$, and setting $u \triangleq (\mathbf{x}, A)$. Let $E$ be the event that $u \cap v \neq \emptyset$.

Re-arrange $\mathbf{a}_1, \ldots, \mathbf{a}_t$ so that for some $0 \le s \le t-1$, $\mathbf{a}_i \in \mathrm{span}(B)$ if and only if $i \le s$. Note that $E$ holds if and only if there exist $c_1, \ldots, c_t \in \mathbb{F}_q^m$ such that $\mathbf{x} + c_1\mathbf{a}_1 + \cdots + c_t\mathbf{a}_t \in \mathrm{span}(B)$. Let $P : \mathbb{F}_q^m \to \mathbb{F}_q^{m-k}$ be the linear map that projects onto the last $m-k$ coordinates. Note that $\ker(P) = B$. For each $i \in [t]$, let $\mathbf{a}'_i \triangleq P\mathbf{a}_i \in \mathbb{F}_q^{m-k}$. Then $E$ holds if and only if $P\mathbf{x} \in \mathrm{span}(\mathbf{a}'_{s+1}, \ldots, \mathbf{a}'_t)$. Therefore, there are at most $q^t$ choices for $P\mathbf{x}$, hence at most $q^{k+t}$ choices for $\mathbf{x}$, out of $q^m$ total choices for $\mathbf{x}$, so $\Pr[E] \le \frac{q^{k+t}}{q^m} = q^{-(m-k-t)}$. □

**Lemma 2.17.** *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 $\mathbf{a}_{i+1} \notin \mathrm{span}\{\mathbf{a}_1, \ldots, \mathbf{a}_i\}$ given that the latter are linearly independent is $1 - q^{-(m-i)}$. Therefore the probability that all of them are independent is

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

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 $1 - q^{-(m-2t)}$. □

# 3 Robustness of lifted codes

In this section, we prove Theorem 3.15, which is simply a more precise restatement of Theorem 1.1. Our approach is a standard one - we first analyze the test for low-dimensional settings (Theorem 3.1), and then use a general projection argument ("bootstrapping") to get an analysis for all dimensions (Theorem 3.15).

## 3.1 Robustness for small dimension

Throughout Sections 3.1 and 3.2, fix a linear affine invariant code $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ with relative distance $\delta \triangleq \delta(\mathcal{C})$. Let $n \ge 1$ be an integer (we will use $n = 3$ or 4) and let $m = nt$. Two codes that play a prominent role are the lift $\mathcal{C}^{t \nearrow m}$ of $\mathcal{C}$ to $m$ dimensions, and the $n$-fold tensor product $\mathcal{C}^{\otimes n}$ of $\mathcal{C}$, which is also an $m$-dimensional code. We begin by giving a tester with robust analysis for $\mathcal{C}^{t \nearrow m}$ for this restricted choice of $m$. We will show that the $(m-t)$-dimensional test is $\left(\frac{\delta^n}{n}\right)^{O(1)}$-robust. (Note the robustness degrades poorly with $n = m/t$ and so can only be applied for small $n$). It is important, for Section 3.3, that there is no dependence on $t$.

**Theorem 3.1.** *Let $n \geq 3$ and $t \geq 1$ and set $m = nt$. Then $\mathcal{C}^{t\nearrow^m}$ is $(\alpha_0, m-t)$-robust for $\alpha_0 = \frac{\delta^{3n}}{16(n^2+3n+2)^3}$.*

**Overview.** For simplicity, we describe the proof idea for $t = 1$. Suppose the average local distance to $\mathcal{C}^{1\nearrow^{(m-1)}}$ on random hyperplanes is small. For $\mathbf{a} \in \mathbb{F}_q^m$, let $\mathcal{C}_{\mathbf{a}}$ be the code consisting of tensor codewords in $\mathcal{C}^{\otimes n}$ whose restrictions to lines in direction $\mathbf{a}$ are also codewords of $\mathcal{C}$. Note that $\bigcap_{\mathbf{a}} \mathcal{C}_{\mathbf{a}} = \mathcal{C}^{1\nearrow^m}$. Our main technical result (Theorem 3.8) of this section shows that $\mathcal{C}_{\mathbf{a}}$ is $\left(\frac{\delta^n}{n}\right)^{O(1)}$-robust. Now, observe that choosing a random hyperplane can be done by choosing $m$ random linearly independent directions, choosing an additional random direction $\mathbf{a}$ that is not spanned by any $m-1$ of the former, and choosing a random hyperplane spanned by $m-1$ of these $m+1$ random directions (call such a hyperplane "special"). Viewing the first $m$ chosen directions as the standard basis directions, we see that the average local distance to $\mathcal{C}^{1\nearrow^{(m-1)}}$, and hence to $\mathcal{C}^{\otimes(m-1)}$, when restricting to special hyperplanes, is still small. Therefore, for most $\mathbf{a}$, the average local distance to $\mathcal{C}^{\otimes(m-1)}$ on special hyperplanes is small. By the robustness of $\mathcal{C}_{\mathbf{a}}$, this implies that our received word is close to some codeword $c_{\mathbf{a}} \in \mathcal{C}_{\mathbf{a}}$ for most $\mathbf{a}$. But these codewords $c_{\mathbf{a}}$ are all codewords of $\mathcal{C}^{\otimes m}$ and close to each other, so they must be the same codeword $c \in \mathcal{C}^{\otimes m}$. So we have shown that we are close to $c \in \mathcal{C}^{\otimes m}$. We proceed by showing that in fact $c \in \mathcal{C}^{1\nearrow^m}$. Note that $c \in \mathcal{C}_{\mathbf{a}}$ for most $\mathbf{a}$. Another technical result, Corollary 5.8, implies that in fact $c \in \mathcal{C}_{\mathbf{a}}$ for all $\mathbf{a}$ and we are done.

To generalize to $t > 1$, we replace dimension $k$ subspaces with dimension $kt$ subspaces throughout. Some work needs to be done to ensure that Theorem 3.8 still works, and also Corollary 5.8 must be generalized appropriately to remove the dependence on $t$. These issues will be discussed in the corresponding sections.

For a set $S$ and integer $c$, let $\binom{S}{c}$ denote the collection of subsets of $S$ of size $c$:

$$\binom{S}{c} \triangleq \{T \subseteq S \mid |T| = c\}.$$

**Definition 3.2.** Let $\ell \leq m$ be an integer. A collection $D \subseteq \binom{\mathbb{F}_q^m}{t}$ is *$\ell$-proper* if for every $k$ and every distinct $A_1, \ldots, A_k \in D$, the union $\bigcup_{i=1}^k A_i$ contains at least $\min\{kt, m-\ell\}$ linearly independent vectors.

**Definition 3.3.** For a set $D \subseteq \binom{\mathbb{F}_q^m}{t}$, for every $\mathbf{x} \in \mathbb{F}_q^m$ define $\mathcal{V}_D^k(\mathbf{x})$ to be the collection of subspaces through $\mathbf{x}$ in directions from $k$ different sets from $D$. More precisely,

$$\mathcal{V}_D^k(\mathbf{x}) \triangleq \left\{ (\mathbf{x}, A) \;\middle|\; A = \bigcup_{i=1}^k D_i, \quad \{D_1, \ldots, D_k\} \in \binom{D}{k} \right\}$$

Define

$$\mathcal{V}_D^k \triangleq \bigcup_{\mathbf{x} \in \mathbb{F}_q^n} \mathcal{V}_D^k(\mathbf{x}).$$

The *testing subspaces through* $\mathbf{x}$ are $\mathcal{T}_D(\mathbf{x}) \triangleq \mathcal{V}_D^{m-1}(\mathbf{x})$ and the *decoding subspaces through* $\mathbf{x}$ are $\mathcal{D}_D(\mathbf{x}) \triangleq \mathcal{V}_D^1(\mathbf{x})$. Similarly, the *testing subspaces* are $\mathcal{T}_D \triangleq \mathcal{V}_D^{m-1}$ and the *decoding subspaces* are $\mathcal{D}_D \triangleq \mathcal{V}_D^1$. If $S = (\mathbf{x}, \cup_{i=1}^k D_i) \in \mathcal{V}_D^k$, then the *blocks of* $S$ are the sets $D_1, \ldots, D_k$. Two testing subspaces are *adjacent* if they differ in at most one block.

**Remark 3.4.** If $D$ is $\ell$-proper for $\ell \leq t$ then for any $k < n$ we have that $\mathcal{V}_D^k$ consists of $kt$-dimensional subspaces.

**Definition 3.5.** Define $\mathcal{C}_D^n$ to be the code of all words $f : \mathbb{F}_q^m \to \mathbb{F}_q$ such that $f|_u \in \mathcal{C}$ for every decoding subspace $u \in \mathcal{D}_D$.

**Remark 3.6.** Observe that $\mathcal{C}^{t\nearrow m}$ is a subcode of $\mathcal{C}_D^n$ for any $D$. If $\bigcup D$ contains the standard basis vectors, then $\mathcal{C}_D^n$ is a subcode of $\mathcal{C}^{\otimes n}$.

*Proof of Theorem 3.1.* Define $\ell \triangleq \left\lfloor \frac{n\log\left(\frac{1}{\delta}\right)+\log(n^2+3n+2)+1}{\log(q)} \right\rfloor$. We note that for the most interesting cases, where $\delta > 0$ and $n$ are fixed and $q \to \infty$, $\ell = 0$. Our first step handles the less interesting cases (by appealing to a known result). Specifically, if $\ell \geq t$ then by Corollary 2.9 we are done since

$$\frac{q^{-3t}}{2} \geq \frac{q^{-3\ell}}{2} \geq \frac{q^{-3\left(\frac{n\log\left(\frac{1}{\delta}\right)+\log(n^2+3n+2)+1}{\log(q)}\right)}}{2} = \frac{\delta^{3n}}{16(n^2+3n+2)^3} = \alpha_0 \ .$$

Now assume $\ell < t$ and let $\rho \triangleq \mathbb{E}_v\left[\delta\left(r|_v, \mathcal{C}^{t\nearrow(m-t)}\right)\right]$, where $v \subseteq \mathbb{F}_q^m$ is a uniformly random $(m-t)$-dimensional affine subspace. We will assume without lost of generality that $\rho \leq \alpha_0$ and in particular $\rho \leq \frac{\delta^{3n}}{16\binom{n+1}{n-1}^2(n^2+3n+2)} \leq \frac{\delta^{2n}q^{-\ell}}{8\binom{n+1}{n-1}^2}$.

Observe that

$$\rho = \mathbb{E}_{A_1,\ldots,A_n \in \binom{\mathbb{F}_q^m}{t}} \mathbb{E}_{A \in \binom{\mathbb{F}_q^n}{t}} \mathbb{E}_{v \in \mathcal{T}_{\{A_1,\ldots,A_n,A\}}} \left[\delta\left(r|_v, \mathcal{C}^{t\nearrow(m-t)}\right)\right]$$

where $A_1, \ldots, A_n$ are random sets such that their union is linearly independent, and $A$ is a random set such that $\{A_1, \ldots, A_n, A\}$ is $\ell$-proper. Fix $A_1, \ldots, A_n$ such that

$$\mathbb{E}_{A \in \binom{\mathbb{F}_q^m}{t}} \mathbb{E}_{v \in \mathcal{T}_{\{A_1,\ldots,A_n,A\}}} \left[\delta\left(r|_v, \mathcal{C}^{t\nearrow(m-t)}\right)\right] \leq \rho.$$

Since $\mathcal{C}^{t\nearrow(m-t)} \subseteq \mathcal{C}^{\otimes(n-1)}$,

$$\mathbb{E}_{A \in \binom{\mathbb{F}_q^m}{t}} \mathbb{E}_{v \in \mathcal{T}_{\{A_1,\ldots,A_n,A\}}} \left[\delta\left(r|_v, \mathcal{C}^{\otimes(n-1)}\right)\right] \leq \rho.$$

By affine-invariance, we may assume without loss of generality that $A_1, \ldots, A_n$ form the standard basis vectors for $\mathbb{F}_q^m$. For any $A \in \binom{\mathbb{F}_q^m}{t}$, let $D_A \triangleq \{A_1, \ldots, A_n, A\}$. By Markov's inequality,

$$\Pr_A\left[\mathbb{E}_{v \in \mathcal{T}_{D_A}}\left[\delta\left(r|_v, \mathcal{C}^{\otimes(n-1)}\right) \geq 2\delta^{-n}\rho\right]\right] < \frac{1}{2}\delta^n.$$

So, for more than $1 - \frac{1}{2}\delta^n$ fraction of blocks $A$ such that $D_A$ is $\ell$-proper, we have a codeword $c_A \in \mathcal{C}_{D_A}^n \subseteq \mathcal{C}^{\otimes n}$ such that (by Theorem 3.8) $\delta(r, c_A) < 2\delta^{-n}\rho\binom{n+1}{n-1} < \frac{1}{2}\delta^n$. For every two such blocks $A, A'$, we have $\delta(c_A, c_{A'}) \leq \delta(c_A, r) + \delta(r, c_{A'}) < \delta^n = \delta(\mathcal{C}^{\otimes n})$, so there is some codeword $c \in \mathcal{C}^{\otimes n}$ such that $c_A = c$ for every such $A$. For such $A$, it follows that for every $\mathbf{b} \in \mathbb{F}_q^m$, the restriction of $c$ to the subspace $(\mathbf{b}, A)$ is a codeword of $\mathcal{C}$, i.e. $c|_{(\mathbf{b},A)} \in \mathcal{C}$. By Claim 3.14, for more than $1 - \frac{1}{2}\delta^n - \binom{n}{2}\frac{q^{-t}}{q-1} - n\frac{q^{-l}}{q-1}$ fraction of blocks $A$ (without the requirement that $D_A$ be proper), $c|_{(\mathbf{b},A)} \in \mathcal{C}$ for every $\mathbf{b} \in \mathbb{F}_q^m$. In particular, $c \in \mathcal{C}^{\otimes n}$ and for every $\mathbf{b} \in \mathbb{F}_q^m$, $c|_{(\mathbf{b},A)} \notin \mathcal{C}$ for less than

$\frac{1}{2}\delta^n + \binom{n}{2}\frac{q^{-t}}{q-1} + n\frac{q^{-\ell}}{q-1}$ fraction of $A$. It sufficient to show that $\frac{1}{2}\delta^n + \binom{n}{2}\frac{q^{-t}}{q-1} + n\frac{q^{-l}}{q-1} \le \delta^n - (n+1)q^{-t}$. Then it will follow from Corollary 5.8 that $c \in \mathcal{C}^{t\nearrow m}$ and since $\delta(r,c) \le 2\delta^{-n}\rho\binom{n+1}{n-1}$ we are done. Calculating:

$$\binom{n}{2}\frac{q^{-t}}{q-1}+n\frac{q^{-l}}{q-1}+(n+1)q^{-t} \le \binom{n}{2}\frac{q^{-l}}{q-1}+n\frac{q^{-l}}{q-1}+(n+1)\frac{q^{-l}}{q-1} = \frac{q^{-l}}{q-1}\left(\frac{n^2+3n+2}{2}\right) \le \frac{q\delta^n}{4(q-1)} \le \frac{1}{2}\delta^n$$

□

The composability of robust tests immediately yields the following corollary where the test is now $2t$ dimensional.

**Corollary 3.7.** *$\mathcal{C}^{t\nearrow 4t}$ is $(\alpha_1, 2t)$-robust, where $\alpha_1 \ge \frac{\delta^{21}}{6\cdot 10^{10}}$.*

*Proof.* By Theorem 3.1, $\mathcal{C}^{t\nearrow 4t}$ is $\left(\frac{\delta^{12}}{432{,}000}, 3t\right)$-robust and $\mathcal{C}^{t\nearrow 3t}$ is $\left(\frac{\delta^{9}}{128{,}000}, 2t\right)$-robust. Therefore, by composing, the $2t$-dimensional robustness of $\mathcal{C}^{t\nearrow 4t}$ is at least $\frac{\delta^{12}}{432{,}000}\cdot\frac{\delta^{9}}{128{,}000} = \frac{\delta^{21}}{55{,}296{,}000{,}000}$ □

## 3.2 Robustness of special tensor codes

In this section, we prove the main technical result (Theorem 3.8) used in Section 3.1.

**Theorem 3.8.** *Let $n \ge 3$ and $\ell \le t$. Set $m = nt$. Let $D \subseteq \binom{\mathbb{F}_q^n}{t}$ be $\ell$-proper with $|D| \ge n$ blocks. Let $r : \mathbb{F}_q^m \to \mathbb{F}_q$ be a word with $\rho \triangleq \mathbb{E}_{v\in\mathcal{T}_D}\left[\delta\left(r|_v, \mathcal{C}^{\otimes(n-1)}\right)\right]$. If $\rho < \frac{\delta^n q^{-\ell}}{4\binom{|D|}{n-1}^2}$, then $\delta(r, \mathcal{C}_D^n) \le \rho\binom{|D|}{n-1}$.*

**Overview.** Our analysis is an adaptation of Viderman's [Vid12]. For simplicity, assume $t = 1$. 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 3.10 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 3.9 shows that every bad point is in a bad hyperplane, and Claim 3.11 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 $\delta q$ 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.

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 3.12 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 3.11. Finally Claim 3.13 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 3.12, in each direction we have enough lines $u$ with no super-bad points, for which $c|_u \in \mathcal{C}$ (by Claim 3.13), so that we can uniquely extend $c$ onto the entire plane (by Proposition 2.15). 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 3.13. 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 for the case $t = 1$. To generalize to $t > 1$, we replace lines with "decoding subspaces" (subspaces of dimension $t$), planes with subspaces of dimension $2t$, and hyperplanes with "testing subspaces" (subspaces of codimension $t$). Some care must be taken when proving Claim 3.12, because the intersection of two decoding subspaces may have non-trivial dimension. We therefore require the notion of "$\ell$-properness" of $D$, and must modify Claim 3.11 and also prove Claim 3.14 to accommodate this notion.

*Proof of Theorem 3.8.* For each testing subspace $v \in \mathcal{T}_D$, define $c_v \in \mathcal{C}^{\otimes(n-1)}$ to be the closest codeword to $r|_v$ (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:

$$\begin{aligned} G &\triangleq \left\{\mathbf{x} \in \mathbb{F}_q^m \mid c_v(\mathbf{x}) = r(\mathbf{x}) \text{ for every } v \in \mathcal{T}_D(\mathbf{x})\right\} \\ F &\triangleq \left\{\mathbf{x} \in \mathbb{F}_q^m \mid c_v(\mathbf{x}) = c_{v'}(\mathbf{x}) \neq r(\mathbf{x}) \text{ for every } v, v' \in \mathcal{T}_D(\mathbf{x})\right\} \\ B &\triangleq \left\{\mathbf{x} \in \mathbb{F}_q^m \mid c_v(\mathbf{x}) \neq c_{v'}(\mathbf{x}) \text{ for some } v, v' \in \mathcal{T}_D(\mathbf{x})\right\}. \end{aligned}$$

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

$$B' \triangleq \{\mathbf{x} \in B \mid \text{every } v \in \mathcal{T}_D(\mathbf{x}) \text{ is bad or } \exists \text{ good } v, v' \in \mathcal{T}_D(\mathbf{x}) \text{ such that } c_v(\mathbf{x}) \neq c_{v'}(\mathbf{x})\}.$$

**Claim 3.9.** *If $v, v' \in \mathcal{T}_D$ are adjacent good testing subspaces, then $c_v|_{v\cap v'} = c_{v'}|_{v\cap v'}$. In particular, every bad point is in a bad testing subspace.*

*Proof.* Suppose $\mathbf{b} \in v \cap v'$ and $c_v(\mathbf{b}) \neq c_{v'}(\mathbf{b})$. Since $v, v'$ are adjacent, they have $n-2$ blocks $A_1, \ldots, A_{n-2}$ in common. Let $v$ have blocks $A_1, \ldots, A_{n-2}, A$ and let $v'$ have blocks $A_1, \ldots, A_{n-2}, A'$.

Let $u \in \mathcal{D}_D$ be the decoding subspace $(\mathbf{b}, A_1)$. Since $c_v|_u, c_{v'}|_u \in \mathcal{C}$ disagree on $\mathbf{b}$, they are distinct codewords and hence disagree on at least $\delta q^t$ points of $u$, say $\mathbf{x}_1, \ldots, \mathbf{x}_{\delta q^t}$. For each $i \in [\delta q^t]$, let $v_i \in \mathcal{T}_D$ be the testing subspace $(\mathbf{x}_i, A_2 \cup \cdots \cup A_{n-2} \cup A \cup A')$.

Since $c_v(\mathbf{x}_i) \neq c_{v'}(\mathbf{x}_i)$, that means $c_{v_i}$ disagrees with one of $c_v, c_{v'}$ at $\mathbf{x}_i$. Without loss of generality, suppose $c_v$ disagrees with $c_{v_1}, \ldots, c_{v_{\delta q^t/2}}$. We will show that $v$ is bad, which proves the first part of the claim.

For each $i \in [\delta q^t]$, let $w_i = (\mathbf{x}_i, A_2 \cup \cdots \cup A_{n-2} \cup A)$. Note that $u \cap w_i = \{\mathbf{x}_i\}$ (since $D$ is $\ell$-proper, for $\ell \leq t$), so all $w_i$ are different parallel subspaces and hence disjoint. Since $w_i \in \mathcal{V}_D^{n-2}$, the restrictions $c_v|_{w_i}, c_{v_i}|_{w_i} \in \mathcal{C}^{\otimes n-2}$ are codewords and are distinct because they disagree on $\mathbf{x}_i$, therefore, by Proposition 2.14, they disagree on at least $\delta^{n-2}q^{m-2t}$ points in $w_i$, which are therefore bad. Thus, each $v_i$ contributes $\delta^{n-2}q^{m-2t}$ bad points to $v$, for a total of $\frac{1}{2}\delta^{n-1}q^{m-t}$ bad points since the $w_i$ are disjoint.

For the second part, suppose $\mathbf{b} \in B$ is a bad point. We will show that $\mathbf{b}$ lies in a bad testing subspace. By definition, there are two testing subspaces $v, v' \in \mathcal{T}_D(\mathbf{b})$ such that $c_v(\mathbf{b}) \neq c_{v'}(\mathbf{b})$. Suppose $v$ has blocks $A_1, \ldots, A_{n-1}$ and $v'$ has directions $A'_1, \ldots, A'_{n-1}$. Assume, without lost of generality, that if $A_i = A'_j$ then $i = j$. Define $v_0 \triangleq v$, and for $i \in [n-1]$, define $v_i \in \mathcal{T}_D$ to be the testing subspace through $\mathbf{b}$ in directions $A'_1, \ldots, A'_i, A_{i+1}, \ldots, A_{n-1}$. Consider the sequence $v_0, v_1, \ldots, v_{n-1}$ of testing subspaces. For each $i$, the testing subspaces $v_i, v_{i+1}$ are adjacent. Since $c_{v_0}(\mathbf{b}) \neq c_{v_{n-1}}(\mathbf{b})$, there exists some $i$ such that $c_{v_i}(\mathbf{b}) \neq c_{v_{i+1}}(\mathbf{b})$, and by the first part of the claim it follows that one of $v_i, v_{i+1}$ is bad. □

**Claim 3.10.** $\rho \geq \frac{|F|}{q^m} + \frac{|B|}{q^m\binom{|D|}{n-1}}$

*Proof.* Observe that $|\mathcal{T}_D| = q^t\binom{|D|}{n-1}$. Therefore,

$$\begin{aligned}
\rho &= \mathbb{E}_{v\in\mathcal{T}_D}\left[\delta\left(r|_v, \mathcal{C}^{\otimes(n-1)}\right)\right] \\
&= \mathbb{E}_{v\in\mathcal{T}_D}\left[\delta\left(r|_v, c_v\right)\right] \\
&= \frac{1}{q^t\binom{|D|}{n-1}} \sum_{v\in\mathcal{T}_D} \frac{1}{q^{m-t}} \sum_{\mathbf{x}\in v} \mathbb{1}_{c_v(\mathbf{x})\neq r(\mathbf{x})} \\
&= \frac{1}{q^m\binom{|D|}{n-1}} \sum_{\mathbf{x}\in\mathbb{F}_q^m} \#\{v \in \mathcal{T}_D(\mathbf{x}) \mid c_v(\mathbf{x}) \neq r(\mathbf{x})\} \\
&\geq \frac{1}{q^m\binom{|D|}{n-1}} \left(\sum_{\mathbf{x}\in G} 0 + \sum_{\mathbf{x}\in F}\binom{|D|}{m-1} + \sum_{\mathbf{x}\in B} 1\right) \\
&= \frac{|F|}{q^m} + \frac{|B|}{q^m\binom{|D|}{n-1}}.
\end{aligned}$$

□

**Claim 3.11.** *There are less than $\frac{1}{2}\delta q^{t-\ell}$ bad testing subspaces.*

*Proof.* By Claim 3.10, there are at most $|B| \leq \rho\binom{|D|}{n-1}q^m$ bad points. Each bad testing subspace has at least $\delta^{n-1}q^{m-t}/2$ bad points by definition. Each bad point has at most $\binom{|D|}{n-1}$ bad testing subspaces through it. Therefore, there are at most

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

bad testing subspaces. □

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

For $\mathbf{x} \in B \setminus B'$, define $c(\mathbf{x}) \triangleq c_v(\mathbf{x})$ for any good testing subspace $v \in \mathcal{T}_D(\mathbf{x})$, whose existence is guaranteed by the fact that $\mathbf{x} \notin B'$. This is well-defined because if $v, v' \in \mathcal{T}_D(\mathbf{x})$ are both good, then it follows from the fact that $\mathbf{x} \notin B'$ that $c_v(\mathbf{x}) = c_{v'}(\mathbf{x})$.

**Claim 3.12.** *Let $w \in \mathcal{V}_D^2$ be a subspace in directions $A_1, A_2 \in D$. For each $i \in \{1,2\}$, $w$ contains less than $\frac{1}{2}\delta q^t$ decoding subspaces in direction $A_i$ which intersect $B'$ or are bad (not contained in any good testing subspace).*

*Proof.* By symmetry, it suffices to consider $i = 2$. Let $A_3, \ldots, A_n \in D$ be blocks in some other direction. Let $u_1, \ldots, u_k \subseteq w$ be decoding subspaces in direction $A_2$ such that, for each $j \in [k]$, $u_j$ intersects $B'$ or is bad. It suffices to exhibit, for each $j \in [k]$, a bad testing subspace $v \in \mathcal{T}_D$ containing $u_j$ which has block $A_2$ but not $A_1$. In this case we will show that $|v \cap w| \le q^{t+\ell}$ so each such bad testing subspace contain at most $q^\ell$ of the $u_i$-s. Since, by Claim 3.11, there are at most $\frac{1}{2}\delta q^{t-\ell}$ such subspaces, we get that $k \le \frac{1}{2}\delta q^t$. Indeed, since $D$ is $\ell$-proper, the subspace $u + v \in \mathcal{V}_D^n$ has dimension at least $m - \ell$. Therefore,

$$\dim(v \cap w) = \dim(v) + \dim(w) - \dim(v+w) \le m - t + 2t - (m-l) = t + l$$

and $|v \cap w| \le q^{t+\ell}$.

Fix $j \in [l]$ and $u \triangleq u_j$ and we will show that $u$ is contained in a bad testing subspace. If $u$ is bad, then we are done, since any testing subspace containing $u$, in particular the testing subspace in directions $A_2, \ldots, A_n$, is bad. Now suppose $u$ has a point $\mathbf{x} \in u \cap B'$. Let $v \in \mathcal{T}_D$ be the testing subspace $(\mathbf{x}, A_2 \cup \cdots \cup A_n)$. If $v$ is bad, we are done. Otherwise, since $\mathbf{x} \in B'$, there exists another good hyperplane $v' \in D$, in directions $A_1', \ldots, A_{n-1}'$, such that $c_v(\mathbf{x}) \ne c_{v'}(\mathbf{x})$. Without loss of generality, assume that if $A_i = A_j'$ then $i = j$ (in particular $A_1 \notin \{A_2', \ldots, A_{n-1}'\}$). For each $i \in [n-1]$, if $A_2 = A_2'$ define $v_i \in \mathcal{T}_D(\mathbf{x})$ to be the testing subspace $(\mathbf{x}, A_2', \ldots, A_i', A_{i+1}, \ldots, A_n)$, and if $A_2 \ne A_2'$ define $v_1$ to be $v$ and $v_i$ to be $(\mathbf{x}, A_2, A_2', \ldots, A_i', A_{i+1}, \ldots, A_{n-1})$. In any case define $v_n \triangleq v'$. For every $i \in [n-1]$, $v_i$ and $v_{i+1}$ are adjacent. Note that for every $i \in [n-1]$, $v_i$ contains the direction $A_2$ and does not contain the direction $A_1$. We will show that $v_i$ is bad for some $i \in [n-1]$. Since $c_{v_1}(\mathbf{x}) \ne c_{v_n}(\mathbf{x})$, there exists some $i \in [n-1]$ such that $c_{v_i}(\mathbf{x}) \ne c_{v_{i+1}}(\mathbf{x})$, and therefore, by Claim 3.9, one of $v_i, v_{i+1}$ is bad. If $i < n-1$, then $i, i+1 \le n-1$, and so we are done. If $i = n-1$, then by assumption $v_n = v'$ is good, so it must be that $v_{n-1}$ is bad. ☐

**Claim 3.13.** *If $u \in \mathcal{D}_D$ is a decoding subspace and $u \cap B' = \emptyset$, then for every $\mathbf{x} \in u$ there is a codeword $c_\mathbf{x} \in \mathcal{C}$ defined on $u$ such that $c_\mathbf{x}(\mathbf{x}) = c(\mathbf{x})$ and $\delta(c_\mathbf{x}, c|_u) < \frac{\delta}{2}$. In particular, $c|_u \in \mathcal{C}$.*

*Proof.* Fix $\mathbf{x} \in u$. Let $A = \{\mathbf{a}_1, \ldots, \mathbf{a}_t\} \in D$ be the directions of $u$. Since $\mathbf{x} \notin B'$, there is a good testing subspace $v \in \mathcal{T}_D(\mathbf{x})$. Let $A' = \{\mathbf{a}_1', \ldots, \mathbf{a}_t'\}$ be some block in $v$ not equal to $A$ and consider the subspace $w = (\mathbf{x}, A \cup A') \in \mathcal{V}_D^2$. For $\mathbf{s}, \mathbf{s}' \in \mathbb{F}_q^t$, let $w(\mathbf{s}, \mathbf{s}') \triangleq \mathbf{x} + \sum_{i=1}^t s_i \mathbf{a}_i + \sum_{i=1}^t s_i' \mathbf{a}_i'$. Let

$$w(\mathbf{s}, *) \triangleq \{w(\mathbf{s}, \mathbf{s}') \mid \mathbf{s}' \in \mathbb{F}_q^t\} \in \mathcal{D}_D$$

and

$$w(*, \mathbf{s}') \triangleq \{w(\mathbf{s}, \mathbf{s}') \mid \mathbf{s} \in \mathbb{F}_q^t\} \in \mathcal{D}_D$$

Let $I \subseteq \mathbb{F}_q^t \setminus \{\mathbf{0}\}$ be the set of points $\mathbf{s} \neq \mathbf{0}$ such that $w(\mathbf{s}, *)$ intersects $B'$ or is bad. Similarly, let $I' \subseteq \mathbb{F}_q^t \setminus \{\mathbf{0}\}$ be the set of points $\mathbf{s}' \neq \mathbf{0}$ such that $w(*, \mathbf{s}')$ intersects $B'$ or is bad. By Claim 3.12, $|I|, |I'| < \frac{1}{2}\delta q^t$. Note that for each $(\mathbf{s}, \mathbf{s}') \in (\mathbb{F}_q^t \setminus I) \times (\mathbb{F}_q^t \setminus I')$, we have $w(\mathbf{s}, \mathbf{s}') \notin B'$: if $\mathbf{s} \neq \mathbf{0}$ or $\mathbf{s}' \neq \mathbf{0}$, this follows from the definition of $I$ and $I'$; if $\mathbf{s} = \mathbf{s}' = \mathbf{0}$, then $w(\mathbf{s}, \mathbf{s}') = \mathbf{x} \notin B'$. Thus $c$ is defined on $w((\mathbb{F}_q^t \setminus I) \times (\mathbb{F}_q^t \setminus I'))$. Note that for each $\mathbf{s} \in \mathbb{F}_q^t \setminus I$, the decoding subspace $w(\mathbf{s}, *)$ is good and hence contained in a good testing subspace $v_{\mathbf{s}} \in \mathcal{T}_D$, therefore $c_{v_{\mathbf{s}}}|_{w(\mathbf{s},*)} \in \mathcal{C}$. Similarly, for each $\mathbf{s}' \in \mathbb{F}_q^t \setminus I'$, the decoding subspace $w(*, \mathbf{s}')$ is contained in a good testing subspace $v_{\mathbf{s}'} \in \mathcal{T}_D$, hence $c_{v_{\mathbf{s}'}}|_{w(*,\mathbf{s}')} \in \mathcal{C}$. Since $|I|, |I'| < \frac{1}{2}\delta q^t$, by Proposition 2.15, $c$ can be extended uniquely into $c_w \in \mathcal{C}^{\otimes 2}$ defined on $w$. Define $c_{\mathbf{x}} \triangleq c_w|_u$. Note that $c_{\mathbf{x}} \in \mathcal{C}$ since it is the restriction of $c_w \in \mathcal{C}^{\otimes 2}$ to $u = w(*, \mathbf{0})$. Also, if $\mathbf{s} \in \mathbb{F}_q^t \setminus I$, then $c|_{w(\mathbf{s},*)} = c_{v_{\mathbf{s}}}|_{w(\mathbf{s},*)} = c_w|_{w(\mathbf{s},*)}$ and in particular, $c(w(\mathbf{s}, \mathbf{0})) = c_w(w(\mathbf{s}, \mathbf{0})) = c_{\mathbf{x}}(w(\mathbf{s}, \mathbf{0}))$. So $\delta(c, c_{\mathbf{x}}) \leq \frac{|I|}{q^t} < \frac{\delta}{2}$. Finally, since $\mathbf{0} \notin I, I'$, we have $c(\mathbf{x}) = c(w(\mathbf{0}, \mathbf{0})) = c_{\mathbf{x}}(w(\mathbf{0}, \mathbf{0})) = c_{\mathbf{x}}(\mathbf{x})$. This proves the first part of the claim.

For the second part (showing $c|_u \in \mathcal{C}$), fix some $\mathbf{x}_0 \in u$. For each $\mathbf{x} \in u$, let $c_{\mathbf{x}}$ be the codeword guaranteed by the previous part. Then, for every $\mathbf{x} \in u$, $\delta(c_{\mathbf{x}_0}, c_{\mathbf{x}}) \leq \delta(c_{\mathbf{x}_0}, c|_u) + \delta(c|_u, c_{\mathbf{x}}) < \delta$, therefore $c_{\mathbf{x}_0} = c_{\mathbf{x}}$. Moreover, for all $\mathbf{x} \in u$, $c_{\mathbf{x}_0}(\mathbf{x}) = c_{\mathbf{x}}(\mathbf{x}) = c(\mathbf{x})$, so $c|_u = c_{\mathbf{x}_0} \in \mathcal{C}$. □

We proceed to define $c(\mathbf{x})$ for $x \in B'$. For such an $\mathbf{x}$, pick any decoding subspace $u \in \mathcal{D}_D(\mathbf{x})$, extend $c|_{u \setminus B'}$ to a codeword $c_u \in \mathcal{C}$, and define $c(\mathbf{x}) \triangleq c_u(\mathbf{x})$. We now argue that this is well-defined. Suppose $u_1, u_2 \in \mathcal{D}_D(\mathbf{x})$ in directions $A_1, A_2 \in D$, respectively. We need to show that $c_{u_1}, c_{u_2}$ are well-defined and that $c_{u_1}(\mathbf{x}) = c_{u_2}(\mathbf{x})$. Let $w \in \mathcal{V}_D^2$ be the unique subspace containing $u_1, u_2$, so $w = (\mathbf{x}, A_1 \cup A_2)$. By Claim 3.12, in each direction $A_1, A_2$, there are less than $\frac{1}{2}\delta q^t$ decoding subspaces in that direction in $w$ which intersect $B'$. In particular, this implies that $u_1, u_2$ each contain less than $\delta q^t$ points from $B'$. By what we just showed, there are sets $J_1, J_2 \subseteq \mathbb{F}_q^t$ of size $|J_1|, |J_2| > (1 - \delta)q^t$ such that the "sub-rectangle" $R \triangleq w(J_1 \times J_2)$ contains no points from $B'$, and therefore $c$ has already been defined on $R$. By Claim 3.13, on each decoding subspace $u$ in $R$ in either direction $A_1$ or $A_2$, $c|_u \in \mathcal{C}$. Applying Proposition 2.15, we see that $c|_R$ can be uniquely extended to a tensor codeword $c_w \in \mathcal{C}^{\otimes 2}$ on $w$, and this gives a way to extend $c|_{u_i \setminus B'}$ to the codeword $c_{u_i} \triangleq c_w|_{u_i} \in \mathcal{C}$ for $i \in \{1, 2\}$. Therefore, the extensions $c_{u_1}, c|_{u_2}$ agree on $\mathbf{x}$ since $c_{u_1}(\mathbf{x}) = c_w(\mathbf{x}) = c_{u_2}(\mathbf{x})$, and moreover for each decoding subspace $u_i$ this extension is unique since each decoding subspace has less than $\delta q^t$ points from $B'$.

Now that we have defined $c : \mathbb{F}_q^m \to \mathbb{F}_q$ and have shown that $\delta(r, c) \leq \rho\binom{|D|}{n-1}$, it only remains to show that $c \in \mathcal{C}_D^n$. Let $u \in \mathcal{D}_D$ be a decoding subspace. If $u \cap B' = \emptyset$, then $c|_u \in \mathcal{C}$ follows from Claim 3.13. If $u$ intersects $B'$, by the way we defined $c(\mathbf{x})$ for $\mathbf{x} \in B'$, we showed that for any decoding subspace $u$ through $\mathbf{x} \in B'$, $c|_u \in \mathcal{C}$ by extending $c|_{u \setminus B'}$ to a codeword.

□

**Claim 3.14.** *Let $\ell \leq t$ be a natural number and $A_1, \ldots, A_n \in \binom{\mathbb{F}_q^m}{t}$ be such that their union is linearly independent. Then at least $1 - \binom{n}{2}\frac{q^{-t}}{q-1} - n\frac{q^{-\ell}}{q-1}$ fraction of $A \in \binom{\mathbb{F}_q^m}{t}$ satisfy that $A, A_1, \ldots, A_n$ is $\ell$-proper.*

*Proof.* Let $\mathbf{a}_1, \ldots, \mathbf{a}_t$ be the random elements comprising $A$. By a union bound, it suffices to show for any $S \in \binom{[n]}{n-2}$ that $\left(\bigcup_{i \in S} A_i\right) \cup A$ is linearly independent with probability at least $1 - \frac{q^{-t}}{q-1}$ and

for any $T \in \binom{[n]}{n-1}$ the probability that $\left(\bigcup_{i\in T} A_i\right) \cup A$ contains at least $m-\ell$ linearly independent elements is at least $1 - \frac{q^{-\ell}}{q-1}$.

Fix $S \in \binom{[n]}{n-2}$ .For any $j \in [t]$, the probability that $\mathbf{a}_j \in \mathbb{F}_q^m$ is in the span of $\left(\bigcup_{i\in S} A_i\right) \cup \{\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}\}$, conditioned on the event that the latter is linearly independent, is $\frac{q^{m-2t+j-1}}{q^m} = q^{-2t+j-1}$. So the probability that $\left(\bigcup_{i\in S} A_i\right) \cup A$ is linearly independent is

$$\begin{aligned}\prod_{j=1}^{t}\left(1-q^{-2t+j-1}\right) &\geq 1-\sum_{j=1}^{t} q^{-2t+j-1} \\ &\geq 1-q^{-t}\sum_{j=1}^{\infty} q^{-j} \\ &= 1-\frac{q^{-t}}{q-1}.\end{aligned}$$

Now fix $T \in \binom{[n]}{n-1}$. Similarly, The probability that $a_j \in \left(\bigcup_{i\in T} A_i\right) \cup \{\mathbf{a}_1, \ldots, \mathbf{a}_{j-1}\}$, condition on the event that the later linearly independent is $q^{-t+j-1}$. So we get that $\left(\bigcup_{i\in S} A_i\right) \cup \{\mathbf{a}_1, \ldots, \mathbf{a}_{t-\ell}\}$ are linearly independent is

$$\begin{aligned}\prod_{j=1}^{t-\ell}\left(1-q^{-t+j-1}\right) &\geq 1-\sum_{j=1}^{t-\ell} q^{-t+j-1} \\ &\geq 1-q^{-\ell}\sum_{j=1}^{\infty} q^{-j} \\ &= 1-\frac{q^{-\ell}}{q-1}.\end{aligned}$$

□

### 3.3 Robustness for large dimension

In this section, we prove our main result:

**Theorem 3.15.** *Let $\rho \triangleq \mathbb{E}_v[\delta(r|_v, \mathcal{C}^{t\nearrow 2t})]$, where $v$ is a random affine subspace of dimension $2t$. Let $\alpha_1$ be the $2t$-dimensional robustness of $\mathcal{C}^{t\nearrow 4t}$ given by Corollary 3.7. If $\rho < \frac{\alpha_1\delta^3}{400} - 3q^{-t}$, then $\rho \geq \left(1-\frac{\delta}{4}\right)\cdot\delta(r, \mathcal{C}^{t\nearrow m})$. In particular, $\mathcal{C}^{t\nearrow m}$ is $(\alpha_2, 2t)$-robust, where $\alpha_2 \geq \frac{\delta^{72}}{2\cdot 10^{52}}$.*

**Notation.** Throughout Section 3.3, fix the received word $r : \mathbb{F}_q^m \to \mathbb{F}_q$ and $\rho \triangleq \mathbb{E}_v[\delta(r|_v, \mathcal{C}^{t\nearrow 2t})]$, and we will assume that $0 < \rho < \frac{\alpha_1\delta^3}{400} - 3q^{-t}$. The case where $\frac{\alpha_1\delta^3}{400} > 3q^{-t}$ is easily dealt with at the end of the proof by using Corollary 2.9. Note that, since $\alpha_1, \delta \leq 1$, this implies $q^{-t} \leq \frac{\delta}{1200}$. Throughout this section we will assume $m \geq 4t$. If $m < 4t$ we can pad the function $f$ to get a function $\hat{f} : \mathbb{F}_q^{4t} \to \mathbb{F}_q$ (by setting $\hat{f}(\mathbf{x}, \mathbf{y}) = f(\mathbf{x})$ for every $\mathbf{x} \in \mathbb{F}_q^m$ and $\mathbf{y} \in \mathbb{F}_q^{4t-m}$) and applying our tester to $\hat{f}$. We will typically use $u, v, w$ to denote affine subspaces of dimension $t$, $2t$, and $4t$ respectively. For any affine subspace $A \subseteq \mathbb{F}_q^m$, let $c_A \in \mathcal{C}^{t\nearrow \dim(A)}$ be the codeword nearest

to $r|_A$, breaking ties arbitrarily. Let $\rho_A \triangleq \mathbb{E}_{v \subseteq A}[\delta(r|_v, \mathcal{C}^{t \nearrow 2t})]$, where the expectation is taken over uniformly random $2t$-dimensional subspaces $v \subseteq A$. Fix the following constants:

$$\begin{aligned} \gamma &\triangleq \frac{\alpha_1 \delta^2}{40} - \alpha_1 q^{-t} \\ \epsilon &\triangleq \frac{\rho + 2q^{-t}}{\gamma}. \end{aligned}$$

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

$$\begin{aligned} 20\delta^{-1}(\alpha_1^{-1}\gamma + q^{-t}) &\leq \frac{\delta}{2} \\ \epsilon &\leq \frac{\delta}{10}. \end{aligned}$$

**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]. For simplicity, assume $t = 1$. 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 $\mathcal{C}^{1 \nearrow m}$. The definition of $c$ is simple: for every $\mathbf{x} \in \mathbb{F}_q^m$, consider the opinion $c_u(\mathbf{x})$ for every line $u$ 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 3.18) of this section shows that most lines agree with each other, so $c$ is well-defined. Lemma 3.18 uses Claim 3.16, which shows that for a 4-dimensional affine subspace $w$, if $\rho_w$ is small, then for every $\mathbf{x} \in w$, most lines $u \subseteq w$ satisfy $c_u(\mathbf{x}) = c_w(\mathbf{x})$. To prove Claim 3.16 we use the results of Section 3.1, in particular the robustness of the plane test in $m = 4$ dimensions (Corollary 3.7). Since the average $\delta(r|_u, c_w|_u)$ over $u$ 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 $\rho_w$ is small. Therefore, for most $u$, $\delta(r|_u, c_w|_u)$ is small and so it must be that $c_u = c_w|_u$.

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

**Claim 3.16.** *If $w \subseteq \mathbb{F}_q^m$ be a $4t$-dimensional affine subspace with $\rho_w \leq \gamma$, then for every $\mathbf{x} \in w$, at least $1 - \frac{\delta}{20}$ fraction of $t$-dimensional subspaces $u \subseteq w$ satisfy $c_u(\mathbf{x}) = c_w(\mathbf{x})$.*

*Proof.* Fix $\mathbf{x} \in w$. Let $U$ be the set of $t$-dimensional subspaces $u$ containing $\mathbf{x}$ such that $\delta(r|_u, c_w|_u) < 20\delta^{-1}(\alpha_1^{-1}\rho_w + q^{-t})$. By Corollary 3.7, $\mathbb{E}_{\substack{u \subseteq w \\ u \ni \mathbf{x}}}[\delta(r|_u, c_w|_u)] \leq \delta(r|_w, c_w) + q^{-t} \leq \alpha_1^{-1}\rho_w + q^{-t}$, so by Markov's inequality, the probability that $\delta(r|_u, c_w|_u) \geq 20\delta^{-1}(\alpha_1^{-1}\rho_w + q^{-t})$ is at most $\frac{\alpha_1^{-1}\rho_w + q^{-t}}{20\delta^{-1}(\alpha_1^{-1}\rho_w + q^{-t})} = \frac{\delta}{20}$. For $u \in U$, since $\delta(r|_u, c_w|_u) < 20\delta^{-1}(\alpha_1^{-1}\rho_w + q^{-t}) \leq \frac{\delta}{2}$ and $c_w|_u \in \mathcal{C}$, we have $c_u = c_w|_u$ and therefore $c_u(\mathbf{x}) = c_w(\mathbf{x})$. ∎

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

*Proof.* Observe that

$$\begin{aligned}
\rho &= \mathbb{E}_v \left[ \delta\left( r|_v, \mathcal{C}^{t \nearrow 2t} \right) \right] \\
&\geq \mathbb{E}_{v : u \cap v = \emptyset} \left[ \delta\left( r|_v, \mathcal{C}^{t \nearrow 2t} \right) \right] \cdot \Pr_v[u \cap v = \emptyset] \\
\text{(Lemma 2.16)} \quad &\geq \mathbb{E}_{v : u \cap v = \emptyset} \left[ \delta\left( r|_v, \mathcal{C}^{t \nearrow 2t} \right) \right] \cdot \left( 1 - q^{-(m-3t)} \right).
\end{aligned}$$

Therefore,

$$\begin{aligned}
\mathbb{E}_{w \supseteq u}[\rho_w] &= \mathbb{E}_{w \supseteq u} \left[ \mathbb{E}_{v \subseteq w} \left[ \delta(r|_v, \mathcal{C}^{t \nearrow 2t}) \right] \right] \\
&\leq \mathbb{E}_{w \supseteq u} \left[ \mathbb{E}_{v \subseteq w} \left[ \delta(r|_v, \mathcal{C}^{t \nearrow 2t}) \;\middle|\; u \cap v = \emptyset \right] + \Pr_{v \subseteq w}[u \cap v \neq \emptyset] \right] \\
\text{(Lemma 2.16)} \quad &\leq \mathbb{E}_{w \supseteq u} \left[ \mathbb{E}_{v \subseteq w} \left[ \delta(r|_v, \mathcal{C}^{t \nearrow 2t}) \;\middle|\; u \cap v = \emptyset \right] \right] + q^{-t} \\
&= \mathbb{E}_{v : u \cap v = \emptyset}[\delta(r|_v, \mathcal{C}^{t \nearrow 2t})] + q^{-t} \\
&\leq \frac{\rho}{1 - q^{-(m-3t)}} + q^{-t} \\
&\leq \rho + 2q^{-t}
\end{aligned}$$

□

**Lemma 3.18** (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 $t$-dimensional affine subspaces through $\mathbf{x}$, such that $c_u(\mathbf{x}) = c_{u'}(\mathbf{x})$ for every $u, u' \in U_1$.*

*Proof.* Let $U$ be the set of all $t$-dimensional affine subspaces $u$ 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 $c_u(\mathbf{x})$. We will show that $\Pr_{u \ni x}[u \in U_1] \geq 1 - \frac{\delta}{5} - \frac{\delta}{600}$. For every $4t$-dimensional subspace $w$, let $U_w$ be the collection of

$t$-dimensional subspaces $u$ through $\mathbf{x}$, guaranteed by Claim 3.16, satisfying $c_u(\mathbf{x}) = c_w(\mathbf{x})$. Then

$$\begin{aligned}
\Pr_{u \ni \mathbf{x}}[u \in U_1] &\geq \Pr_{u,u' \ni \mathbf{x}}[\exists i \;\; u, u' \in U_i] \\
&= \Pr_{u,u' \ni \mathbf{x}}[c_u(\mathbf{x}) = c_{u'}(\mathbf{x})] \\
\text{(Lemma 2.17)} \quad &\geq \Pr_{u \cap u' = \{\mathbf{x}\}}[c_u(\mathbf{x}) = c_{u'}(\mathbf{x})] - q^{-(m-2t)} \\
&= \mathbb{E}_{w \ni \mathbf{x}}\left[\Pr_{\substack{u,u' \subseteq w \\ u \cap u' = \{\mathbf{x}\}}}[c_u(\mathbf{x}) = c_{u'}(\mathbf{x})]\right] - q^{-(m-2t)} \\
\text{(Lemma 2.17)} \quad &\geq \mathbb{E}_{w \ni \mathbf{x}}\left[\Pr_{\substack{u,u' \subseteq w \\ u,u' \ni \mathbf{x}}}[c_u(\mathbf{x}) = c_{u'}(\mathbf{x})\right] - q^{-2t} - q^{-(m-2t)} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}}\left[\Pr_{\substack{u,u' \subseteq w \\ u,u' \ni \mathbf{x}}}[c_u(\mathbf{x}) = c_{u'}(\mathbf{x})\right] - \frac{\delta}{600} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}}\left[\Pr_{\substack{u,u' \subseteq w \\ u,u' \ni \mathbf{x}}}[c_u(\mathbf{x}) = c_{u'}(\mathbf{x})] \;\middle|\; \rho_w \leq \gamma\right] \cdot \Pr_{w \ni \mathbf{x}}[\rho_w \leq \gamma] - \frac{\delta}{600} \\
&\geq \mathbb{E}_{w \ni \mathbf{x}}\left[\Pr_{\substack{u,u' \subseteq w \\ u,u' \ni \mathbf{x}}}[u, u' \in U_w] \;\middle|\; \rho_w \leq \gamma\right] \cdot \Pr_{w \ni \mathbf{x}}[\rho_w \leq \gamma] - \frac{\delta}{600} \\
\text{(Claim 3.16)} \quad &\geq \left(1 - \frac{\delta}{20}\right)^2 \cdot \Pr_{w \ni \mathbf{x}}[\rho_w \leq \gamma] - \frac{\delta}{600} \\
\text{(Markov)} \quad &\geq \left(1 - \frac{\delta}{20}\right)^2 \cdot \left(1 - \frac{\mathbb{E}_{w \ni \mathbf{x}}[\rho_w]}{\gamma}\right) - \frac{\delta}{600} \\
\text{(Claim 3.17)} \quad &\geq \left(1 - \frac{\delta}{20}\right)^2 \cdot \left(1 - \frac{\rho + 2q^{-t}}{\gamma}\right) - \frac{\delta}{600} \\
&\geq 1 - \frac{\delta}{10} - \frac{\rho + 2q^{-t}}{\gamma} - \frac{\delta}{600} \\
&= 1 - \frac{\delta}{10} - \epsilon - \frac{\delta}{600} \\
&\geq 1 - \frac{\delta}{5} - \frac{\delta}{600}
\end{aligned}$$

□

We are now ready to prove the main theorem.

*Proof of Theorem 3.15.* 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 $\mathcal{C}^{t \nearrow m}$. For $\mathbf{x} \in \mathbb{F}_q^m$, define $c(\mathbf{x}) \triangleq \text{Majority}_{u \ni \mathbf{x}}\{c_u(\mathbf{x})\}$, where the majority is

over $t$-dimensional affine subspaces $u$ through $\mathbf{x}$. Since $\frac{\delta}{5} + \frac{\delta}{600} < \frac{1}{2}$, it follows from Lemma 3.18 that $c$ is well-defined.

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

$$\begin{aligned}
\rho &= \mathbb{E}_v[\delta(r|_v, c_v)] \\
&\geq \mathbb{E}_u[\delta(r|_u, c_u)] \\
&= \mathbb{E}_u\left[\mathbb{E}_{\mathbf{x}\in u}\left[\mathbb{1}_{c_u(\mathbf{x})\neq r(\mathbf{x})}\right]\right] \\
&= \mathbb{E}_{\mathbf{x}}\left[\mathbb{E}_{u\ni\mathbf{x}}\left[\mathbb{1}_{c_u(\mathbf{x})\neq r(\mathbf{x})}\right]\right] \\
&\geq \mathbb{E}_{\mathbf{x}}\left[\mathbb{E}_{u\ni\mathbf{x}}\left[\mathbb{1}_{c_u(\mathbf{x})\neq r(\mathbf{x})}\right] \;\middle|\; c(\mathbf{x}) \neq r(\mathbf{x})\right] \cdot \Pr_{\mathbf{x}}[c(\mathbf{x}) \neq r(\mathbf{x})] \\
&\geq \mathbb{E}_{\mathbf{x}}\left[\Pr_{u\ni\mathbf{x}}[c_u(\mathbf{x}) = c(\mathbf{x})] \;\middle|\; c(\mathbf{x}) \neq r(\mathbf{x})\right] \cdot \delta(r, c) \\
\text{(Lemma 3.18)} \quad &\geq \left(1 - \frac{\delta}{4}\right) \cdot \delta(r, c).
\end{aligned}$$

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

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

Observe that for any $\mathbf{y} \in u$, picking a random $4t$-dimensional $w$ containing $u$ and then picking a random $t$-dimensional $u' \subseteq w$ through $\mathbf{y}$ that intersect $u$ only on $y$ is equivalent to picking a random $t$-dimensional $u'$ through $\mathbf{y}$ that intersect $u$ only on $y$ and then picking a random $4t$-dimensional $w$ containing both $u, u'$. Therefore, for any fixed $\mathbf{y} \in u$

$$\begin{aligned}
\mathbb{E}_{w\supseteq u}\left[\Pr_{\substack{u'\subseteq w\\ u'\ni\mathbf{y}}}[c_{u'}(\mathbf{y}) \neq c(\mathbf{y})]\right] &= \mathbb{E}_{\substack{w\supseteq u\\ u'\subseteq w, u'\ni\mathbf{y}}}\left[\mathbb{1}_{c_{u'}(\mathbf{y})\neq c(\mathbf{y})}\right] \\
&\leq \mathbb{E}_{\substack{w\supseteq u\\ u'\subseteq w, u'\ni\mathbf{y}}}\left[\mathbb{1}_{c_{u'}(\mathbf{y})\neq c(\mathbf{y})} \mid u \cap u' = \{\mathbf{y}\}\right] + \Pr_{\substack{w\supseteq u\\ u'\subseteq w, u'\ni\mathbf{y}}}\left[u \cap u' \neq \{\mathbf{y}\}\right] \\
\text{(Lemma 2.17)} \quad &\leq \mathbb{E}_{u'\ni\mathbf{y}}\left[\mathbb{1}_{c_{u'}(\mathbf{y})\neq c(\mathbf{y})} \mid u \cap u' = \{y\}\right] + q^{-2t} \\
\text{(Lemma 2.17)} \quad &\leq \mathbb{E}_{u'\ni\mathbf{y}}\left[\mathbb{1}_{c_{u'}(\mathbf{y})\neq c(\mathbf{y})}\right] + q^{-(m-2t)} + q^{-2t} \\
\text{(Lemma 3.18 and definition of } c) \quad &\leq \frac{\delta}{5} + \frac{\delta}{600} + 2q^{-2t} \leq \frac{\delta}{5} + \frac{\delta}{300} \leq \frac{\delta}{4}.
\end{aligned}$$

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

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

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

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

Finally, since $\mathbb{E}_{w \supseteq u}[\rho_w] \leq \rho + 2q^{-t}$ (by Claim 3.17), we have

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

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 $\mathbf{y} \in u$ is good, then $c_w(\mathbf{y}) = c(\mathbf{y})$. Indeed, since more than $1 - \frac{\delta}{2}$ fraction of points in $u$ are good, we have $\delta(c_w|_u, c|_u) < \frac{\delta}{2}$. Therefore $c_w|_u = c'_u$, and since $\mathbf{x}$ is good, we have $c(\mathbf{x}) = c_w(\mathbf{x}) = c'_u(\mathbf{x})$ as desired. It remains to prove that $c_w(\mathbf{y}) = c(\mathbf{y})$ for good $\mathbf{y} \in u$. By Claim 3.16, at least $1 - \frac{\delta}{20}$ fraction of $t$-dimensional $u' \subseteq w$ through $\mathbf{y}$ satisfy $c_{u'}(\mathbf{y}) = c_w(\mathbf{y})$. Since $\mathbf{y}$ is good, more than $\frac{\delta}{20}$ fraction of $t$-dimensional $u' \subseteq w$ through $\mathbf{y}$ satisfy $c_{u'}(\mathbf{y}) = c(\mathbf{y})$. Therefore, there must be some $t$-dimensional $u' \subseteq w$ through $\mathbf{y}$ which satisfies $c_w(\mathbf{y}) = c_{u'}(\mathbf{y}) = c(\mathbf{y})$.

Finally, for the robustness statement: if $q^{-t} \geq \frac{\delta^{24}}{10^{14}}$, then by Corollary 2.9, the robustness is at least $\frac{q^{-3t}}{2} \geq \frac{\delta^{72}}{2 \cdot 10^{52}}$. Otherwise, the robustness is at least $\frac{\alpha_1 \delta^3}{57{,}600 \cdot 400} - 3q^{-t} \geq \frac{\delta^{24}}{2 \cdot 10^{14}}$. □

# 4 Low-degree testing

In this section, we prove Theorem 4.2, which is simply a more precise restatement of Theorem 1.3. We do so by proving Theorem 4.1, a generalization from which Theorem 4.2 follows immediately. Theorem 4.1 replaces the Reed-Solomon code with an arbitrary univariate linear affine-invariant code $\mathcal{C}_0$ and replaces the bivariate Reed-Muller code with an arbitrary $t$-variate linear affine-invariant code $\mathcal{C}_1$ which is a strict subcode of $(\mathcal{C}_0)^{1 \nearrow t}$.

**Theorem 4.1.** *Let $t > 1$ and let $m \geq 3$. Let $\mathcal{C}_0 \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ and $\mathcal{C}_1 \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be linear affine-invariant codes such that $\mathcal{C}_1 \subsetneq (\mathcal{C}_0)^{1 \nearrow t}$. Let $\delta \triangleq \delta(\mathcal{C}_0)$. Fix $r : \mathbb{F}_q^m \to \mathbb{F}_q$. Let $\rho \triangleq \mathbb{E}_u[\delta(r|_u, \mathcal{C}_1)]$, where the expectation is taken over random $t$-dimensional $u \subseteq \mathbb{F}_q^m$. Let $\alpha_2$ be the $t$-dimensional robustness of $(\mathcal{C}_0)^{1 \nearrow m}$. Then $\rho \geq \min\left\{\frac{\alpha_2 \delta^2}{4}, \left(\frac{\delta}{2} - 2q^{-1}\right) \cdot \frac{\delta}{2}\right\} \cdot \delta(r, (\mathcal{C}_1)^{t \nearrow m})$.*

**Theorem 4.2 (Robust plane testing for Reed-Muller).** *Let $m \geq 3$. Fix a positive constant $\delta > 0$ and a degree $d = (1 - \delta) \cdot q$. Let $\mathrm{RM}(m)$ be the $m$-variate Reed-Muller codes of degree $d$ over $\mathbb{F}_q$. Then $\mathrm{RM}(m)$ is $\left(\frac{\delta^{74}}{8 \cdot 10^{52}}, 2\right)$-robust.*

*Proof.* Let RS be the Reed-Solomon code over $\mathbb{F}_q$ of degree $d$. Let $p$ be the characteristic of $q$. Let $\alpha_1$ be the 2-dimensional robustness of $\mathrm{RS}^{1\nearrow m}$. Then $\alpha_2 \geq \frac{\delta^{72}}{2\cdot 10^{52}}$ by Theorem 3.1 if $m = 3$, and by Theorem 3.15 if $m \geq 4$.

If $d < q - q/p - 1$, then $\mathrm{RM}(m) = \mathrm{RS}^{1\nearrow m}$, and so in this case the theorem follows immediately from Theorem 3.15. If $d \geq q - q/p$ and $q \geq \frac{8}{\delta}$, then $\mathrm{RM}(2) \subsetneq \mathrm{RS}^{1\nearrow 2}$ but $\mathrm{RM}(m) = \mathrm{RM}(2)^{2\nearrow m}$, and so in this case the theorem follows immediately from Theorem 4.1, with $\mathcal{C}_0 = \mathrm{RS}$, $t = 2$, and $\mathcal{C}_1 = \mathrm{RM}(2)$. If $q < \frac{8}{\delta}$ then the theorem follows from Corollary 2.9. ☐

**Overview of Proof of Theorem 4.1.** We illustrate the idea for the case where $t = 2$, $\mathcal{C}_0$ is the Reed-Solomon code, and $\mathcal{C}_1$ is the bivariate Reed-Muller code of the same degree. The generalization to arbitrary $t$ and codes $\mathcal{C}_0, \mathcal{C}_1$ is straightforward. If $r$ is far from the lifted code, then on random planes $r$ will be far from the bivariate lifted code and hence also from the bivariate Reed-Muller code. So the remaining case is when $r$ is close to the lifted code. If the nearest function is a Reed-Muller codeword, then the theorem follows from the robustness of the lifted code. Otherwise, if the nearest function $c$ is not Reed-Muller, then we show (through Corollary 5.9) that on many planes $c$ is not a bivariate Reed-Muller codeword, and so $r$ (being close to $c$) is not close to a bivariate Reed-Muller codeword (by the distance of the code).

*Proof of Theorem 4.1.* Observe that, since $(\mathcal{C}_1)^{t\nearrow m} \subset (\mathcal{C}_0)^{1\nearrow m}$, we have $\delta(r, (\mathcal{C}_0)^{1\nearrow m}) \leq \delta(r, (\mathcal{C}_1)^{t\nearrow m})$. If $\delta(r, (\mathcal{C}_0)^{1\nearrow m}) \geq \min\left\{\frac{\delta^2}{4}, \delta(r, (\mathcal{C}_1)^{t\nearrow m})\right\}$, then we are done since

$$\begin{aligned}
\rho &= \mathbb{E}_u\left[\delta\left(r|_u, \mathcal{C}_1\right)\right] \\
&\geq \mathbb{E}_u\left[\delta\left(r|_u, (\mathcal{C}_0)^{1\nearrow t}\right)\right] \\
&\geq \alpha_2 \cdot \delta(r, (\mathcal{C}_0)^{1\nearrow m}) \\
&\geq \alpha_2 \cdot \min\left\{\frac{\delta^2}{4}, \delta(r, (\mathcal{C}_1)^{t\nearrow m})\right\} \\
&\geq \frac{\alpha_2\delta^2}{4} \cdot \delta(r, (\mathcal{C}_1)^{t\nearrow m}).
\end{aligned}$$

Therefore, suppose $\delta(r, (\mathcal{C}_0)^{1\nearrow m}) < \min\left\{\frac{\delta^2}{4}, \delta(r, (\mathcal{C}_1)^{t\nearrow m})\right\}$. Let $f \in (\mathcal{C}_0)^{1\nearrow m}$ be the nearest codeword to $r$, so that $f \notin (\mathcal{C}_1)^{t\nearrow m}$ and $\delta(r, f) < \frac{\delta^2}{4}$. If $u$ is a $t$-dimensional subspace for which $f|_u \notin \mathcal{C}_1$, then, since $\mathcal{C}_1$ is a subcode of $(\mathcal{C}_0)^{1\nearrow t}$, $\delta(r|_u, \mathcal{C}_1) \geq \delta - \delta(r|_u, f|_u)$. Since

$$\mathbb{E}_u\left[\delta\left(r|_u, f|_u\right)\right] = \delta(r, f) < \frac{\delta^2}{4},$$

by Markov,

$$\Pr_u\left[\delta(r|_u, f|_u) \geq \frac{\delta}{2}\right] \leq \frac{\delta}{2}$$

By Corollary 5.9,

$$\Pr_u\left[f|_u \in \mathcal{C}_1\right] \leq 1 - \delta + 2q^{-1}.$$

By the union bound, it follows that for at least $\frac{\delta}{2} - 2q^{-1}$ fraction of the $t$-dimensional $u \subseteq \mathbb{F}_q^m$, it holds that

$$\delta(r|_u, \mathcal{C}_1) \geq \delta - \delta(r|_u, f|_u) \geq \frac{\delta}{2}.$$

Therefore,

$$\rho = \mathbb{E}_u\left[\delta\left(r|_u, \mathcal{C}_1\right)\right] \geq \left(\frac{\delta}{2} - 2q^{-1}\right) \cdot \frac{\delta}{2}.$$

□

# 5 Technical algebraic results

The purpose of this section is to prove Theorem 5.7 and its Corollaries 5.8 and 5.9. If we allow our robustness in Theorem 3.15 to depend on $t$, the dimension of the base code, then proving what we need for Theorem 5.7 is easy. However, removing the dependence on $t$ requires some new ideas, including the definition of a new operation ("degree lifting") on codes, and the analysis of the distance of degree lifted codes. In Section 5.1, we define degree lifting and analyze the degree lifted codes (Proposition 5.4). In Section 5.2, we prove Theorem 5.7 and its corollaries.

**Notation.** For any vector $\mathbf{a} = (a_1, \ldots, a_m) \in \mathbb{N}^m$, define $\|\mathbf{a}\| \triangleq \sum_{i=1}^m a_i$. For an integer $a = \sum_i a_i p^j$, $0 \leq a_i \leq p-1$, and integers $b_1, \ldots, b_m$, with $b_j = \sum_i b_{ji} p^i$, $0 \leq b_{ji} \leq p-1$, we say that $\mathbf{b} = (b_1, \ldots, b_m) \leq_p a$ if $\sum_j b_{ji} = a_i$ for every $i$. Moreover, let $\binom{a}{\mathbf{b}} \triangleq \frac{a!}{b_1! \cdots b_m!}$ denote the $m$-nomial coefficient, which is the coefficient of $\mathbf{X}^{\mathbf{b}}$ in $(X_1 + \cdots + X_m)^a$. If $\mathbf{B}$ is an $m \times n$ matrix, let $\mathbf{B}_{i*}$ be the $i$-th row of $\mathbf{B}$ and let $\mathbf{B}_{*j}$ be the $j$-th column of $\mathbf{B}$. If $\mathbf{a} = (a_1, \ldots, a_m)$, then we say $\mathbf{B} \leq_p \mathbf{a}$ if $\mathbf{B}_{i*} \leq_p a_i$ for each $i$, i.e. row-wise $p$-shadow.

## 5.1 Degree lift

In this section, we define the degree lift operation on codes with degree sets. The operation can be thought of as "Reed-Mullerization", in the sense that the degree lift of the Reed-Solomon code of degree $d$ is the Reed-Muller code of degree $d$. This resembles the degree lift operation of Ben-Sasson et al. [BGK+13] who defined a "Reed-Mullerization" for algebraic-geometry codes (in constrast, we want to define it for codes over $\mathbb{F}_q^m$ spanned by monomials).

**Definition 5.1** (Degree lift)**.** Let $\mathcal{C} \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ have degree set $\mathrm{Deg}(\mathcal{C})$. For positive integer $s \geq 1$, define the *$s$-wise degree lift* $\mathcal{C}(s) \subseteq \{\mathbb{F}_q^{ms} \to \mathbb{F}_q\}$ of $\mathcal{C}$ to be the code with degree set

$$\mathrm{Deg}(\mathcal{C}(s)) \triangleq \left\{ (\mathbf{d}_1, \ldots, \mathbf{d}_s) \in \{0, 1, \ldots, q-1\}^{m \times s} \;\middle|\; \sum_{j=1}^{s} \mathbf{d}_j \in \mathrm{Deg}(\mathcal{C}) \right\}.$$

Our goal with this definition is to prove Proposition 5.4, which says that the distance of $\mathcal{C}(s)$ is nearly the same as the distance of $\mathcal{C}$. One can show that $\delta(\mathcal{C}(s)) \geq \delta(\mathcal{C}) - mq^{-1}$ To do so, we will use the following fact.

**Proposition 5.2.** *Let $t, n \geq 1$ and let $m = nt$. Let $\mathcal{C}_0 \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be linear affine-invariant and let $\mathcal{C} \triangleq (\mathcal{C}_0)^{\otimes n}$. For each $i \in [n]$, let $\mathbf{X}_i = (X_{i1}, \ldots, X_{it})$. If $f(\mathbf{X}_1, \ldots, \mathbf{X}_n) \in \mathcal{C}$, and $A_1, \ldots, A_n : \mathbb{F}_q^t \to \mathbb{F}_q^t$ are affine transformations, then $f(A_1(\mathbf{X}_1), \ldots, A_n(\mathbf{X}_n)) \in \mathcal{C}$.*

*Proof.* By linearity, it suffices to consider the case where $f(\mathbf{X}_1, \ldots, \mathbf{X}_n) = \prod_{i=1}^n \mathbf{X}_i{}^{\mathbf{d}_i}$ is a monomial, where $\mathbf{d}_i = (d_{i1}, \ldots, d_{it}) \in \{0, 1, \ldots, q-1\}^t$. Each $\mathbf{X}_i{}^{\mathbf{d}_i} \in \mathcal{C}_0$, so by affine-invariance $A_i(\mathbf{X}_i)^{\mathbf{d}_i} \in \mathcal{C}_0$. Therefore, by Proposition 2.12, $f(A_1(\mathbf{X}_1), \ldots, A)_n(\mathbf{X}_n)) = \prod_{i=1}^n A_i(\mathbf{X}_i)^{\mathbf{d}_i} \in (\mathcal{C}_0)^{\otimes n} = \mathcal{C}$. □

**Overview.** To prove Proposition 5.4, we show, through Lemma 5.3, that there is a special subset of $m$-dimensional subspaces $A$, such that for any $f \in \mathcal{C}(s)$, $f|_A \in \mathcal{C}$. Then, we analyze the distance of from $f$ to the zero function by looking at the distance on a random special $m$-dimensional $A$. This will yield a distance of $\delta(\mathcal{C}(s)) \geq \delta(\mathcal{C}) - o(1)$ as long as the special subspaces sample $\mathbb{F}_q^m$ well. However, we require the $o(1)$ term to be $(nq^{-t})^{O(1)}$, otherwise we would not be able to remove the dependence on $t$ in the robustness of Theorem 3.15. In order to do so, we need to further assume that $\mathcal{C}$ is the tensor product $(\mathcal{C}_0)^n$ of some $t$-dimensional code $\mathcal{C}_0$ (which is satisfied by our use case).

We now describe the special subspaces we consider in Lemma 5.3. Label the variables of $\mathbb{F}_q^{ms} = \mathbb{F}_q^{nts}$ by $X_{cij}$, where $c \in [n]$, $i \in [t]$, $j \in [s]$. Let $Y_{ci}$, for $c \in [n]$, $i \in [t]$, be the variables parameterizing $A$. Note that an arbitrary subspace restriction corresponds to substituting, for each $X_{cij}$, an affine function of all of the variables $Y_{11}, \ldots, Y_{nt}$. This is too much to hope for. However, if we substitute for $X_{cij}$ an affine function of just $Y_{c1}, \ldots, Y_{ct}$, this works.

**Lemma 5.3.** *Let $t, n \geq 1$ and $m = nt$. Let $\mathcal{C}_0 \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be linear affine-invariant and let $\mathcal{C} \triangleq (\mathcal{C}_0)^{\otimes n}$. Let $s \geq 1$, and let $f(\mathbf{X}) \in \mathcal{C}(s)$, with variables $\mathbf{X} = (X_{cij})_{c\in[n],i\in[t],j\in[s]}$. Let $g(Y_{11}, \ldots, Y_{nt})$ be the $m$-variate polynomial obtained from $f(\mathbf{X})$ by setting, for each $c \in [n], i \in [t]$, and $j \in [s]$, $X_{cij} = \sum_{k=1}^t a_{cijk} Y_{ck} + b_{cij}$, for some $a_{cijk}, b_{cij} \in \mathbb{F}_q$. That is, for all $(c, i, j) \in [n] \times [t] \times [s]$ $X_{cij}$ is an affine function of $Y_{c1}, \ldots, Y_{ct}$. Then $g \in \mathcal{C}$.*

*Proof.* By linearity, it suffices to consider the case where $f(\mathbf{X}) = \prod_{c=1}^n \prod_{i=1}^t \prod_{j=1}^s X_{cij}^{d_{cij}}$ is a monomial, for some $0 \leq d_{cij} \leq q-1$. For each $j \in [s]$, define $\mathbf{d}_j \triangleq (d_{11j}, \ldots, d_{ntj})$, so that $(\mathbf{d}_1, \ldots, \mathbf{d}_s) \in \mathrm{Deg}(\mathcal{C}(s))$, i.e. $\sum_{i=1}^s \mathbf{d}_i \in \mathrm{Deg}(\mathcal{C})$. Then

$$\begin{aligned} g(Y_{11}, \ldots, Y_{nt}) &= \prod_{c=1}^n \prod_{i=1}^t \prod_{j=1}^s \left( \sum_{k=1}^t a_{cijk} Y_{ck} + b_{cij} \right)^{d_{cij}} \\ &= \prod_{c=1}^n \prod_{i=1}^t \prod_{j=1}^s \sum_{\mathbf{e}_{cij} \leq d_{cij}} \binom{d_{cij}}{\mathbf{e}_{cij}} b_{cij}^{e_{cij0}} \prod_{k=1}^t a_{cijk}^{e_{cijk}} Y_{ck}^{e_{cijk}} \\ &= \sum_{\substack{\mathbf{e}_{cij} \leq_p d_{cij} \\ \forall\ i,j}} (\cdots) \prod_{c=1}^n \prod_{k=1}^t Y_{ck}^{\sum_{i=1}^t \sum_{j=1}^s e_{cijk}} \end{aligned}$$

where the $(\cdots)$ denotes constants in $\mathbb{F}_q$. So, it suffices to show that each monomial of the form $\prod_{c=1}^n \prod_{k=1}^t Y_{ck}^{\sum_{i=1}^t \sum_{j=1}^n e_{cijk}} \in \mathcal{C}$, which we show in the remainder of the proof.

Let $h(Y_{11}, \ldots, Y_{nt})$ be the $m$-variate polynomial obtained from $f$ by substituting $X_{cij} = Y_{ci}$ for each $c \in [n]$, $i \in [t]$, $j \in [s]$. Then $h(Y_{11}, \ldots, Y_{nt}) = \prod_{c=1}^n \prod_{i=1}^t \prod_{j=1}^s Y_{ci}^{d_{cij}} = \prod_{c=1}^n \prod_{i=1}^t Y_{ci}^{\sum_{j=1}^s d_{cij}}$ is a monomial with degree $\left( \sum_{j=1}^s d_{11j}, \ldots, \sum_{j=1}^s d_{ntj} \right) = \sum_{j=1}^s \mathbf{d}_j \in \mathrm{Deg}(\mathcal{C})$, hence $h \in \mathcal{C}$. Now, consider applying an affine transformation as follows: for each $1 \leq c \leq n$ and each $1 \leq i \leq t$, substitute $Y_{ci} \leftarrow \sum_{k=1}^t \alpha_{cik} Y_{ck} + \beta_{ci}$, and call the new polynomial $h'$. By Proposition 5.2, $h' \in \mathcal{C}$.

On the other hand,

$$\begin{aligned}
h'(Y_1,\dots,Y_m) &= \prod_{c=1}^{n}\prod_{i=1}^{t}\left(\sum_{k=1}^{t}\alpha_{cik}Y_{ck}+\beta_{ci}\right)^{\sum_{j=1}^{s}d_{cij}} \\
&= \prod_{c=1}^{n}\prod_{i=1}^{t}\prod_{j=1}^{s}\left(\sum_{k=1}^{t}\alpha_{cik}Y_{ck}+\beta_{ci}\right)^{d_{cij}} \\
&= \prod_{c=1}^{n}\prod_{i=1}^{t}\prod_{j=1}^{s}\sum_{\mathbf{e}_{cij}\le_p d_{cij}}\binom{d_{cij}}{\mathbf{e}_{cijk}}\beta_{ci}^{e_{cij0}}\prod_{k=1}^{t}\alpha_{cik}^{e_{cijk}}Y_{ck}^{e_{cijk}} \\
&= \sum_{\substack{\mathbf{e}_{cij}\le_p d_{cij}\\ \forall\ c,i,j}}\left(\prod_{c,i,j}\binom{d_{cij}}{\mathbf{e}_{cijk}}\beta_{ci}^{e_{cij0}}\right)\prod_{c=1}^{n}\prod_{k=1}^{t}\left(\prod_{i=1}^{t}\alpha_{cik}^{\sum_{j=1}^{s}e_{cijk}}\right)Y_{ck}^{\sum_{i=1}^{t}\sum_{j=1}^{s}e_{cijk}}
\end{aligned}$$

and since the $\alpha_{cik}$ and the $\beta_{ci}$ are arbitrary and $\mathcal{C}$ has a degree set $\mathrm{Deg}(\mathcal{C}) = \mathrm{Deg}(\mathcal{C}_0)^n$, each monomial $\prod_{c=1}^{n-}\prod_{k=1}^{t}Y_{ck}^{\sum_{i=1}^{t}\sum_{j=1}^{n}e_{cijk}} \in \mathcal{C}$, as desired. □

**Proposition 5.4.** *Let $t, n \ge 1$ and $m = nt$. Let $\mathcal{C}_0 \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be linear affine-invariant and let $\mathcal{C} \triangleq (\mathcal{C}_0)^{\otimes n}$. For any positive integer $s \ge 1$, $\delta(\mathcal{C}(s)) \ge \delta(\mathcal{C}) - nq^{-t} = \delta(\mathcal{C}_0)^n - nq^{-t}$.*

*Proof.* Let $f(\mathbf{X}) \in \mathcal{C}(s)$ be a nonzero codeword with variables $\mathbf{X} = (X_{cij})_{c\in[n],i\in t],j\in[s]}$. For $c \in [n]$, $i \in [m]$, $j \in [s]$, $k \in [t]$, let $a_{cijk}, b_{cij} \in \mathbb{F}_q$, and let $\mathbf{a} \triangleq (a_{cijk})_{c\in[n],i\in[t],j\in[s],k\in[t]}$ and $\mathbf{b} \triangleq (b_{cij})_{c\in[n],i\in[t],j\in[s]}$. Let $g_{\mathbf{a},\mathbf{b}}(Y_{11},\dots,Y_{nt})$ be the $m$-variate polynomial obtained by setting $X_{cij} = \sum_{k=1}^{t} a_{cijk}Y_{ck} + b_{cij}$ for each $1 \le c \le n$ and $1 \le i \le t$.

By linearity of $\mathcal{C}$ and thus of $\mathcal{C}(s)$, it suffices to show that $\delta(f,0) \ge \delta(\mathcal{C}) - nq^{-t}$. Let $\mathbf{b} \in \mathbb{F}_q^{nts}$ be a point such that $f(\mathbf{b}) \ne 0$. Consider choosing $\mathbf{a}$ uniformly at random. Then $g_{\mathbf{a},\mathbf{b}} \ne 0$ since $g_{\mathbf{a},\mathbf{b}}(\mathbf{0}) = f(\mathbf{b}) \ne 0$. For fixed $y_{11},\dots,y_{nt}$, as long as for each $c \in [n]$ there is some $k \in [t]$ such that $y_{ck} \ne 0$, then the points $\sum_{k=1}^{t} a_{cijk}y_{ck} + b_{cij}$ are independent and uniform over $\mathbb{F}_q$. This occurs with probability at least $1 - nq^{-t}$. Therefore,

$$\begin{aligned}
\delta(\mathcal{C}) &\le \mathbb{E}_{\mathbf{a}}\left[\delta\left(g_{\mathbf{a},\mathbf{b}},0\right)\right] \\
&= \mathbb{E}_{\mathbf{a}}\left[\mathbb{E}_{\mathbf{y}}\left[\mathbb{1}_{g_{\mathbf{a},\mathbf{b}}(\mathbf{y})\ne 0}\right]\right] \\
&= \mathbb{E}_{\mathbf{y}}\left[\mathbb{E}_{\mathbf{a}}\left[\mathbb{1}_{g_{\mathbf{a},\mathbf{b}}(\mathbf{y})\ne 0}\right]\right] \\
&\le nq^{-t} + \mathbb{E}_{\mathbf{y}\ne\mathbf{0}}\left[\mathbb{1}_{g_{\mathbf{a},\mathbf{b}}(\mathbf{y})\ne 0}\right] \\
&= nq^{-t} + \mathbb{E}_{\mathbf{y}\ne\mathbf{0}}\left[\mathbb{1}_{f((\sum_{k=1}^{t} a_{cijk}y_{ck}+b_{cij}))\ne 0}\right] \\
&= nq^{-t} + \delta(f,0).
\end{aligned}$$

□

## 5.2 Analysis of subspace restrictions

In this section we prove Theorem 5.7 and its corollaries.

**Overview.** Corollary 5.8 says that if a codeword $f$ of the tensor product $\mathcal{C}^{\otimes n}$ of a $t$-dimensional code $\mathcal{C}$ is not a codeword of $\mathcal{C}^{t\nearrow nt}$, then on there is a point $\mathbf{b}$ such that on many $t$-dimensional subspaces $u$ through $\mathbf{b}$, the restriction $f|_u \notin \mathcal{C}$. We use this in the proof of Theorem 3.1 when arguing that if a tensor codeword $c \in \mathcal{C}^{\otimes m}$ satisfies $c \in \mathcal{C}_{\mathbf{a}}$ (see overview) for many $\mathbf{a}$, then $c \in \bigcap_{\mathbf{a}} \mathcal{C}_{\mathbf{a}} = \mathcal{C}^{1\nearrow m}$. A special case of Corollary 5.9 says that if $f$ is a lifted Reed-Solomon codeword but not a Reed-Muller codeword, then on many planes $f$ is not a bivariate Reed-Muller code. The actual corollary merely generalizes this to arbitrary $t$ and codes $\mathcal{C}_0, \mathcal{C}_1$.

Both Corollaries 5.8 and 5.9 are proved in a similar manner. Note that both are statements of the form "if $f$ is in some big code but not in a lifted code, then on many subspaces it is not a codeword of the base code". A natural approach is to write $f$ out as a linear combination of monomials, restrict to an arbitrary subspace of the appropriate dimension, re-write the restriction as a linear combination of monomials in the parameterizing variables, and note that the coefficients of the monomials are functions in the parameterization coefficients. Since $f$ is not in the lift, there is a monomial outside the base code whose coefficient (the "offending coefficient") is a nonzero function. Then, one shows that these functions belong to a code with good distance, so for many choices of parameterizing coefficients, the offending coefficient is nonzero.

Theorem 5.7 abstracts the above approach and shows that, in the case of Corollary 5.8, the offending coefficient is a codeword of the degree lift $(\mathcal{C}^{\otimes n})(t)$ of $\mathcal{C}^{\otimes n}$, and in the case of Corollary 5.9, the offending coefficient is a codeword of a lifted code. This necessitates the analysis of the distance of degree lifted codes, hence the need for Section 5.1.

Recall the following characterization of degree sets of lifts.

**Proposition 5.5.** *Let $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be a linear affine-invariant code. Then $\mathbf{d} = (d_1, \ldots, d_m) \in \mathrm{Deg}(\mathcal{C}^{t\nearrow m})$ if and only if, for every $m \times (t+1)$ matrix $\mathbf{E} \leq_p \mathbf{d}$, with rows $1, \ldots, m$ and columns $0, 1, \ldots, t$, it holds that $(\|\mathbf{E}_{*1}\| \bmod^* q, \ldots, \|\mathbf{E}_{*t}\| \bmod^* q) \in \mathrm{Deg}(\mathcal{C})$.*

**Lemma 5.6.** *Let $\mathcal{C} \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ be a linear code with a $p$-shadow-closed degree set. If $f \in \mathcal{C}$, and*

$$f\left(a_{10} + \sum_{j=1}^{t} a_{1j} Y_j, \ldots, a_{m0} + \sum_{j=1}^{t} a_{mj} Y_j\right) = \sum_{\mathbf{e} \in \{0,1,\ldots,q-1\}^t} f_{\mathbf{e}}(\mathbf{a}) \cdot \mathbf{Y}^{\mathbf{e}}$$

*where $\mathbf{a} = (a_{ij})_{1 \leq i \leq m; 0 \leq j \leq t} \in \mathbb{F}_q^{m(t+1)}$, then, for every $\mathbf{e} \in \{0, 1, \ldots, q-1\}^t$,*

$$f_{\mathbf{e}}(\mathbf{a}) = \sum_{\substack{\mathbf{d} \in D \\ \mathbf{E} \leq_p \mathbf{d} \\ \|\mathbf{E}_{*j}\| = e_j \ \forall j}} f_{\mathbf{d}} \cdot \prod_{i=1}^{m} \binom{d_i}{\mathbf{E}_{i*}} a_{i0}^{e_{i0}} \prod_{j=1}^{t} a_{ij}^{e_{ij}}.$$

*In particular,*

1. *$f_{\mathbf{e}} \in \mathcal{C}(t+1)$, the $(t+1)$-wise degree lift of $\mathcal{C}$ (see Definition 5.1);*
2. *if $\mathcal{C} = (\mathcal{C}_0)^{1\nearrow m}$ for some linear affine-invariant code $\mathcal{C}_0 \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$, then $f_{\mathbf{e}} \in (\mathcal{C}_0)^{1\nearrow m(t+1)}$*

*Proof.* Let $D$ be the degree set of $\mathcal{C}$. Write $f(\mathbf{X}) = \sum_{\mathbf{d}\in D} f_{\mathbf{d}} \cdot \mathbf{X}^{\mathbf{d}}$. Expanding, we get

$$\begin{aligned}
f\left(a_{10} + \sum_{j=1}^{t} a_{1j}Y_j, \ldots, a_{m0} + \sum_{j=1}^{t} a_{mj}Y_j\right) &= \sum_{\mathbf{d}\in D} f_{\mathbf{d}} \cdot \prod_{i=1}^{m} \left(a_{i0} + \sum_{j=1}^{t} a_{ij}Y_j\right)^{d_i} \\
&= \sum_{\mathbf{d}\in D} f_{\mathbf{d}} \cdot \prod_{i=1}^{m} \left(\sum_{\mathbf{e}_i \le_p d_i} \binom{d_i}{\mathbf{e}_i} a_{i0}^{e_{i0}} \cdot \prod_{j=1}^{t} a_{ij}^{e_{ij}} Y_j^{e_{ij}}\right) \\
&= \sum_{\mathbf{d}\in D} f_{\mathbf{d}} \cdot \sum_{\mathbf{E}\le_p \mathbf{d}} \left(\prod_{i=1}^{m} \binom{d_i}{\mathbf{E}_{i*}} a_{i0}^{e_{i0}} \prod_{j=1}^{t} a_{ij}^{e_{ij}}\right) \cdot \prod_{j=1}^{t} Y_j^{\|\mathbf{E}_{*j}\|} \\
&= \sum_{\mathbf{e}\in\{0,1,\ldots,q-1\}^t} \mathbf{Y}^{\mathbf{e}} \cdot \sum_{\substack{\mathbf{d}\in D \\ \mathbf{E}\le_p \mathbf{d} \\ \|\mathbf{E}_{*j}\| \bmod^* q = e_j \ \forall j}} f_{\mathbf{d}} \cdot \prod_{i=1}^{m} \binom{d_i}{\mathbf{E}_{i*}} a_{i0}^{e_{i0}} \prod_{j=1}^{t} a_{ij}^{e_{ij}}
\end{aligned}$$

and therefore, for each $\mathbf{e} \in \{0, 1, \ldots, q-1\}^t$,

$$f_{\mathbf{e}}(\mathbf{a}) = \sum_{\substack{\mathbf{d}\in D \\ \mathbf{E}\le_p \mathbf{d} \\ \|\mathbf{E}_{*j}\| \bmod^* q = e_j \ \forall j}} f_{\mathbf{d}} \cdot \prod_{i=1}^{m} \binom{d_i}{\mathbf{E}_{i*}} a_{i0}^{e_{i0}} \prod_{j=1}^{t} a_{ij}^{e_{ij}}.$$

View the variables $\mathbf{a} = (a_{ij})$ in the order $(a_{10}, \ldots, a_{m0}, \ \ldots \ , a_{1t}, \ldots, a_{mt})$, and interpret $\mathbf{E}$ as $(\mathbf{E}_{*0}, \ldots, \mathbf{E}_{*t})$. If $\mathbf{E} \le_p \mathbf{d}$ and $\mathbf{d} \in D = \mathrm{Deg}(\mathcal{C})$, then $\mathbf{E} \in \mathrm{Deg}(\mathcal{C}(t+1))$. Therefore, $f_{\mathbf{e}} \in \mathcal{C}(t+1)$.

Now suppose $\mathcal{C} = (\mathcal{C}_0)^{1\nearrow m}$ for some linear affine-invariant $\mathcal{C}_0 \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$. It suffices to show that if $\mathbf{d} = (d_1, \ldots, d_m) \in \mathrm{Deg}(\mathcal{C})$ and $\mathbf{E} \le_p \mathbf{d}$ with entries $e_{ij}$, $i \in [m]$, $0 \le j \le t$, then the length $m(t+1)$ vector $(\mathbf{E}_{*0}, \mathbf{E}_{*1}, \ldots, \mathbf{E}_{*t}) \in \mathrm{Deg}((\mathcal{C}_0)^{1\nearrow m(t+1)})$. By Proposition 5.5, it suffices to show that, if $u_{ij} \le_p e_{ij}$ for every $i \in [m]$ and $0 \le j \le t$, then $\sum_{ij} u_{ij} \bmod^* q \in \mathrm{Deg}(\mathcal{C}_0)$. Since $\mathbf{d} \in \mathrm{Deg}(\mathcal{C}) = \mathrm{Deg}((\mathcal{C}_0)^{1\nearrow m})$, this implies that if $e'_i \le_p d_i$ for $i \in [m]$, then $\sum_i e'_i \bmod^* q \in \mathrm{Deg}(\mathcal{C}_0)$. Set $e'_i \triangleq \sum_{j=0}^{t} u_{ij}$. Observe that, since $(e_{i0}, e_{i1}, \ldots, e_{it}) \le_p d_i$, this implies that $e'_i \le_p d_i$. Therefore, $\sum_{ij} u_{ij} \bmod^* q = \sum_i e'_i \bmod^* q \in \mathrm{Deg}(\mathcal{C}_0)$, as desired. ☐

**Theorem 5.7.** *Let $1 \le t < m$. Let $\mathcal{C}_1 \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be a linear affine-invariant code, and let $\mathcal{C}_2 \subseteq \{\mathbb{F}_q^m \to \mathbb{F}_q\}$ have a p-shadow-closed degree set. Suppose $f \in \mathcal{C}_2 \setminus {\mathcal{C}_1}^{t\nearrow m}$. Then the following hold:*

1. *if $\mathcal{C}_2 = (\mathcal{C}_0)^{\otimes n}$ for some linear affine-invariant code $\mathcal{C}_0 \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$, where $m = nt$, then there exists a point $\mathbf{b} \in \mathbb{F}_q^m$ such that for at least $\delta(\mathcal{C}_0)^n - (n+1)q^{-t}$ fraction of $t$-dimensional affine subspaces $A \subseteq \mathbb{F}_q^m$ passing through $\mathbf{b}$, the restriction $f|_A \notin \mathcal{C}_1$;*
2. *if $\mathcal{C}_2 = (\mathcal{C}_0)^{1\nearrow m}$ for some linear affine-invariant code $\mathcal{C}_0 \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$, then for at least $\delta(\mathcal{C}_0) - q^{-1}$ fraction of $t$-dimensional affine subspaces $A \subseteq \mathbb{F}_q^m$, the restriction $f|_A \notin \mathcal{C}_1$.*

*Proof.* Let $p$ be the characteristic of $\mathbb{F}_q$. Let $A$ be parameterized by $X_i = a_{i0} + \sum_{j=1}^{t} a_{ij}Y_j$, where the matrix $\{a_{ij}\}_{i=1,j=1}^{m,t} \in \mathbb{F}_q^{m\times t}$ has full rank. Write

$$f|_A(\mathbf{Y}) = \sum_{\mathbf{e}\in\{0,1,\ldots,q-1\}^t} f_{\mathbf{e}}(\mathbf{a}) \cdot \mathbf{Y}^{\mathbf{e}}.$$

Since $f \notin \mathcal{C}_1^m$, there exists $\mathbf{e} \notin \mathrm{Deg}(\mathcal{C}_1)$ such that $f_{\mathbf{e}} \neq 0$.

1. By Corollary 2.13, $\mathcal{C}_2$ has a $p$-shadow-closed degree set. By Lemma 5.6 (1), $f_{\mathbf{e}} \in \mathcal{C}_2(t+1)$. For each $\mathbf{b} = (b_1, \ldots, b_m) \in \mathbb{F}_q^m$, let $f_{\mathbf{e},\mathbf{b}}$ denote the polynomial $f_{\mathbf{e}}$ with the variable $a_{i0}$ fixed to value $b_i$ for each $i \in [m]$ (i.e. insisting that $A$ passes through $\mathbf{b}$). Observe that each $f_{\mathbf{e},\mathbf{b}} \in \mathcal{C}_2(t)$. Since $f_{\mathbf{e}} \neq 0$, there exists $\mathbf{b} \in \mathbb{F}_q^m$ such that $f_{\mathbf{e},\mathbf{b}} \neq 0$. By Proposition 5.4, for at least $\delta(\mathcal{C}_2(t)) \geq \delta(\mathcal{C}_0)^n - nq^{-t}$ fraction of matrices $\{a_{ij}\}_{i\in[m];j\in[t]}$, we have $f_{\mathbf{e},\mathbf{b}}(\{a_{ij}\}_{i\in[m];j\in[t]}) \neq 0$. Since, by Lemma 2.17, at least $1 - q^{t-m}$ fraction of such matrices have full rank, we get that for at least $\delta(\mathcal{C}_0)^n - nq^{-t} - q^{t-m} \geq \delta(\mathcal{C}_0)^n - (n+1)q^{-t}$ of the full rank matrices satisfy $f_{\mathbf{e},\mathbf{b}}\left(\{a_{ij}\}_{i=1,j=1}^{m,t}\right) \neq 0$ , and therefore $f|_A(\mathbf{Y}) \notin \mathcal{C}_1$.

2. By Proposition 2.4 it has a $p$-shadow-closed degree set. By Lemma 5.6 (2), $f_{\mathbf{e}} \in (\mathcal{C}_0)^{1\nearrow m(t+1)}$, so $f_{\mathbf{e}}(\mathbf{a}) \neq 0$ for at least $\delta((\mathcal{C}_0)^{1\nearrow m(t+1)}) \geq \delta(\mathcal{C}_0) - q^{-1}$ fraction of choices $\mathbf{a}$ (including such that the corresponding matrix does not have full rank), and therefore, by Lemma 2.17, $f|_A(\mathbf{Y}) \notin \mathcal{C}_1$ for at least $\delta(\mathcal{C}_0) - q^{-1} - q^{t-m} \geq \delta(\mathcal{C}_0) - 2q^{-1}$.

□

**Corollary 5.8.** *Let $t, n \geq 1$ and let $m = nt$. Let $\mathcal{C} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be a linear affine-invariant code. If $f \in \mathcal{C}^{\otimes n} \setminus \mathcal{C}^{t\nearrow m}$, then there is a point $\mathbf{b} \in \mathbb{F}_q^m$ such that for $\delta(\mathcal{C})^n - (n+1)q^{-t}$ fraction of $t$-dimensional subspaces $u$ through $\mathbf{b}$, the restriction $f|_u \notin \mathcal{C}$.*

*Proof.* Follows immediately from Theorem 5.7 (1) with $\mathcal{C}_0 = \mathcal{C}_1 = \mathcal{C}$, and $\mathcal{C}_2 = \mathcal{C}^{\otimes n}$. □

**Corollary 5.9.** *Let $1 \leq t \leq m$. Let $\mathcal{C}_0 \subseteq \{\mathbb{F}_q \to \mathbb{F}_q\}$ be a linear affine-invariant code. Let $\mathcal{C}_1 \subsetneq (\mathcal{C}_0)^{1\nearrow t}$ be a linear affine-invariant code that is a strict subcode of $(\mathcal{C}_0)^{1\nearrow t}$. If $f \in (\mathcal{C}_0)^{1\nearrow m} \setminus (\mathcal{C}_1)^{t\nearrow m}$, then for at least $\delta(\mathcal{C}_0) - 2q^{-1}$ fraction of $t$-dimensional subspaces $A \subseteq \mathbb{F}_q^m$, the restriction $f|_A \notin \mathcal{C}_1$.*

*Proof.* Follows immediately from Theorem 5.7 (2) with $\mathcal{C}_2 = (\mathcal{C}_0)^{1\nearrow m}$. □

## 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.

[BGK+13] Eli Ben-Sasson, Ariel Gabizon, Yohay Kaplan, Swastik Kopparty, and Shubhangi Saraf. A new family of locally correctable codes based on degree-lifted algebraic geometry codes. In Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors, *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 833–842. ACM, 2013.

[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.

[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.



ECCC ISSN 1433-8092

http://eccc.hpi-web.de