THEORY OF COMPUTING, Volume 11 (12), 2015, pp. 299–338
www.theoryofcomputing.org

SPECIAL ISSUE: APPROX-RANDOM 2013

# Absolutely Sound Testing of Lifted Codes

Elad Haramaty* Noga Ron-Zewi† Madhu Sudan

*Received September 11, 2013; Revised February 23, 2015; Published August 13, 2015*

**Abstract:** In this paper we present a strong analysis of the testability of a broad, and to date the most interesting known, class of "affine-invariant" codes. Affine-invariant codes are codes whose coordinates are associated with a vector space and in addition these codes are invariant under affine transformations of the coordinate space. Affine-invariant linear codes form a natural abstraction of algebraic properties such as linearity and low-degree, which have been of significant interest in theoretical computer science in the past. The study of affine-invariance is motivated in part by its relationship to property testing: affine-invariant linear codes tend to be locally testable under fairly minimal and almost necessary conditions.

Recent work by Ben-Sasson et al. (CCC 2011) and Guo et al. (ITCS 2013) introduced a new class of affine-invariant linear codes based on an operation called "lifting." Given a base code over a $t$-dimensional space, its $m$-dimensional lift consists of all words whose restriction to every $t$-dimensional affine subspace is a codeword of the base code. Lifting not only

An extended abstract of this paper appeared in the Proceedings of the 17th International Workshop on Randomization and Computation (RANDOM'13), pages 671-682, 2013.

*Research supported in part by NSF grant CCF-1319206. Research was mainly conducted while the author was an intern at Microsoft Research New-England, Cambridge, MA.

†Supported in part by the Rothschild fellowship and NSF grant CCF-1412958. Research was conducted in part while the author was visiting Microsoft Research New-England, Cambridge, MA, and supported in part by a scholarship from the Israel Ministry of Science and Technology. The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement number 257575.

**ACM Classification:** H.1.1, F.1.3

**AMS Classification:** 68W20, 68Q87

**Key words and phrases:** locally testable codes, affine-invariant codes, lifted codes, query complexity, soundness

 DOI: 10.4086/toc.2015.v011a012

captures the most familiar codes, which can be expressed as lifts of low-degree polynomials, it also yields new codes whose rate is better than that of the corresponding polynomial codes, and all other combinatorial qualities are no worse, when applied to "medium-degree" polynomials.

In this paper we show that codes obtained by lifting are also testable in an "absolutely sound" way. Specifically, we consider the natural test: Pick a random affine subspace of base dimension and verify that a given word is a codeword of the base code when restricted to the chosen subspace. While this test accepts codewords with probability one, we show that it rejects words at constant distance from the code with constant probability (depending only on the alphabet size). This work thus extends the results of Bhattacharyya et al. (FOCS 2010) and Haramaty et al. (FOCS 2011), while giving concrete new codes of higher rate that have absolutely sound testers. In particular, we show that there exist codes satisfying the requirements of Barak et al. (FOCS 2012) for constructing small-set expanders with a large number of eigenvalues close to the maximal one, with rate slightly higher than that of the codes used in their work.

# 1 Introduction

We present results on the testability of "affine-invariant linear codes." We start with some basic terminology before describing our work in greater detail.

Let $Q$ be a prime power, $Q$ be a power of $q$ and let $\mathbb{F}_q$ (and $\mathbb{F}_Q$) denote the finite fields of order $q$ (and $Q$, respectively). Finally, let $\{\mathbb{F}_Q^n \to \mathbb{F}_q\}$ denote the set of functions mapping $\mathbb{F}_Q^n$ to $\mathbb{F}_q$. In this work a code (or a family) will be a subset of functions $\mathcal{F} \subseteq \{\mathbb{F}_Q^n \to \mathbb{F}_q\}$. We use $\delta(f,g)$ to denote the normalized Hamming distance between $f$ and $g$, i. e., the fraction of inputs $x \in \mathbb{F}_Q^n$ for which $f(x) \neq g(x)$. We use $\delta(\mathcal{F})$ to denote $\min_{f \neq g, f,g \in \mathcal{F}}\{\delta(f,g)\}$ and $\delta_{\mathcal{F}}(f)$ to denote $\min_{g \in \mathcal{F}}\{\delta(f,g)\}$. A code $\mathcal{F}$ is said to be a linear code if it is an $\mathbb{F}_q$-subspace, i. e., for every $\alpha \in \mathbb{F}_q$ and $f,g \in \mathcal{F}$, we have $\alpha f + g \in \mathcal{F}$. A function $T : \mathbb{F}_Q^n \to \mathbb{F}_Q^n$ is said to be an affine transformation if there exists a matrix $B \in \mathbb{F}_Q^{n \times n}$ and vector $c \in \mathbb{F}_Q^n$ such that $T(x) = Bx + c$. The code $\mathcal{F} \subseteq \{\mathbb{F}_Q^n \to \mathbb{F}_q\}$ is said to be affine-invariant if for every affine transformation $T$ and every $f \in \mathcal{F}$ we have $f \circ T \in \mathcal{F}$ (where $(f \circ T)(x) = f(T(x))$).

When $Q = q$, affine-invariant linear codes form a very natural abstraction of the class of low-degree polynomials: the set of $n$-variate polynomials of degree at most $d$ over $\mathbb{F}_q$ is a linear subspace and is closed under affine transformations. Furthermore, as shown by Kaufman and Sudan [18], affine-invariant linear codes retain some of the "locality" properties of multivariate polynomial codes (or Reed-Muller codes), such as local testability and local decodability, that have found many applications in computational complexity. This has led to a sequence of papers exploring these codes, but most of this work produced codes of smaller rate than known ones, or gave an alternative understanding of known codes [12, 11, 6, 5, 4]. Recent work by Guo et al. [14], however, changes the picture significantly. They study a "lifting" operator on codes and show that it leads to codes with, in some cases dramatic, improvement in parameters compared to Reed-Muller codes. Our work complements theirs by showing that one family of "best-known" tests manages to work abstractly for codes developed by lifting.

We start by describing the lifting operation. Roughly speaking, a lifting of a base code leads to a code in more variables whose codewords are words of the base code on every affine subspace of the base dimension. We define this formally next. For $f : \mathbb{F}_Q^n \to \mathbb{F}_q$ and $S \subseteq \mathbb{F}_Q^n$, let $f|_S$ denote the restriction of $f$ to the set $S$. A set $A \subseteq \mathbb{F}_Q^n$ is said to be a $t$-dimensional affine subspace, if there exist $\alpha_0, \ldots, \alpha_t \in \mathbb{F}_Q^n$ such that

$$A = \left\{ \alpha_0 + \sum_{i=1}^{t} \alpha_i x_i \;\middle|\; x_1, \ldots, x_t \in \mathbb{F}_Q \right\}.$$

We use some arbitrary $\mathbb{F}_Q$-linear isomorphism from $A$ to $\mathbb{F}_Q^t$ to view $f|_A$ as a function from $\{\mathbb{F}_Q^t \to \mathbb{F}_q\}$. Given an affine-invariant linear base code $\mathcal{B} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ and integer $n \geq t$, the *n-dimensional lift* of $\mathcal{B}$, denoted $\mathrm{Lift}_n(\mathcal{B})$, is the set

$$\left\{ f : \mathbb{F}_Q^n \to \mathbb{F}_q \;\middle|\; f|_A \in \mathcal{B} \text{ for every } t\text{-dimensional affine subspace } A \subseteq \mathbb{F}_Q^n \right\}.$$

The lifting operation was introduced by Ben-Sasson et al. [5] as a way to build new affine-invariant linear codes that were *not* locally testable. Their codes were also of much lower rate than known affine-invariant linear codes of similar distance. However, in more recent work, Guo et al. [14], showed that lifting could be used positively; they used it to build codes with very good locality properties (especially decodability) with rate much better than known affine-invariant linear ones, and matching qualitatively the performance of the best known codes. The present paper attempts to complement their work by showing that these codes, over constant sized alphabets, can be "locally tested" as efficiently as polynomial codes.

**Testing and absolutely sound testing.** A code $\mathcal{F} \subseteq \{\mathbb{F}_Q^n \to \mathbb{F}_q\}$ is said to be a $(k, \varepsilon, \delta)$-locally testable code (LTC), if $\delta(\mathcal{F}) \geq \delta$ and there exists a probabilistic oracle algorithm that, on oracle access to $f : \mathbb{F}_Q^n \to \mathbb{F}_q$, makes at most $k$ queries to $f$ and accepts $f \in \mathcal{F}$ with probability one, while rejecting $f \notin \mathcal{F}$ with probability at least $\varepsilon \delta_{\mathcal{F}}(f)$.

For an ensemble of codes $\{\mathcal{F}_m \subseteq \{\mathbb{F}_Q^{n_m} \to \mathbb{F}_q\}\}_m$ for infinitely many $m$, where the code $\mathcal{F}_m$ is a $(k(m), \varepsilon(m), \delta(m))$-LTC, we say that the code has an *absolutely sound* tester if there exists $\varepsilon > 0$ such that $\varepsilon(m) \geq \varepsilon$ for every $m$.

Any tester can be converted into an absolutely sound one by repeating the test $1/\varepsilon(m)$ times. However, this comes with an increase in the query complexity (the parameter $k(m)$) and so it makes sense to ask what is the minimum $k$ one can get for an absolutely sound test.

Previous work by Bhattacharyya et al. [8] and Haramaty et al. [15] raised this question in the context of multivariate polynomial codes (Reed-Muller codes) and showed that the "natural tester" for multivariate polynomial codes is absolutely sound, without any repetitions! The natural test here is derived as follows for prime fields:

> To test if a function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ is a polynomial of degree at most $d$, let $t$ be the smallest integer such that there exist functions of degree greater than $d$ in $t$ variables. Pick a random $t$-dimensional affine subspace $A$ and verify that $f|_A$ is a degree-$d$ polynomial.

The natural test thus makes roughly $q^t = q^{(d+1)/(q-1)}$ queries. This number turns out to be optimal for prime fields in that every function looks like a degree-$d$ polynomial if queried at at most $q^{t-1}$ points. Such optimal analyses of low-degree tests are used in computational complexity: In particular, one of the many ingredients in the elegant constructions of Barak et al. [3] is the absolutely sound analysis of the polynomial codes over $\mathbb{F}_2$.

The natural test above is less natural and not quite optimal when dealing with non-prime fields. Namely, one needs to use a larger value of $t$ than the one in the definition above (specifically, $t = (d+1)/(q-q/p)$ where $p$ is the characteristic of the field $\mathbb{F}_q$). While it is unclear if sampling all the points in the larger dimensional space is really necessary for absolutely sound testing, the results so far seem to suggest working with prime fields is a better option.

### 1.1 Our work: Motivation and results

The motivation for our work is twofold. Our first motivation is to understand "low-degree testing" better. Low-degree testing has played a fundamental role in computational complexity and yet its proofs are barely understood. They tend to involve a mix of probabilistic, algebraic, and geometric arguments, and the only setting where the mix of these features seems applicable is the setting of low-degree polynomials. Affine-invariant codes naturally separate the geometry of subspaces in high-dimensional spaces from the algebra of polynomials of low degree. Thus extending a proof or analysis method from the setting of low-degree polynomials to the setting of generic geometric arguments has the nice feature that it has the potential to separate the geometric arguments from the algebraic ones.

Within the theme of low-degree testing, the previous works have revealed interesting analyses. And several of these variations in the resulting theorems have played a role in the construction of efficient PCPs or more recently in other searches for explicit objects. In particular, the literature includes tests such as those originally given by Blum, Luby and Rubinfeld [9] for testing linearity and followed by [23, 1, 17, 16] for testing higher-degree polynomials. The aspects of this family of tests are well abstracted in Kaufman and Sudan [18]. But the literature contains other very interesting theorems, such as those of Raz and Safra [21] and Arora and Sudan [2] which tend to work in the "list-decoding" regime. The analysis of the former in particular seems especially amenable to a "generic proof" in the affine-invariant setting and yet such a proof is not yet available. Our work explores a third such paradigm in the analysis of low-degree tests, which was introduced in the above-mentioned "absolutely-sound testers" of Bhattacharyya et al. and Haramaty et al.

Our work starts by noticing that the natural tests above are really "lifting tests." Namely, the test could be applied to any code that is defined as the lift of a base code with the test checking if a given function is a codeword of the base code when restricted to a random small-dimensional affine subspace of the base dimension. Indeed this is the natural way of interpreting almost all the previous results in low-degree testing (with the exception of that of [22]). If so, it is natural to ask if the analysis can be carried out to show the absolute soundness of such tests.

The second, more concrete, motivation for our work is the work of Guo et al. [14]. Over prime fields, it was well-known that lifts of low-degree polynomials lead only to polynomials of the same degree (in more variables). Guo et al. show that lifting over non-prime fields leads to better codes than over prime fields! (Prior to their work, it seemed that working with non-prime fields was worse than working with prime fields.) The improved rate gives motivation to study lifted codes in general, and in particular, one class of results that would have been nice to extend was the absolutely sound tester of [15].

In this work we show that the natural test of lifted codes is indeed absolutely sound. The following theorem spells this statement out precisely.

**Theorem 1.1** (Main)**.** *For every prime power $q$ and $Q$ a power of $q$, there exists $\varepsilon_Q > 0$ such that the following holds: Let $t \le n$ be positive integers and let $\mathcal{B} \subsetneq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be any affine-invariant linear code. Then $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ is $(Q^t, \varepsilon_Q, Q^{-t})$-locally testable.*

We also note that the literature on property testing includes other general theorems which would imply the testability of the families covered in Theorem 1.1 above. For instance the authors of [7] use only the affine invariance of the families (and do not need the fact that $\mathcal{F}$ is a $\mathbb{F}_q$-vector space). However, such testability results are quantitatively much weaker than those of [19] and do not satisfy our (somewhat strong) definition of $(k, \varepsilon, \delta)$-testability for any positive $\varepsilon$.

We stress that the importance of the above is in the absolute soundness, i. e., the fact that $\varepsilon_Q$ does not depend on $t$ or $\mathcal{B}$. If one is willing to let $\varepsilon_Q$ depend on $t$ and $\mathcal{B}$ then such a result follows from the main theorem of [18].

Our result also sets into proper light the previous work of Haramaty et al. [15] who show that the "natural test" for degree-$d$ polynomials over the field $\mathbb{F}_q$ of characteristic $p$ makes $q^{(d+1)/(q-q/p)}$ queries and is absolutely sound. Our result does not mention any dependence on $p$, the characteristic of the field. It turns out that such a dependence comes due to the following proposition.

Let $\mathrm{RM}(n,d,q)$ denote the set of polynomials of degree at most $d$ in $n$ variables mapping $\mathbb{F}_q^n$ to $\mathbb{F}_q$.

**Proposition 1.2.** *For positive integers $d$ and $q$ where $q$ is a power of a prime $p$, let*

$$t = t_{d,q} = \left\lceil \frac{d+1}{q-q/p} \right\rceil .$$

*Then for every $n \ge t$, the Reed-Muller code $\mathrm{RM}(n,d,q)$ equals the code $\mathrm{Lift}_n(\mathrm{RM}(t,d,q))$.*

Applying Theorem 1.1 to $\mathrm{RM}(n,d,q)$ we immediately obtain the main results of [8] and [15]. And the somewhat cumbersome dependence on the characteristic of $q$ can be blamed on the proposition above, rather than any weakness of the testing analysis. Furthermore, as is exploited by Guo et al. [14] if one interprets the proposition above correctly, then one should use lifts of Reed-Muller codes over non-prime fields with dimension being smaller than $t_{d,q}$. These will yield codes of higher rate while our main theorem guarantees that testability does not suffer.

One concrete consequence of our result is in the use of Reed-Muller codes in the work of Barak et al. [3]. They show how to construct small-set expander graphs with many large eigenvalues and one of the ingredients in their result is a tester of Reed-Muller codes over the domain $\mathbb{F}_2^n$ (codes obtained by lifting an appropriate family of base codes over domain $\mathbb{F}_2^t$). Until this work, the binary Reed-Muller code seemed to be the only code with performance good enough to derive their result. Our work shows that using codes over the domain $\mathbb{F}_4^n$ or $\mathbb{F}_8^n$ (or any constant power of 2) would serve their purpose at least as well, and even give slight (though really negligible) improvements. We elaborate on these codes and their exact parameters in Section 7. (In particular, see Theorem 7.3.)

Finally, unlike the works of Bhattacharyya et al., and Haramaty et al., we cannot claim that our testers are "optimal." This is not because of a weakness in our analysis, rather it is due to the generality of our theorem. For some codes, including the codes considered in the previous works, our theorem is obviously optimal (being the same test and more or less the same analysis as previously). Other codes, however, may possess special properties making them testable much better. In such cases we cannot rule out better tests, though we hope our techniques will still be of some use in analyzing tests for such codes.

**Future research directions.** As noted earlier, the field of low-degree testing has seen several different themes in the analyses. Combined with the work of Kaufman and Sudan [19] our work points to the possibility that much of that study can be explained in terms of the geometry of affine-invariance, and the role of algebra can be encapsulated away nicely. One family of low-degree tests that would be very nice to include in this general view would be that of Raz and Safra [21]. Their work presents a very general proof technique that uses really little algebra; and seems ideally amenable to extending to the affine-invariant setting. We hope that future work will address this.

We also hope that future work improve the dependence of $\varepsilon_Q$ on $Q$ in Theorem 1.1 (which is unfortunately outrageous). Indeed it is not clear why there should be any dependence at all and it would be nice to eliminate it if possible.

**Organization.** We give an overview of the proof of Theorem 1.1 in Section 2, where we also introduce the main technical theorem of this paper (Theorem 2.1). We also describe our technical contributions in this section, contrasting the current proof with those of [8, 15], which we modify. The remaining sections are devoted to the formal proof of Theorem 1.1. Specifically we introduce some of the background material in Section 3. We then prove Theorem 2.1 in Section 4. In Section 5 we show how to prove Theorem 1.1 for the special case in which $Q = q$ using Theorem 2.1. In Section 6 we then prove Theorem 1.1 for general $Q$ via a simple reduction to the case in which $Q = q$. Finally, in Section 7 we give an example of a family of lifted codes to which our main theorem applies.

## 2 Overview of proof

From now on we shall deal only with the special case in which $Q = q$. In Section 6 we show a simple reduction from the general $Q \neq q$ case to the case in which $Q = q$.

### 2.1 Some natural tests

Our proof of Theorem 1.1 follows the paradigm used in [8] and [15]. Both works consider a natural family of tests (and not just the "most" natural test), and analyze their performance by studying the behavior of functions when restricted to "hyperplanes." We introduce the family of tests first.

From now onwards all codes we consider will be linear and affine-invariant unless we explicitly say otherwise. Given a base code $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ and $n \geq \ell \geq t$, we let $\mathcal{L}_\ell = \mathrm{Lift}_\ell(\mathcal{B})$, with $\mathcal{F} = \mathcal{L}_n$. The *$\ell$-dimensional test* for membership in $\mathcal{F}$ works as follows: Pick a random $\ell$-dimensional affine subspace $A$ in $\mathbb{F}_q^n$ and accept $f$ if and only if $f|_A \in \mathcal{L}_\ell$.

Let $\mathrm{Rej}_\ell(f)$ denote the probability with which the $\ell$-dimensional test rejects. Our main theorem aims to show that $\mathrm{Rej}_\ell(f) = \Omega(\delta_{\mathcal{F}}(f))$ when $\ell = t$. As in previous works, our analysis will first lower bound $\mathrm{Rej}_\ell(f)$ for $\ell = t + O(1)$ and then relate the performance of this test to the performance of the $t$-dimensional test.

### 2.2 Overview of proof of Main Theorem 1.1

The analysis of the performance of the $\ell$-dimensional tests is by induction on the number of variables $n$ and based on the behavior of functions when restricted to "hyperplanes." A *hyperplane* in $\mathbb{F}_q^n$ is an affine subspace of dimension $n-1$.

The inductive strategy to analyzing $\mathrm{Rej}_\ell(f)$ is based on the observation that $\mathrm{Rej}_\ell(f) = \mathbb{E}_H[\mathrm{Rej}_\ell(f|_H)]$ where $H$ is a uniform hyperplane. If we know that on most hyperplanes $\delta_{\mathcal{L}_{n-1}}(f|_H)$ is large, then we can prove the right hand side above is large by induction. Thus the inductive strategy relies crucially on showing that if $f$ is far from $\mathcal{F}$, then $f|_H$ cannot be too close to $\mathcal{L}_{n-1}$ on too many hyperplanes. We state this technical result in the contrapositive form below.

**Theorem 2.1** (Main technical)**.** *For every $q$ there exists $\tau$ such that the following holds: Let $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be an affine-invariant linear code and for $\ell \geq t$ let $\mathcal{L}_\ell = \mathrm{Lift}_\ell(\mathcal{B})$. For $n > t$, let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function and let $H_1, \ldots, H_k$ be hyperplanes in $\mathbb{F}_q^n$ such that $\delta_{\mathcal{L}_{n-1}}(f|_{H_i}) \leq \delta$ for every $i \in [k]$ for $\delta < (1/2)q^{-(t+1)}$. Then, if $k \geq q^{t+\tau}$, we have $\delta_{\mathcal{L}_n}(f) \leq 2\delta + 4(q-1)/k$.*

The theorem thus states that if $f$ is sufficiently close to a lift of $\mathcal{B}$ on a sufficiently large number of hyperplanes, yet a very small number (independent of $n$) of hyperplanes, then $f$ is close to a lift of $\mathcal{B}$. The dependence of the number of hyperplanes on $q$ and $t$ is actually important to our (and previous) analysis. The fact that it is some fixed multiple of $q^t$, where the multiple depends only on $q$ and not on $t$, is crucial to the resulting performance.

Going from Theorem 2.1 above to Theorem 1.1 is relatively straightforward. In particular, using Theorem 2.1 we can get a lower bound on $\mathrm{Rej}_{t+\tau}(f)$ without any changes to the proof of [15]. However, going from such an analysis to a lower bound on $\mathrm{Rej}_t(f)$ involves some extra work, with complications similar to (but simpler than), those in the proof of Theorem 2.1 so we omit a discussion here. Section 5 contains all the details.

The main contribution of this paper is the proof of Theorem 2.1. Here, the previous proofs, both in [8] and [15] crucially relied on properties of polynomials and in particular, the first step in both proofs, when testing degree-$d$ polynomials, is to consider the case of $f$ being a degree-$(d+1)$ (or a degree-$(d+q)$) polynomial. In our case there is no obvious candidate for the notion of a degree-$(d+1)$ polynomial and it is abstracting such properties that forms the bulk of our work. In what follows we give an overview of some of the issues arising in such steps and how we deal with them.

### 2.3 Overview of proof of Theorem 2.1

To understand our proof of Theorem 2.1 we need to give some background, specifically to the proofs from the previous work of [15]. Recall the analogous statement in [15] attempted to show that if $f$ was far from being a polynomial of degree $d$, then the number of hyperplanes where $f$ turns out to be close to being a degree-$d$ polynomial is at most $O(q^t)$ (where $t \approx d/q$, the exact number will not be important to us). In [15], the authors reasoned about this in a sequence of steps:

(1) They first showed that any function of degree greater than $d$, stays of degree greater than $d$ on at least $1/q$ fraction of all hyperplanes (provided $n > t$).

(2) Next they reasoned about functions of degree $d+1$ and showed that such a function reduces its degree on at most $O(q^t)$ hyperplanes.

(3) In the third step they consider a general function $f$ that is *far* from being of degree $d$ and show that the number of hyperplanes on which $f$ becomes a degree-$d$ polynomial *exactly* is $O(q^t)$. (This is the step where the big-Oh becomes a really big-Oh.)

(4) Finally, they show that for functions of the type considered in the previous step the number of hyperplanes where they even get *close* to being of degree $d$ is at most $O(q^t)$, thus yielding the analog of Theorem 2.1.

In implementing the program above (which is what we will end up doing) in our more general/abstract setting, our first bottleneck is that, for instance in Step (2) above, we do not have a notion of degree $d+1$ or some notion of functions that are "just outside our good set $\mathcal{F}$." Natural notions of things outside our set do exist, but they do not necessarily satisfy our needs. To understand this issue better, let us see why polynomials of degree $d+O(1)$ appear in the analysis of a theorem such as Theorem 2.1. Consider a simple case where $H_1,\dots,H_q$ are parallel hyperplanes completely covering $\mathbb{F}_q^n$ and $\delta=0$ so $f$ is known to be a good function (member of $\mathcal{F}$, or degree-$d$) when restricted to these hyperplanes. So, in the setting of testing polynomials of degree at most $d$, the hypothesis asserts that $f$ restricted to these hyperplanes is a polynomial of degree at most $d$. For notational simplicity we assume that $H_i$ is the hyperplane given by $x_1=\eta_i$ where $\mathbb{F}_q=\{\eta_1,\dots,\eta_q\}$. Then $f|_{H_i}=P_i(x_2,\dots,x_n)$ for some polynomial $P_i$ of degree $d$. By polynomial interpolation, it follows that $f$ can be described as a degree-$(d+q-1)$ polynomial in $x_1,\dots,x_n$. The bulk of the analysis in [8, 15] now attempts to use the remaining $K-q$ hyperplanes on which $f$ reduces to degree at most $d$, in conjunction with the fact that $f$ is a polynomial of degree at most $d+q-1$ to argue that $f$ is of degree at most $d$.

For us, the main challenge is that in the generic setting of the lift of some code $\mathcal{B}$, we do not have a ready notion of a degree-$(d+q-1)$ polynomial and so we have to define one. Thus the first step in this work is to define such a code. The formal definition appears in Section 4.1: For our current discussion it suffices to say that there is an affine-invariant linear code, which we denote $\mathcal{F}^+$, which contains all "interpolating functions" of elements of $\mathcal{F}$ (so $\mathcal{F}^+$ contains every function $f$ for which there exist some $q$ parallel hyperplanes $H_1,\dots,H_q$ such that $f|_{H_i}$ is a function in $\mathcal{L}_{n-1}$ for all $i$). Of course such a set is not useful if it does not have some nice structure. The key property of our definition of $\mathcal{F}^+$ is that it is the lift of a non-trivial code on at most $t+q-1$ dimensions. We prove this in Section 4.1. This definition of $\mathcal{F}^+$ and its analysis rely centrally on some of the structural understanding of affine-invariant linear codes derived in previous works [18, 12, 11, 6, 5, 4]. Lemma 4.5 allows us to say that $\mathcal{F}^+$ is almost as nice as $\mathcal{F}$, roughly analogous to the way the set of degree-$(d+q-1)$ polynomials is almost as nice as the set of degree-$d$ polynomials.

The notion of $\mathcal{F}^+$ turns out to be easy enough to use to be able to carry out the Steps (3) and (4) in the program above by directly mimicking the proofs of [15], assuming Step (2) holds. (See Section 4.3.) But Steps (1) and (2) turn out to be more tricky. So we turn to these, and in particular, Step (2) next.

Our next barrier in extending the proofs of [15] is the notion of "canonical monomials" which plays a crucial role in Step (2) of [15]. For a function $f$ of degree $d+1$, the canonical monomial is a monomial $M$ of degree $d+1$ supported on very few variables such that $M$ is in the support of $f\circ T$ for some affine transformation $T$. The fact that the number of variables in the support is small, while the monomial remains a "forbidden one" turns out to be central to their analysis and allows them to convert questions of the form: "Does $f$ become a polynomial of smaller degree on the hyperplane $H$?"(which are typically not well-understood) to questions of the form "Does $g$ become the zero polynomial when restricted to $H$?" (which is a very well-studied question).

In our case, we need to work with some function $f$ in $\mathcal{F}^+$ which is not a function of $\mathcal{F}$. The fact that $\mathcal{F}^+$ is a lift of a "few-dimensional" code, in principle ought to help us find a monomial supported on few variables that is not in $\mathcal{F}$. But isolating the "right one" to work with for $f$ turns out to be a subtle issue and we work hard, and come up with a definition that is very specific to each function $f \in \mathcal{F}^+ \setminus \mathcal{F}$. (In contrast the canonical monomials of [15] were of similar structure for every function $f$.) Armed with this definition and some careful analysis we are able to simulate Step (2) in the program above. Details may be found in Section 4.2. Finally, Step (1) is also dealt with similarly, using some of the same style of ideas as in the proof of Step (2). (See Lemma 5.3.)

# 3 Background and preliminary material

In this section we fix some notation and provide some background material on affine-invariant linear codes, needed later on. We start with some basic notation.

Recall we are working with the field $\mathbb{F}_q$ where $q = p^r$, for prime $p$ and integer $r$. Throughout we will consider $q$ as a constant, and so asymptotic notations such as $O(\cdot), \Omega(\cdot)$ in this work may neglect dependence on $q$. All linear-algebraic terminology as subspaces, dimension, span, etc. will be over the field $\mathbb{F}_q$.

We will let $\mathbb{Z}_q$ denote the set $\{0,\ldots,q-1\}$ and $\mathbb{N}$ denote the set of non-negative integers. For $n > t$, we think of $\{\mathbb{F}_q^t \to \mathbb{F}_q\}$ as a subset of $\{\mathbb{F}_q^n \to \mathbb{F}_q\}$ by using the standard embedding $E : \{\mathbb{F}_q^t \to \mathbb{F}_q\} \to \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ given by $(E(f))(x_1,\ldots,x_n) = f(x_1,\ldots,x_t)$.

We let $\mathrm{Aff}_n \subseteq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ represent the set of all the affine functions. I. e.,

$$\mathrm{Aff}_n = \left\{ L : \mathbb{F}_q^n \to \mathbb{F}_q \;\middle|\; \exists \alpha_0,\ldots,\alpha_n \in \mathbb{F}_q \text{ such that } L(x) = \sum_{i=1}^{n} \alpha_i x_i + \alpha_0 \;\forall x = (x_1,\ldots,x_n) \in \mathbb{F}_q^n \right\}.$$

For $L \in \mathrm{Aff}_n$ define $H_L \subseteq \mathbb{F}_q^n$ to be the hyperplane $\left\{x \in \mathbb{F}_q^n \mid L(x) = 0\right\}$. We let $\mathrm{Aff}_{n\times n}$ represent the set of affine transformations from $\mathbb{F}_q^n$ to $\mathbb{F}_q^n$. I. e.,

$$\mathrm{Aff}_{n\times n} := \left\{ T : \mathbb{F}_q^n \to \mathbb{F}_q^n \mid \exists B \in \mathbb{F}_q^{n\times n}, c \in \mathbb{F}_q^n \text{ such that } T(x) = Bx + c \;\forall x \in \mathbb{F}_q^n \right\}.$$

For a function $f \in \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ and $T \in \mathrm{Aff}_{n\times n}$, we denote by $f \circ T$ the composition of $f$ and $T$. I. e., $\forall x \in \mathbb{F}_q^n : f \circ T(x) = f\big(T(x)\big)$.

We view monomials defined on variables $x_1,\ldots,x_n$ as functions mapping $\mathbb{F}_q^n$ to $\mathbb{F}_q$, given by the evaluations of the monomials. The set $\mathcal{M}_n \subseteq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ denotes the set of such monomial functions. For $M = \prod_{i=1}^n x_i^{a_i} \in \mathcal{M}_n$ where $\{a_i\}_{i=1}^n \subseteq \{0,\ldots,q-1\}$, $\deg_{x_i}(M) = a_i$. As usual, $\deg(M) = \sum_{i=1}^n \deg_{x_i}(M)$.

Note that for $a \in \mathbb{N}$, the monomials $M = x_i^a$ and $M' = x_i^{a \bmod q-1}$ are equivalent when $q-1 \nmid a$ or $a = 0$, while when $q-1 \mid a$ and $a \neq 0$ the monomials $M = x_i^a$ and $M' = x_i^{q-1}$ are equivalent. Motivated by this, we define the operation $a \bmod^* k$ as follows

$$a \bmod^* k = \begin{cases} a \mod k, & \text{if } a = 0 \text{ or } k \nmid a, \\ k, & \text{otherwise.} \end{cases}$$

For every function $f \in \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ there is a unique representation as a polynomial

$$f = \sum_{M \in \mathcal{M}_n} c_M^f M \quad \text{for some coefficients} \quad \left\{ c_M^f \;\middle|\; M \in \mathcal{M}_n \right\} \subseteq \mathbb{F}_q \,.$$

We define the *support* of such a function $f$ to be

$$\mathrm{supp}(f) := \left\{ M \in \mathcal{M}_n \;\middle|\; c_M^f \neq 0 \right\},$$

and we let

$$\deg(f) = \max\left\{ \deg(M) \;\middle|\; M \in \mathrm{supp}(f) \right\}.$$

## 3.1 The structure of affine-invariant linear codes

One main feature of affine-invariant linear codes is that they can be characterized by the set of monomials in the support of the functions in these codes. Let $\mathcal{F} \subseteq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ be an affine-invariant linear code. The support $\mathrm{supp}(\mathcal{F})$ of $\mathcal{F}$ is simply the union of the supports of the functions in $\mathcal{F}$, i. e., $\mathrm{supp}(\mathcal{F}) = \bigcup_{f \in \mathcal{F}} \mathrm{supp}(f)$. The following lemma from [18] says that every affine-invariant linear code is uniquely determined by its support.

**Lemma 3.1** (Monomial extraction lemma, [18, Lemma 4.2]). *Let $\mathcal{F} \subseteq \left\{ \mathbb{F}_q^n \to \mathbb{F}_q \right\}$ be an affine-invariant linear code. Then $\mathcal{F}$ has a monomial basis, that is, $\mathcal{F} = \mathrm{span}(\mathrm{supp}(\mathcal{F}))$.*

For a monomial $M \in \mathcal{M}_n$, let $\mathrm{Aff}_{n\times n}(M)$ denote the set of all monomials that can be obtained from $M$ by applying an affine transformation $T \in \mathrm{Aff}_{n\times n}$ on $M$, that is,

$$\mathrm{Aff}_{n\times n}(M) = \left\{ M' \in \mathcal{M}_n \;\middle|\; \exists T \in \mathrm{Aff}_{n\times n} \text{ such that } M' \in \mathrm{supp}(M \circ T) \right\}.$$

We will call $\mathrm{Aff}_{n\times n}(M)$ the *$n$-dimensional affine set* of $M$. When the dimension $n$ is clear from the context we will omit the subscript $n \times n$. Note that if $M \in \mathcal{F}$, $M' \in \mathrm{Aff}_{n\times n}(M)$ and $\mathcal{F}$ is an affine-invariant linear code then $M' \in \mathcal{F}$. The following lemma, also from [18], gives a sufficient condition under which a monomial belongs to $\mathrm{Aff}_{n\times n}(M)$.

**Lemma 3.2** (Monomial spread lemma, [18, Lemma 4.6]). *Let*

$$M' = \prod_{i=1}^n x_i^{a_i}, \qquad M = \prod_{i=1}^n x_i^{b_i}$$

*be a pair of monomials in $\mathcal{M}_n$, where $a_i, b_i \in \{0, \ldots, q-1\}$ for all $1 \le i \le n$. For $1 \le i \le n$, let*

$$a_i = \sum_j a_j^{(i)} p^j, \qquad b_i = \sum_j b_j^{(i)} p^j$$

*be the base-$p$ representation of $a_i, b_i$, respectively. Assume that for all $j$, $\sum_{i=1}^n a_j^{(i)} \le \sum_{i=1}^n b_j^{(i)}$. Then $M' \in \mathrm{Aff}_{n\times n}(M)$.*

We shall also use the following theorem from [13] which says that if a linear code is invariant under invertible affine transformations then it is also invariant under general affine transformations.

**Theorem 3.3** ( [13, Theorem A.1]). *If $\mathcal{F} \subseteq \left\{\mathbb{F}_q^n \to \mathbb{F}_q\right\}$ is an $\mathbb{F}_q$-linear code invariant under invertible affine transformations, then $\mathcal{F}$ is invariant under all affine transformations.*

## 3.2 Lifts of affine-invariant linear codes

The following claim relates the support of the base code to the support of its lift.

**Claim 3.4.** *Let $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be an affine-invariant linear base code and let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ be its $n$-dimensional lift. Then the following hold:*

1. $\mathrm{supp}(\mathcal{B}) = \mathrm{supp}(\mathcal{F}) \cap \mathcal{M}_t$.
2. $\mathrm{supp}(\mathcal{F}) = \left\{M \in \mathcal{M}_n \;\middle|\; \mathrm{Aff}_{n\times n}(M) \cap \mathcal{M}_t \subseteq \mathrm{supp}(\mathcal{B})\right\}$.

*Proof.* For the proof of the first part of the claim, suppose first that $M \in \mathrm{supp}(\mathcal{F}) \cap \mathcal{M}_t$ and let $A \subseteq \mathbb{F}_q^n$ be the $t$-dimensional subspace containing all vectors supported on the first $t$ coordinates. The fact that $M \in \mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ implies that $M|_A \in \mathcal{B}$. Since $M \in \mathcal{M}_t$ we thus have that $M \in \mathrm{supp}(\mathcal{B})$.

On the other hand, suppose that $M \in \mathrm{supp}(\mathcal{B})$. Then in this case we clearly have that $M \in \mathcal{M}_t$. To see that $M$ is also contained in $\mathrm{supp}(\mathcal{F})$ let $A$ be an arbitrary $t$-dimensional affine subspace of $\mathbb{F}_q^n$. Then the fact that $\mathcal{B}$ is an affine-invariant code and $M \in \mathcal{B}$ implies that $M|_A \in \mathcal{B}$. Since $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ this implies in turn that $M \in \mathcal{F}$, so we conclude that $M \in \mathcal{M}_t \cap \mathrm{supp}(\mathcal{F})$.

We proceed to the proof of the second part of the claim. Suppose first that $M \in \mathrm{supp}(\mathcal{F})$ and let $M' \in \mathrm{Aff}_{n\times n}(M) \cap \mathcal{M}_t$. Then there exists an affine transformation $T \in \mathrm{Aff}_{n\times n}$ such that

$$M' \in \mathrm{supp}\left(M \circ T\; |_{x_{t+1}=0,\ldots,x_n=0}\right).$$

But if we let $e_1, \ldots, e_n$ denote the standard basis for $\mathbb{F}_q^n$ and we let $A$ denote the $t$-dimensional subspace containing all vectors of the form $T(0) + \sum_{i=1}^t (T(e_i) - T(0))x_i$ for $x_i \in \mathbb{F}_q$ then

$$M \circ T\; |_{x_{t+1}=0,\ldots,x_n=0} \in \mathcal{B}$$

if and only if $M|_A \in \mathcal{B}$. Since $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ and $M \in \mathcal{F}$ we have that $M|_A \in \mathcal{B}$ and so $M' \in \mathrm{supp}(\mathcal{B})$.

For the other direction, suppose that $M \in \mathcal{M}_n$ is such that $\mathrm{Aff}_{n\times n}(M) \cap \mathcal{M}_t \subseteq \mathrm{supp}(\mathcal{B})$, we will show that $M \in \mathrm{supp}(\mathcal{F})$. For this we need to show that $M|_A \in \mathcal{B}$ for every $t$-dimensional affine subspace $A$. Let $A$ be a $t$-dimensional affine subspace and let $\alpha_0, \alpha_1, \ldots, \alpha_t$ be such that

$$A = \left\{\alpha_0 + \sum_{i=1}^t \alpha_i x_i \;\middle|\; x_i \in \mathbb{F}_q\right\}.$$

Let $T \in \mathrm{Aff}_{n\times n}$ be the affine transformation defined as $T(e_i) = \alpha_i + \alpha_0$ for all $1 \le i \le t$ and $T(e_i) = 0$ for all $t < i \le n$. Then

$$\mathrm{supp}\left(M \circ T\; |_{x_{t+1}=0,\ldots,x_n=0}\right) \subseteq \mathrm{Aff}_{n\times n}(M) \cap \mathcal{M}_t$$

and so we also have that $\mathrm{supp}(M|_A) \subseteq \mathrm{Aff}_{n\times n}(M) \cap \mathcal{M}_t$. Our assumption that $\mathrm{Aff}_{n\times n}(M) \cap \mathcal{M}_t \subseteq \mathrm{supp}(\mathcal{B})$ implies in turn that $\mathrm{supp}(M|_A) \subseteq \mathrm{supp}(\mathcal{B})$ and so $M|_A \in \mathcal{B}$ as required. □

The following proposition bounds the distance of lifts of general affine-invariant linear codes from $\mathbb{F}_Q^t$ to $\mathbb{F}_q$.

**Proposition 3.5** ( [18, Theorem 5.1]). *Let $Q$ be a power of $q$, let $\mathcal{B} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be an affine-invariant linear base code and let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ be its $n$-dimensional lift. Then $\delta(\mathcal{B}) \geq \delta(\mathcal{F}) \geq \delta(\mathcal{B}) - Q^{-t}$.*

From the above proposition one can derive the following corollary.

**Corollary 3.6.** *Let $\mathcal{B} \subsetneq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be some non-trivial affine-invariant linear code and let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ be its $n$-dimensional lift. Then $\delta(\mathcal{F}) \geq Q^{-t}$.*

*Proof.* From Proposition 3.5 it is enough to show that $\delta(\mathcal{B}) \geq 2Q^{-t}$. Assume toward a contradiction that $\delta(\mathcal{B}) < 2Q^{-t}$. From linearity of $\mathcal{B}$ there is a function $f \in \mathcal{B}$ such that there is only one point $v \in \mathbb{F}_Q^t$ such that $f(v) \neq 0$. To reach a contradiction we show that any function $g : \mathbb{F}_Q^t \to \mathbb{F}_q$ can be written as a linear combination of affine transformations of $f$. Because $\mathcal{B}$ is affine-invariant linear code it will follow that $\mathcal{B} = \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$. Indeed, we can express any $g : \mathbb{F}_Q^t \to \mathbb{F}_q$ as

$$g(x) = \sum_{u \in \mathbb{F}_Q^t} \frac{g(u)}{f(v)} f(x + v - u)$$

and the result follows. □

# 4 Proof of Main Technical Theorem 2.1

In this section we prove our Main Technical Theorem 2.1. Our goal then will be to show that if $f$ is far from $\mathcal{F}$ then on most hyperplanes it remains far from $\mathcal{F}$. In particular, if $\mathcal{F}$ is the lift of a $t$-dimensional code, then $f$ should get close on at most $q^{t+O(1)}$ hyperplanes. We start by studying the special case where $f$ results from an "interpolation" of several functions in $\mathcal{F}$.

## 4.1 The code $\mathcal{F}^+$

We start with the definition of the code $\mathcal{F}^+$ which contains all functions obtained from interpolations of functions in $\mathcal{F}$. The code $\mathcal{F}^+$ is defined below as the $n$-dimensional lift of a non-trivial code $\mathcal{B}^+$ on $t+q-1$ variables. We will then show that the code $\mathcal{F}^+$ contains all interpolations of functions in $\mathcal{F}$.

**Definition 4.1** (The code $\mathcal{F}^+$). Let $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be an affine-invariant linear base code with support $\mathrm{supp}(\mathcal{B}) = D$. Let $t^+ = t + (q-1)$ and $D^+ \subseteq \{\mathbb{F}_q^{t^+} \to \mathbb{F}_q\}$ be the set

$$D^+ = \mathrm{Aff}_{t^+ \times t^+} \left\{ M \prod_{i=1}^{q-1} x_{t+i}^{q-1} \;\middle|\; M \in D \right\}.$$

Finally, let $\mathcal{B}^+ = \mathrm{span}(D^+)$ and $\mathcal{F}^+ = \mathrm{Lift}_n(\mathcal{B}^+)$.

We first show that $\mathcal{F}^+$ is non-trivial (i. e., $\mathcal{F}^+ \neq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$), provided the base code $\mathcal{B}$ is non-trivial.

**Claim 4.2.** *If $\mathcal{B} \neq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$, then $\mathcal{F}^+ \neq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$.*

*Proof.* Since $\mathcal{B} \neq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ and since, by Lemma 3.2, every monomial on $t$ variables is in the affine set of the monomial $\prod_{i=1}^t x_i^{q-1}$, it follows that $\prod_{i=1}^t x_i^{q-1} \notin D = \mathrm{supp}(\mathcal{B})$. Hence we have that for every monomial $M' \in D$, $\deg(M') < t(q-1)$. From the definition of $D^+$ it follows that every monomial $M \in D^+$ must have degree strictly less than $t^+ \cdot (q-1)$. It follows that $\mathcal{B}^+ \neq \{\mathbb{F}_q^{t^+} \to \mathbb{F}_q\}$ and $\mathcal{F}^+ \neq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$. □

Next we show that $\mathcal{F}^+$ contains all functions resulting from interpolation of functions in $\mathcal{F}$, as per the following definition.

**Definition 4.3** (Interpolation of functions in $\mathcal{F}$)**.** We say that $f$ is an *interpolation* of functions in $\mathcal{F}$ if there exist $q$ parallel hyperplanes $H_1, \ldots, H_q$ (so $H_i \cap H_j = \emptyset$ for $i \neq j$ and $\bigcup_i H_i = \mathbb{F}_q^n$) and $q$ functions $f_1, \ldots, f_q \in \mathcal{F}$ such that $f|_{H_i} = f_i|_{H_i}$ for every $i \in [q]$.

**Claim 4.4.** *A function $f \in \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ is an interpolation of functions in $\mathcal{F}$ if and only if there exists an affine function $L \in \mathrm{Aff}_n$ and functions $\{f_a \in \mathcal{F} \mid a \in \{0, \ldots, q-1\}\}$ such that $f = \sum_{a \in \{0,\ldots,q-1\}} f_a L^a$.*

*Proof.* The proof is straightforward by polynomial interpolation. □

**Lemma 4.5.** *If $f$ is an interpolation of functions in $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$, then $f \in \mathcal{F}^+$.*

*Proof.* Fix $f = \sum_a f_a L^a$ for affine function $L$ and $f_a \in \mathcal{F}$. We need to show that for every $t^+$-dimensional affine subspace $A$ it is the case that $\mathrm{supp}\big(f|_A\big) \subseteq D^+$. Equivalently, we need to show that for every $T \in \mathrm{Aff}_{n\times n}$, the restriction of $\mathrm{supp}\big(f \circ T\big)$ to the subspace

$$\left\{x \in \mathbb{F}_q^n \,\middle|\, x_{t^++1} = \cdots = x_n = 0\right\}$$

is contained in $D^+$.

First observe that for every $T \in \mathrm{Aff}_{n\times n}$,

$$f \circ T = \sum_{a \in \{0,\ldots,q-1\}} L'^a f'_a$$

where $L'$ is an affine function and $f'_a \in \mathcal{F}$ (so it is of the same form as $f$). Note that every monomial in $\mathrm{supp}(f \circ T)$ is of the form $M \prod_{j=1}^a x_{i_j}$ where $a \in \{0, \ldots, q-1\}$, $i_1, \ldots, i_a \in [n]$ and $M \in \mathrm{supp}(\mathcal{F})$. Further, restricting $f \circ T$ to the subspace

$$\left\{x \in \mathbb{F}_q^n \,\middle|\, x_{t^++1} = \cdots = x_n = 0\right\}$$

allows us to focus only on the cases $i_1, \ldots, i_a \in [t^+]$ and $M \in \mathcal{M}_{t^+}$.

We will show in this case that $M \prod_{j=1}^a x_{i_j} \in D^+$. Fix $M \in \mathcal{M}_{t^+} \cap \mathrm{supp}(\mathcal{F})$, $i_1, \ldots, i_a \in [t^+]$ and let $I \subseteq [t^+]$ be such that $|I| = q-1$ and $\{i_1, \ldots, i_a\} \subseteq I$. Write $M = \prod_{k=1}^{t^+} x_k^{a_k}$ and choose $M' \in \mathcal{M}_t$ to be a monomial of the form $\prod_{k=1}^t x_k^{b_k}$ where $\{b_k \mid k \in [t]\} = \{a_k \mid k \in [t^+] \setminus I\}$. Then by Lemma 3.2,

$$M \prod_{j=1}^a x_{i_j} = \prod_{k \notin I} x_k^{a_k} \prod_{k \in I} x_k^{a_k + \#\{j \mid i_j = k\}} \in \mathrm{Aff}_{t^+\times t^+}\left(\prod_{k=1}^t x_k^{b_k} \prod_{i=1}^{q-1} x_{t+i}^{q-1}\right) = \mathrm{Aff}_{t^+\times t^+}\left(M' \prod_{i=1}^{q-1} x_{t+i}^{q-1}\right).$$

Observe, again by Lemma 3.2, that $M' \in \mathrm{Aff}_{n\times n}(M)$, so $M' \in \mathrm{supp}(\mathcal{F}) \cap \mathcal{M}_t$. By Claim 3.4, this implies in turn that $M' \in \mathrm{supp}(\mathcal{B})$. Consequently, $M \prod_{j=1}^a x_{i_j} \in D^+$, which concludes the proof of the lemma. □

## 4.2 Restrictions of functions in $\mathcal{F}^+$ to hyperplanes

Let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ for a non-trivial affine-invariant linear code $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$. Let $\mathcal{B}^+$ be the code given by Definition 4.1 and let $\mathcal{F}^+ = \mathrm{Lift}_n(\mathcal{B}^+)$. Our goal in this section will be to show that for every $f \in \mathcal{F}^+ \setminus \mathcal{F}$, the number of hyperplanes $H$ for which $f|_H \in \mathcal{F}$ is upper bounded by $O(q^{t^+})$. (See Theorem 4.9 below for formal statement.) We remark that throughout this section one could replace $\mathcal{F}^+$ by any affine-invariant linear code that is the lift of a non-trivial affine-invariant linear base code contained in $\{\mathbb{F}_q^{t^+} \to \mathbb{F}_q\}$ and that the same holds for $\mathcal{F}$ (so $\mathcal{F}^+$ does not have to be as in Definition 4.1 and $\mathcal{F}$ could be a lift of a base code defined over $t^+$ variables and not only $t$ variables).

The overall strategy is as follows.

(1) We will first show in Lemma 4.6 that for every such $f$ there exists an invertible affine transformation $T$ and a monomial $M \notin \mathcal{F}$ supported on the first $t^+$ variables such that $M$ is in the support of $f \circ T$. We further assume that $T$ is such that the degree of $M$ is maximal. Since we can just prove the theorem about $f \circ T$, we assume that $M$ is in the support of $f$.

(2) Next we partition the space of all possible hyperplanes into $q^{t^+ + 1}$ sets (based on their coefficients on the first $t^+$ variables). Our goal will be to show that in each set in the partition there are at most some constant (depending on $q$) number of hyperplanes such that $f$ restricted to these hyperplanes becomes a member of $\mathcal{F}$. To do so we extract from $f$ a non-zero low-degree function $g$ (this function $g$ depends on $M$ and the set in the partition under consideration), such that for a hyperplane $H$ from this set, $f|_H \in \mathcal{F}$ only if $g|_H \equiv 0$. (See Lemma 4.7.)

(3) The final task, to bound the number of hyperplanes on which a low-degree polynomial becomes zero, turns out to be relatively easy and we give this bound in Lemma 4.8.

Below we state the three lemmas mentioned above. We defer their proofs to later in this section. We show how they imply Theorem 4.9 immediately after stating them.

The first of our lemmas isolates a "canonical monomial" for every function $f \in \mathcal{F}^+ \setminus \mathcal{F}$. We note that this is similar to such a step in [15] with the main difference being that the canonical monomials here can be quite different for different functions $f$ (whereas in [15] all canonical monomials of functions $f \in \mathcal{F}^+ \setminus \mathcal{F}$ were of a similar structure).

**Lemma 4.6.** *For every $f \in \mathcal{F}^+ \setminus \mathcal{F}$ there exists an invertible affine transformation $T$ and a monomial $M \in \mathcal{M}_{t^+}$ such that $M \notin \mathcal{F}$ and $M$ is in the support of $f \circ T$.*

Our next lemma, which is the bulk of this section, reduces the task of counting hyperplanes where $f$ becomes a member of $\mathcal{F}$, to the task of counting hyperplanes where a related function becomes zero.

**Lemma 4.7.** *Let $M \in \mathcal{M}_{t^+}$ be a monomial in the support of $f \in \mathcal{F}^+ \setminus \mathcal{F}$ with $M \notin \mathcal{F}$. Suppose furthermore that for every invertible affine transformation $T$ all monomials $M' \in (\mathrm{supp}(f \circ T) \cap \mathcal{M}_{t^+}) \setminus \mathcal{F}$ satisfy that $\deg(M') \le \deg(M)$. Then for every $\alpha_0, \alpha_1, \ldots, \alpha_{t^+} \in \mathbb{F}_q$ there exists a non-zero function $g$ with $\deg(g) \le q^2(q-1)$ such that the following holds: For every choice of $\alpha_{t^+ + 1}, \ldots, \alpha_n \in \mathbb{F}_q$ the hyperplane*

$$H = \left\{ x \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^{n} \alpha_i x_i + \alpha_0 = 0 \right\}$$

*satisfies* $f|_H \in \mathcal{F}$ *only if* $g|_H \equiv 0$.

Finally, we bound the number of hyperplanes where a non-zero low-degree function can become zero.

**Lemma 4.8.** *Let* $f : \mathbb{F}_q^n \to \mathbb{F}_q$ *be a non-zero polynomial of degree* $d$*. Then there are at most* $q^{\frac{d}{q-1}+1}$ *hyperplanes* $H$ *such that* $f|_H \equiv 0$.

**Remark 4.1.** We remark that any bound that is constant for constant $d$ and $q$ would have been good enough to suffice for our purpose. We also note that the bound above is close to the right one. In particular, if $d = t(q-1)$ and

$$f(x_1,\ldots,x_n) = \prod_{i=1}^{t}(x_i^{q-1}-1)$$

then $f$ is zero on every hyperplane of the form

$$x_t = \sum_{i=1}^{t-1} \alpha_i x_i + \beta\,,$$

with the $\alpha_i$ being arbitrary and $\beta$ being non-zero, and there are at least $(q-1)\cdot q^{d/(q-1)-1}$ of these.

We now state and prove our main theorem of this section.

**Theorem 4.9.** *Let* $\mathcal{B} \subsetneq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ *be an affine-invariant linear code and let* $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$*. Let* $\mathcal{B}^+$ *be the code given by Definition 4.1, let* $\mathcal{F}^+ = \mathrm{Lift}_n(\mathcal{B}^+)$ *and let* $f \in \mathcal{F}^+ \setminus \mathcal{F}$*. Then there are at most* $q^{t^+ + q^2 + 2}$ *hyperplanes* $H$ *such that* $f|_H \in \mathcal{F}$.

*Proof.* Let $T$ and $M$ be the invertible affine transformation and the monomial given by Lemma 4.6 above, respectively. Suppose furthermore that $T$ maximizes the degree of $M$, in the sense that for every other invertible affine transformation $T'$ all monomials $M' \in (\mathrm{supp}(f \circ T') \cap \mathcal{M}_{t^+}) \setminus \mathcal{F}$ satisfy that $\deg(M') \le \deg(M)$.

Applying Lemma 4.7 to the function $f \circ T$ and the monomial $M$, we get that for every $\alpha_0, \alpha_1, \ldots, \alpha_{t^+}$ there is a non-zero polynomial $g$ of degree at most $(q-1)q^2$ such that $g|_H \equiv 0$ whenever $(f \circ T)|_H \in \mathcal{F}$. By Lemma 4.8 there are at most $q^{q^2+1}$ such hyperplanes $H$. Summing over all possible choices of $\alpha_0, \alpha_1, \ldots, \alpha_{t^+}$, we get that there are at most $q^{t^+ + q^2 + 2}$ hyperplanes $H$ such that $(f \circ T)|_H \in \mathcal{F}$. The theorem follows from the fact that there is a one-to-one correspondence between the hyperplanes for which the restriction of $f \circ T$ is in $\mathcal{F}$ and the hyperplanes for which the restriction of $f$ is in $\mathcal{F}$. $\square$

In the remaining subsections of this section we prove the three lemmas mentioned above.

#### 4.2.1 Proof of Lemma 4.6

**Lemma 4.6 (restated).** *For every* $f \in \mathcal{F}^+ \setminus \mathcal{F}$ *there exists an invertible affine transformation* $T$ *and a monomial* $M \in \mathcal{M}_{t^+}$ *such that* $M \notin \mathcal{F}$ *and* $M$ *is in the support of* $f \circ T$.

*Proof.* Let $\mathcal{F}_f \subseteq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ be the minimal affine-invariant linear code containing $f$. Note that

$$\mathcal{F}_f = \left\{ \sum_{T \in \mathcal{T}} c_T \cdot (f \circ T) \,\middle|\, c_T \in \mathbb{F}_q \right\},$$

where $\mathcal{T}$ denotes the set of all invertible affine transformations in $\mathrm{Aff}_{n\times n}$ (the fact that one can sum only over invertible transformations follows from Theorem 3.3).

Let $\mathcal{B}^* \subseteq \{\mathbb{F}_q^{t^+} \to \mathbb{F}_q\}$ be the code

$$\mathcal{B}^* = \left\{ g|_{x_{t^++1}=0,\dots,x_n=0} \,\middle|\, g \in \mathcal{F}_f \right\}.$$

By definition $\mathcal{B}^*$ is an affine-invariant linear code and $f \in \mathrm{Lift}_n(\mathcal{B}^*)$. Since

$$f \notin \mathrm{Lift}_n(\mathcal{B}) = \mathrm{Lift}_n(\mathrm{Lift}_{t^+}(\mathcal{B})),$$

it follows that $\mathcal{B}^* \not\subseteq \mathrm{Lift}_{t^+}(\mathcal{B})$. So there must exist a monomial $M \in \mathcal{B}^* \setminus \mathrm{Lift}_{t^+}(\mathcal{B})$ (since $\mathcal{B}^*$ is spanned by the monomials in it, by Lemma 3.1). Clearly, we have that $M \in \mathcal{M}_{t^+}$. Furthermore, by Claim 3.4 $\mathrm{supp}(\mathrm{Lift}_{t^+}(\mathcal{B})) = \mathrm{supp}(\mathcal{F}) \cap \mathcal{M}_{t^+}$ and so $M \notin \mathcal{F}$. Finally, note that the definition of $B^*$ implies that $M$ belongs also to $\mathcal{F}_f$. By the fact that

$$\mathcal{F}_f = \left\{ \sum_{T \in \mathcal{T}} c_T \cdot (f \circ T) \,\middle|\, c_T \in \mathbb{F}_q \right\}$$

it follows that there exists an invertible affine transformation $T$ such that $M \in \mathrm{supp}(f \circ T)$. The lemma follows. □

#### 4.2.2 Proof of Lemma 4.7

**Lemma 4.7 (restated).** *Let $M \in \mathcal{M}_{t^+}$ be a monomial in the support of $f \in \mathcal{F}^+ \setminus \mathcal{F}$ with $M \notin \mathcal{F}$. Suppose furthermore that for every invertible affine transformation $T$ all monomials $M' \in (\mathrm{supp}(f \circ T) \cap \mathcal{M}_{t^+}) \setminus \mathcal{F}$ satisfy that $\deg(M') \le \deg(M)$. Then for every $\alpha_0, \alpha_1, \dots, \alpha_{t^+} \in \mathbb{F}_q$ there exists a non-zero function $g$ with $\deg(g) \le q^2(q-1)$ such that the following holds: For every choice of $\alpha_{t^++1}, \dots, \alpha_n \in \mathbb{F}_q$ the hyperplane*

$$H = \left\{ x \in \mathbb{F}_q^n \,\middle|\, \sum_{i=1}^n \alpha_i x_i + \alpha_0 = 0 \right\}$$

*satisfies $f|_H \in \mathcal{F}$ only if $g|_H \equiv 0$.*

*Proof.* As a first step, we perform a change of basis that will allow us to assume, without loss of generality, that $\alpha_1 = -1$ and $\alpha_0 = \alpha_2 = \cdots = \alpha_{t^+} = 0$ and so restriction of $f$ to the hyperplane given by $\alpha_{t^++1}, \dots, \alpha_n$ is given by the function

$$f\left( \sum_{i=t^++1}^n \alpha_i x_i, x_2, \dots, x_n \right).$$

We will analyze such functions in later steps.

Fix $\alpha_0, \alpha_1, \ldots, \alpha_{t^+} \in \mathbb{F}_q$ and let $\mathcal{H} = \mathcal{H}_{\alpha_0,\ldots,\alpha_{t^+}}$ be the set of hyperplanes $H$ such that there exist $\alpha_{t^++1}, \ldots, \alpha_n$ so that

$$H = \left\{ x \in \mathbb{F}_q^n \,\middle|\, \sum_{i=1}^{n} \alpha_i x_i + \alpha_0 = 0 \right\} .$$

First we dismiss the case $\alpha_1 = \cdots = \alpha_{t^+} = 0$. In this case for every hyperplane $H \in \mathcal{H}$, the function $f|_H$ still has the monomial $M$ in its support and so $f|_H \notin \mathcal{F}$. (So formally, $g = 1$ satisfies the condition of the lemma.) So from here on we assume there exists $c \in [t^+]$ such that $\alpha_c \neq 0$. Without loss of generality we assume $c$ is the minimal such index, and that $\alpha_c = -1$. For notational simplicity we assume below that $c = 1$. Now consider the affine transformation $S \in \mathrm{Aff}_{n \times n}$ such that

$$S(e_1) = e_1 + \sum_{i=2}^{t^+} \alpha_i e_i + \alpha_0$$

and $S(e_i) = e_i$ for all $i \geq 2$. Let $f' = f \circ S$. For hyperplane

$$H = \left\{ x \,\middle|\, \sum_{i=1}^{n} \alpha_i x_i + \alpha_0 = 0 \right\} ,$$

let $H'$ be the hyperplane

$$H' = \left\{ x \,\middle|\, x_1 = \sum_{i=t^++1}^{n} \alpha_i x_i \right\} .$$

Notice that $f|_H \in \mathcal{F}$ if and only if $f'|_{H'} \in \mathcal{F}$ and $H'$ corresponds to $\alpha'_1 = -1$ and $\alpha'_i = 0$ for $i \in \{0, 2, 3, \ldots, t^+\}$.

Now let $M' \in \mathrm{supp}(f') \cap \mathcal{M}_{t^+}$ be a monomial such that $M \in \mathrm{supp}(M' \circ T)$ for some invertible $T \in \mathrm{Aff}_{t^+ \times t^+}$. Note such a monomial $M'$ must exist since $S$ is an invertible transformation in $\mathrm{Aff}_{t^+ \times t^+}$. Since $M \in \mathrm{supp}(M' \circ T)$ and $M \notin \mathcal{F}$ it follows that $M' \notin \mathcal{F}$. Furthermore, the fact that $M \in \mathrm{supp}(M' \circ T)$ implies that $\deg(M) \leq \deg(M')$ and hence $M'$ is also maximal with respect to degree. That is, for every invertible affine transformation $T'$ it holds that all monomials $M'' \in (\mathrm{supp}(f' \circ T') \cap \mathcal{M}_{t^+}) \setminus \mathcal{F}$ satisfy that $\deg(M'') \leq \deg(M')$.

In what follows we prove that the lemma holds for the polynomial $f'$ with monomial $M'$ and coefficients $\alpha'_0, \ldots, \alpha'_{t^+}$, i.e., we prove the existence of a non-zero polynomial $g'$ of degree at most $q^2(q-1)$ such that $g'|_{H'} \equiv 0$ whenever $f'|_{H'} \in \mathcal{F}$. The lemma follows for $f$ by setting $g = g' \circ S^{-1}$. For notational simplicity we drop the primes below and simply assume $\alpha_1 = -1$ and $\alpha_i = 0$ for all other $i \leq t^+$ and so $f = f'$, $M = M'$.

Let $\bar{M} \in \mathbb{F}_q[x_2, \ldots, x_{t^+}]$ and let $a \geq 0$ be an integer such that $M = x_1^a \bar{M}$. Write $f = g_1 \bar{M} + r_1$ where $g_1 \in \mathbb{F}_q[x_1, x_{t^++1}, \ldots, x_n]$ is such that $g_1 \bar{M}$ contains all monomials in $\mathrm{supp}(f)$ whose degrees in variables $x_2, \ldots, x_{t^+}$ equal their degrees in $\bar{M}$ and $r_1$ is the remaining terms. Further write $g_1 = g + g_2$ where $g$ includes all monomials $M'$ of degree $\deg(M') \bmod^*(q-1) = a$ and $g_2$ includes all monomials $M''$ of degree $\deg(M'') \bmod^*(q-1) \neq a$. Rewriting we have $f = g \cdot \bar{M} + r$ where $r = g_2 \bar{M} + r_1$, $g \in \mathbb{F}_q[x_1, x_{t^++1}, \ldots, x_n]$ and $r \in \mathbb{F}_q[x_1, \ldots, x_n]$. We show below, using a series of claims that $g$ satisfies the conditions of the lemma. Specifically, fix $\alpha_{t^++1},\dots,\alpha_n$, let $L(x)$ be the linear function $L(x)=\sum_{i=t^++1}^n \alpha_i x_i$, and let $H$ be the hyperplane given by $\{x_1=L(x)\}$. We wish to show that $g|_H\equiv 0$ if $f|_H\in\mathcal{F}$.

Let $\mathcal{F}_f$ be the minimal affine-invariant linear code containing $f$. Let

$$\mathcal{F}_{-\bar{M}}=\left\{h\in\mathbb{F}_q[x_1,x_{t^++1},\dots,x_n]\;\middle|\;\bar{M}\cdot h\in\mathcal{F}\right\},$$

and let

$$\mathcal{F}_{f,-\bar{M}}=\left\{h\in\mathbb{F}_q[x_1,x_{t^++1},\dots,x_n]\;\middle|\;\bar{M}\cdot h\in\mathcal{F}_f\right\}.$$

Below we state and prove four claims about $g$ (Claims 4.10- 4.13) from which the lemma follows immediately. Specifically, the first two prove that $g$ is non-zero and of low-degree. And the final two prove that $g$ becomes zero on $H$ if $f|_H\in\mathcal{F}$. Claim 4.11 uses Lemma 4.14 which we state and prove after we prove the current lemma.

**Claim 4.10.** *$g\neq 0$ and $g\in\mathcal{F}_{f,-\bar{M}}$.*

*Proof.* The fact that $g$ is non-zero follows from the fact that $M$ is in the support of $f$ and $M=x_1^a\bar{M}$ and so $x_1^a$ is in the support of $g$. Since $\operatorname{supp}(g\cdot\bar{M})\subseteq\operatorname{supp}(f)$ we have that $g\cdot\bar{M}\in\mathcal{F}_f$ and so by definition of $\mathcal{F}_{f,-\bar{M}}$ we have $g\in\mathcal{F}_{f,-\bar{M}}$. □

**Claim 4.11.** *Every function in $\mathcal{F}_{f,-\bar{M}}$ has degree at most $q^2(q-1)$.*

*Proof.* In Lemma 4.14 we prove that for any affine-invariant linear code $\mathcal{G}$, if there exists a monomial $N$ of degree at most $\ell$ that is not in $\mathcal{G}$, then every function in $\mathcal{G}$ has degree at most $(1/2)q^2\cdot\ell$. So to prove the current claim it suffices to show that there is a monomial of degree at most $2(q-1)$ that is not contained in $\mathcal{F}_{f,-\bar{M}}$. We now show that the monomial $N=x_1^a x_{t^++1}^{q-1}\notin\mathcal{F}_{f,-\bar{M}}$. Notice that $N$ is a monomial of degree at most $a+(q-1)\le 2(q-1)$, and so with Lemma 4.14 this suffices to prove the claim.

Assume for contradiction that

$$x_1^a x_{t^++1}^{q-1}\in\mathcal{F}_{f,-\bar{M}}\quad\text{and so}\quad M\cdot x_{t^++1}^{q-1}=x_1^a x_{t^++1}^{q-1}\bar{M}\in\mathcal{F}_f.$$

Since $\mathcal{B}^+\neq\{\mathbb{F}_q^{t^+}\to\mathbb{F}_q\}$ and $M\in\operatorname{supp}(\mathcal{F}^+)\cap\mathcal{M}_{t^+}=\operatorname{supp}(\mathcal{B}^+)$, we have $M\neq\prod_{i=1}^{t^+}x_i^{q-1}$. We conclude there exists $i\in[t^+]$ such that $d_i\triangleq\deg_{x_i}(M)\neq q-1$. But if $x_1^a x_{t^++1}^{q-1}\bar{M}\in\mathcal{F}_f$ then by exchanging the variables $x_i$ and $x_{t^++1}$ we also have the monomial

$$Mx_i^{q-1-d_i}x_{t^++1}^{d_i}\in\mathcal{F}_f\quad\text{and so}\quad Mx_i^{q-1-d_i}\in\mathcal{F}_f.$$

We show below that this contradicts the maximality of $M$.

Note first that $Mx_i^{q-1-d_i}$ is a monomial in $\mathcal{M}_{t^+}$. Furthermore, since

$$\mathcal{F}_f=\left\{\sum_{T\in\mathcal{T}}c_T\cdot(f\circ T)\;\middle|\;c_T\in\mathbb{F}_q\right\}$$

we have that $Mx_i^{q-1-d_i}\in\operatorname{supp}(f\circ T)$ for some invertible affine transformation $T$. Finally, by Lemma 3.2 we have that $M\in\operatorname{Aff}_{n\times n}(Mx_i^{q-1-d_i})$ and so the fact that $M\notin\mathcal{F}$ implies that $Mx_i^{q-1-d_i}\notin\mathcal{F}$. Concluding, we have just shown that $Mx_i^{q-1-d_i}$ is a monomial in variables $x_1,\dots,x_{t^+}$ contained in $\operatorname{supp}(f\circ T)\setminus\mathcal{F}$ for some invertible affine transformation $T$. Given that $\deg(Mx_i^{q-1-d_i})>\deg(M)$, this clearly violates the maximality of $M$. □

**Claim 4.12.** *If $f|_H \in \mathcal{F}$ then $g|_H \in \mathcal{F}_{-\bar{M}}$.*

*Proof.* Recall that
$$H = \left\{ x \in \mathbb{F}_q^n \,\middle|\, x_1 = L(x_{t^+ +1}, \dots, x_n) \right\}.$$
Let
$$f'(x_2, \dots, x_n) = f(L(x_{t^+ +1}, \dots, x_n), x_2, \dots, x_n)$$
denote the function $f|_H$. As in the partitioning of $f$, let $f' = g_1'\bar{M} + r_1'$ where $g_1'\bar{M}$ includes all monomials of $f'$ whose degrees in $x_2, \dots, x_{t^+}$ equal their degrees in $\bar{M}$. Further let $g_1' = g' + g_2'$ where $g'$ includes all terms of degree $d$ for $d \bmod^*(q-1) = a$ and $g_2'$ collects the remaining terms.

The proof of the claim relies crucially on the following property of $g'$, namely that
$$g'(x_{t^+ +1}, \dots, x_n) = g(L(x_{t^+ +1}, \dots, x_n), x_{t^+ +1}, \dots, x_n)$$
is the function $g|_H$. To see this, note that when substituting $x_1 = L(x_{t^+ +1}, \dots, x_n)$ degrees in $x_2, \dots, x_{t^+}$ do not change and so we have $g_1' = g_1(L(x), x_{t^+ +1}, \dots, x_n)$. Next we note that for every monomial of degree $d$, the reductions modulo $x_i^q - x_i$ (for every $i$) can only change the degree of the monomial to $d'$ which satisfies $d' \bmod^*(q-1) = d$ and so $g' = g(L(x), x_{t^+ +1}, \dots, x_n)$.

The claim now follows easily. From the property of the previous paragraph our claim can be rephrased as asserting that if $f' \in \mathcal{F}$ then $g' \in \mathcal{F}_{-\bar{M}}$. But if $f' = g'\bar{M} + r' \in \mathcal{F}$, then it follows that $g'\bar{M}$ (with its support being a subset of the support of $f'$) is also in $\mathcal{F}$ and so $g' \in \mathcal{F}_{-\bar{M}}$. □

**Claim 4.13.** *If $g|_H \in \mathcal{F}_{-\bar{M}}$ then $g|_H \equiv 0$.*

*Proof.* Assume for contradiction that $g|_H \in \mathcal{F}_{-\bar{M}}$ and $g|_H \not\equiv 0$. Let
$$g'(x_{t^+ +1}, \dots, x_n) = g|_H(x) = g(L(x), x_{t^+ +1}, \dots, x_n).$$
Every monomial of $g$ is of degree $d$ where $d \bmod^*(q-1) = a$, and hence the same holds also for $g'$. For $\overline{\beta} = (\beta_{t^+ +1}, \dots, \beta_n)$, let
$$p_{\overline{\beta}}(x_1) = g'(\beta_{t^+ +1}, \dots, \beta_n) x_1^a.$$
Since $g|_H \not\equiv 0$, there exists $\overline{\beta} = (\beta_{t^+ +1}, \dots, \beta_n)$ such that $g'(\beta_{t^+ +1}, \dots, \beta_n) \neq 0$ and so $p_{\overline{\beta}}(x_1)$ has $x_1^a$ in its support. Note furthermore that $p_{\overline{\beta}}(x_1)$ is obtained by an affine (although non-invertible) transformation of the coordinates of $g'$ which is given by $T(e_i) = \beta_i e_1$ for all $i \in \{e_{t^+ +1}, \dots, e_n\}$. Thus the fact that $g' \in \mathcal{F}_{-\bar{M}}$ implies in turn that $x_1^a \in \mathcal{F}_{-\bar{M}}$. But, by the definition of $\mathcal{F}_{-\bar{M}}$ this implies $M = x_1^a \bar{M} \in \mathcal{F}$ which contradicts the hypothesis of the lemma. □

This concludes the proof of Lemma 4.7. □

We now state and prove a lemma which bounds the maximal degree of functions in any affine-invariant linear code given a single monomial not in the code, which was used in the proof above.

**Lemma 4.14.** *Let $\mathcal{G} \subseteq \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ be an affine-invariant linear code and let $M$ be a monomial of degree $\ell$ such that $M \notin \mathcal{G}$. Then, for every function $f \in \mathcal{G}$, we have* $\deg(f) \leq (1/2)q^2\ell$.

*Proof.* We first note that we can assume, without loss of generality, that $\ell q \leq n$. Else (if $n < \ell q$) we can prove the result for the code $\mathcal{G}' = \mathrm{Lift}_{\ell q}(\mathcal{G})$, and then use the identity $\mathcal{G} = \mathcal{G}' \cap \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ to derive the result for $\mathcal{G}$. So from now we have $n \geq \ell q$.

Let $p$ be a prime number and $t$ be an integer such that $q = p^t$. Let $M' = \prod_{i=1}^n x_i^{a_i}$ be a monomial in $f \in \mathcal{G}$, write any degree $a_i$ in base $p$ as

$$a_i = \sum_{j=0}^{t-1} a_j^{(i)} p^j ,$$

where $a_j^{(i)} \in \{0, \dots, p-1\}$ for all $0 \leq j \leq t-1$ and $i \in [n]$.

We will show that

$$\sum_{i=1}^n a_j^{(i)} < \ell p^{t-j}$$

for every $0 \leq j \leq t-1$. This will show that

$$\deg(M') = \sum_{i=1}^n a_i = \sum_{i=1}^n \sum_{j=0}^{t-1} a_j^{(i)} p^j < \sum_{j=0}^{t-1} \ell p^{t-j} p^j = tq\ell \leq \frac{1}{2} q^2 \ell ,$$

thereby yielding the lemma.

Assume for contradiction that there is some $j$, such that

$$\sum_{i=1}^n a_j^{(i)} \geq \ell p^{t-j} .$$

Then, by Lemma 3.2 the monomial

$$M_1 = \prod_{i=1}^{\ell p^{t-j}} x_i^{p^j}$$

is in $\mathcal{G}$. By applying the linear transformation $T_1$ given by $T_1(e_i) = e_{i \bmod \ell}$ for every $i$ in the monomial $M_1$, we deduce that $\prod_{i=1}^{\ell} x_i^q \in \mathcal{G}$. In turn the resulting monomial is equivalent to the monomial $M_2 = \prod_{i=1}^{\ell} x_i$ over $\mathbb{F}_q$. Let $\ell_i$ denote the degree of $x_i$ in $M$ so that $\sum_i \ell_i = \ell$. Now consider the transformation $T_2$ defined by $\forall i \in [n], \forall k$ such that

$$\sum_{j=1}^{i-1} \ell_j < k \leq \sum_{j=1}^{i} \ell_j : \ T_2(e_k) = e_i .$$

We have $M_2 \circ T_2 = M$, yielding $M \in \mathcal{G}$ which contradicts our assumption. The lemma follows. □

### 4.2.3 Proof of Lemma 4.8

We conclude the section by proving Lemma 4.8 which we restate below for convenience.

**Lemma 4.8 (restated).** *Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a non-zero polynomial of degree $d$. Then there are at most $q^{\frac{d}{q-1}+1}$ hyperplanes $H$ such that $f|_H \equiv 0$.*

*Proof.* Let $H_1,\dots,H_k$ be all the hyperplanes that satisfy $f|_{H_i} \equiv 0$. Consider the set

$$S \triangleq \left\{x \in \mathbb{F}_q^n \mid \forall i \in k,\ x \notin H_i\right\}.$$

We will find an upper and lower bound on the density of the set $S$ as a function of $k$ and this will yield the claimed bound on $k$.

Consider a point $x \in \mathbb{F}_q^n$, chosen uniformly at random. We first give an upper bound on the probability that $x \in S$. Let $Z_i$ be a random variable such that $Z_i = 1$ if and only if $x \in H_i$. Note that we wish to upper bound the probability that $\sum_{i=1}^k Z_i = 0$. We bound this probability using the Chebychev bound.

Clearly, for all $i \in [k]$,

$$\mathbb{E}\left[Z_i^2\right] = \mathbb{E}\left[Z_i\right] = \frac{|H_i|}{\left|\mathbb{F}_q^n\right|} = \frac{1}{q}.$$

Moreover, for $i \neq j$, $\mathbb{E}\left[Z_iZ_j\right] \le 1/q^2$. ($E[Z_iZ_j] = 1/q^2$ if $H_i$ and $H_j$ are not parallel, and equals zero if they are.) Calculating the variance,

$$\begin{aligned}\mathrm{Var}\left(\sum_{i=1}^k Z_i\right) &= \mathbb{E}\left[\left(\sum_{i=1}^k Z_i\right)^2\right] - \mathbb{E}\left[\sum_{i=1}^k Z_i\right]^2 = 2\sum_{i<j}\mathbb{E}\left[Z_iZ_j\right] + \sum_{i=1}^k \mathbb{E}\left[Z_i^2\right] - \left(\frac{k}{q}\right)^2 \\ &\le \frac{k(k-1)}{q^2} + \frac{k}{q} - \frac{k^2}{q^2} = \frac{k(q-1)}{q^2}.\end{aligned}$$

We bound the density of $S$ by Chebyshev's inequality,

$$\Pr[x \in S] = \Pr\left[\sum_{i=1}^k Z_i = 0\right] \le \Pr\left[\left|\sum_{i=1}^k Z_i - \frac{k}{q}\right| \ge \frac{k}{q}\right] \le \frac{\mathrm{Var}\left(\sum_{i=1}^k Z_i\right)}{\left(\frac{k}{q}\right)^2} \le \frac{q-1}{k}.$$

On the other hand, by the well-known polynomial-distance lemma (see, for instance, [15, Lemma 3.2])

$$\Pr\left[x \in S\right] \ge \Pr\left[f(x) \neq 0\right] \ge q^{-\frac{d}{q-1}}.$$

Combining the above, we have $q^{-\frac{d}{q-1}} \le (q-1)/k$ which yields

$$k \le q^{\frac{d}{q-1}}(q-1) < q^{\frac{d}{q-1}+1},$$

as claimed. □

### 4.3 Restrictions of general functions to hyperplanes

We finally turn to the proof of the Main Technical Theorem 2.1. The proof of this section is a straightforward adaptation of the proof of the corresponding theorem in [15], given Theorem 4.9. We give a brief overview of the proof first.

Recall that Theorem 2.1 says that if a function $f \in \{\mathbb{F}_q^n \to \mathbb{F}_q\}$ is $\delta$-close to functions from $\mathcal{F}$ on $k$ hyperplanes (for sufficiently large $k$), then $f$ is itself close to some function from $\mathcal{F}$. It turns out that the central difficulty in proving this theorem already arises when $\delta = 0$, and the theorem for general $\delta$ follows immediately. Theorem 4.15 states this special case, which we prove first. The proof of Theorem 2.1 follows easily and we prove it later in Section 4.3.4.

The proof of Theorem 4.15 is itself by induction on $n$, however, now the hardest part is the base case. We prove the base case separately as Lemma 4.18 in Section 4.3.2. We then prove Theorem 4.15 as a consequence in Section 4.3.3.

### 4.3.1 Interpolation from exact agreement

We start by stating Theorem 4.15 which implies the special case of Theorem 2.1 for the case of $\delta = 0$.

**Theorem 4.15.** *For every $q$ there exists $\tau$ such that the following holds: Let $n > t$, let $\mathcal{B} \subsetneq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be an affine-invariant linear code and let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function and $H_1, \ldots, H_k$ be hyperplanes in $\mathbb{F}_q^n$ such that $f|_{H_i} \in \mathcal{F}$ for every $i \in [k]$. Then, if $k \geq q^{t+\tau}$, there exists a function $h \in \mathcal{F}$ such that $f|_{H_i} = h|_{H_i}$ for all $i \in [k]$.*

We will prove Theorem 4.15 in Section 4.3.3 by induction on $n$. Our proof will rely on a slightly stronger (smaller) bound on $k$ as $n$ gets smaller. This makes the base case of small values of $n$ more challenging and we deal with this first.

### 4.3.2 The base case

Here we consider the case where $n = t + O(1)$. In this case the number of hyperplanes $k \geq q^{t+\tau}$ is a "constant" fraction of all the hyperplanes. We view these hyperplanes as points in a $(n+1)$-dimensional subspace (the hyperplane given by $\sum_{i=1}^n \alpha_i x_i = \alpha_0$ is associated with the point $(\alpha_0, \ldots, \alpha_n) \in \mathbb{F}_q^{n+1}$), and then use the well-known Hales–Jewett Theorem from additive combinatorics to infer that there are $q$ points in a straight line among this set of points. (Indeed by choosing our density to be slightly larger we may conclude that there are many straight lines among the given set of points. We use such a version that was already used in [15].) In terms of hyperplanes these lines lead to a small set that cover most of $\mathbb{F}_q^n$. We use this set to derive that there is a function $h$ from $\mathcal{F}^+$ that is consistent with $f$ on all the given hyperplanes. We then use Theorem 4.9 to conclude that $h$ must actually be an element of $\mathcal{F}$.

We start by stating the version of the Hales-Jewett theorem we will use after a basic definition.

**Definition 4.16.** Let $v \in \mathbb{F}_q^n$ and $u \in \mathbb{F}_q^n \setminus \{0\}$. A line through $v$ in direction $u$ is the set $\left\{ v + \alpha u \;\middle|\; \alpha \in \mathbb{F}_q \right\}$. Notice that the direction of a given line is unique up to multiplication by an element of $\mathbb{F}_q \setminus \{0\}$.

The following theorem is a corollary of the Hales–Jewett theorem [10, 20].

**Theorem 4.17** ([15, Corollary 3.5])**.** *For every prime power $q$ and every $c > 0$ there exists an integer $\lambda_{q,c}$ such that for every integer $m \in \mathbb{N}$ the following holds: if $n \geq \lambda_{q,c} + m$ then every set $A \subseteq \mathbb{F}_q^n$ of size $|A| \geq q^{n-c}$ contains $m$ lines whose directions are linearly independent.*

The following lemma now states Theorem 4.15 for the special (base) case of $n \leq t + O(1)$.

**Lemma 4.18.** *For every $q$, and constant $c$, there exists a constant $\tau_c$ such that the following holds: Let $n, t \in \mathbb{N}$ be such that $t < n \leq t + \tau_c$. Let $\mathcal{B} \subsetneq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ be an affine-invariant linear code and let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function and $H_1, \ldots, H_k$ be hyperplanes in $\mathbb{F}_q^n$ such that $f|_{H_i} \in \mathcal{F}$ for every $i \in [k]$. Then, if $k \geq q^{t+\tau_c-c}$, there exists a function $h \in \mathcal{F}$ such that $f|_{H_i} = h|_{H_i}$ for all $i \in [k]$.*

*Proof.* We prove the lemma for $\tau_c = \lambda + q + c$ where $\lambda = \max\{\lambda_{q,c+1} + 1, q^2 + 4\}$ and $\lambda_{q,c+1}$ is as given by Theorem 4.17.

**Overview:** We start by giving an overview of the proof. Using a natural correspondence between hyperplanes in $\mathbb{F}_q^n$ and points in $\mathbb{F}_q^{n+1}$ (the hyperplane $\sum_{i=1}^n \alpha_i x_i = \alpha_0$ corresponds to the point $(\alpha_0, \ldots, \alpha_n) \in \mathbb{F}_q^{n+1}$) and the Hales–Jewett theorem in $\mathbb{F}_q^{n+1}$ we find many hyperplanes of a "somewhat structured" type. We will formally describe these later below, but an example of hyperplanes corresponding to points on a line would be the set of hyperplanes $x_1 + \lambda x_2 = 0$ for every $\lambda \in \mathbb{F}_q$. This set of hyperplanes almost covers the entire region $\mathbb{F}_q^n$, except the points with $x_1 \neq 0$ and $x_2 = 0$.

We then proceed in three steps: We first observe that for every hyperplane of the form $x_2 = \eta$ for $\eta \neq 0$, $f$ restricted to this hyperplane is an element of $\mathcal{F}^+$. Observing further that $f|_{x_2=\eta}$ is a function of $\mathcal{F}$ when restricted to many hyperplanes in $\mathbb{F}_q^{n-1}$, we use Theorem 4.9 to claim that $f|_{x_2=\eta} \in \mathcal{F}$. Now if we only could claim that $f|_{x_2=0}$ is also an element of $\mathcal{F}$ we would be done by a similar sequence of observations. However, this is not necessarily true. To deal with this, we show in the first step, using the fact that there are many hyperplanes, that for many variables $x_i$ we have $f|_{x_i=\eta} \in \mathcal{F}$ for every $\eta \neq 0$.

In the second step we apply some algebraic interpolations to show for every $i \in [m]$ the existence of a function $h_i : \mathbb{F}_q^n \to \mathbb{F}_q$ such that $h_i \in \mathcal{F}^+$ and $h_i|_{x_i=\eta} = f|_{x_i=\eta}$ for every $\eta \neq 0$.

In the third and last step we show how to build a single function $h \in \mathcal{F}^+$ that agrees with $f|_{x_i=\eta}$ for every choice of $i$ and for every $\eta \neq 0$, and then show that this function is in $\mathcal{F}$ and agrees with $f$ on every given hyperplane. We note that this step requires some non-trivial extensions of corresponding steps in [15] as well. We now turn to the formal proof.

**The formal proof:** We start by showing that some very structured set of hyperplanes are included among the given $k$ hyperplanes. For a point $\alpha = (\alpha_0, \ldots, \alpha_n) \in \mathbb{F}_q^{n+1}$ let $H_\alpha$ denote the hyperplane

$$H_\alpha = \left\{ x \in \mathbb{F}_q^n \;\middle|\; \sum_{i=1}^n \alpha_i x_i = \alpha_0 \right\}.$$

For an affine transformation $T$, let $H_\alpha \circ T$ denote the hyperplane $H_{T(\alpha)}$.

**Claim 4.19.** *Let $m = t + q + 1$. There exists an invertible affine transformation $T$ and $m$ invertible affine functions $L_1, \ldots, L_m : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that for every $i \in [m]$ and $\gamma \in \mathbb{F}_q$ the hyperplane*

$$H_{i,\gamma} \triangleq \{x \mid L_i(x) + \gamma x_i = 0\}$$

*is included in the set $\{H_1 \circ T, \ldots, H_k \circ T\}$.*

*Proof.* Let $P = \{\alpha^{(1)}, \ldots, \alpha^{(k)}\} \subseteq \mathbb{F}_q^{n+1}$ be a set of $k$ points such that $H_i = H_{\alpha^{(i)}}$ for every $i \in [k]$. We assume without loss of generality that $\alpha_0^{(i)} \in \{0, 1\}$ for all $i \in [k]$ since the other $\alpha_j^{(i)}$ can be scaled to achieve this. Note furthermore that if $n < \log_q k$ then there is nothing to prove since in this case one cannot find $k$ distinct hyperplanes inside $\mathbb{F}_q^n$. Hence we may assume that $n \geq \log_q k \geq t + \tau_c - c$. Since the density of $P$ in $\mathbb{F}_q^{n+1}$ is $k/q^{n+1} \geq q^{-(c+1)}$ and $n \geq t + \tau_c - c \geq t + \lambda_{q,c+1} + 1 + q$, by Theorem 4.17 we have that there are at least $m = t+q+1$ linearly independent lines in $P$. Since all points in $P$ have their 0th coordinate in $\{0,1\}$ these lines must be constant in the 0th direction.

By applying an invertible linear transformation to the last $n$ coordinates, we can assume without loss of generality that the lines are parallel to the axes in directions $x_1,\dots,x_m$. Let $T$ be such a transformation and let $T(P) = \{T(\alpha)|\alpha \in P\}$. Then we get that there are vectors $\beta^{(1)},\dots,\beta^{(m)} \in \mathbb{F}_q^{n+1}$ such that for every $i \in [m]$ and every $\gamma \in \mathbb{F}_q$, the vector $\beta^{(i)} + \gamma \vec{e}^{(i)} \in T(P)$, where $\vec{e}^{(i)} = (e_0^{(i)},\dots,e_n^{(i)})$ has $e_i^{(i)} = 1$ and is 0 on every other coordinate. For $i \in [m]$, let

$$L_i(x) = \sum_{j=1}^{n} \beta_j^{(i)} x_j - \beta_0^{(i)} .$$

The claim follows for this choice of $T$ and the $L_i$. □

In what follows, we assume that the affine transformation $T$ above is the identity transform (or else we can simply prove Lemma 4.18 for the function $f \circ T$).

### First step

**Claim 4.20.** *For every $i \in [m], \eta \in \mathbb{F}_q^*$, we have $f|_{x_i=\eta} \in \mathcal{F}$ (i. e., $f$ is an element of $\mathcal{F}$ when restricted to the hyperplane given by fixing $x_i$ to $\eta$).*

*Proof.* In order to prove the claim we first prove that $f|_{x_i=\eta}$ is in $\mathcal{F}^+$ and then use Theorem 4.9 to deduce that $f|_{x_i=\eta}$ is actually in $\mathcal{F}$.

Fix $x \in \mathbb{F}_q^n$ such that $x_i = \eta$ and let $\beta = L_i(x)$. By definition $x \in H_{L_i - \eta^{-1}\beta x_i}$ (note that here we use the fact that $\eta \neq 0$). We thus conclude that

$$H_{x_i-\eta} = \bigcup_{\gamma \in \mathbb{F}_q} \left(H_{x_i-\eta} \cap H_{L_i-\gamma x_i}\right).$$

In other words the hyperplane $H_{x_i-\eta}$ is covered by $q$ parallel hyperplanes in $\mathbb{F}_q^{n-1}$. Thus, since for every $\gamma \in \mathbb{F}_q$ we have $f|_{H_{L_i-\gamma x_i}} \in \mathcal{F}$, we get

$$f|_{H_{x_i-\eta} \cap H_{L_i-\gamma x_i}} \in \mathcal{F}$$

as well. We thus conclude, by Lemma 4.5, that $f|_{x_i-\eta} \in \mathcal{F}^+$.

Now, consider the set

$$S = \left\{H_{x_i-\eta} \cap H_j \mid j \in [k]\right\}.$$

Allowing for $q$ of the $H_j$ to be parallel to $H_{x_i-\eta}$ and for $q$ different subspaces $H_j$ to become identical when restricted to $H_{x_i-\eta}$, we still get $(k/q)-1 > q^{t+q^2+q+2}$ many distinct $(n-2)$-dimensional affine subspaces of $H_{x_i-\eta}$ in $S$. For each such subspace $H_j$, we have

$$f|_{H_{x_i-\eta} \cap H_j} = \left(f|_{H_j}\right)|_{H_{x_i-\eta}} \in \mathcal{F}.$$

Therefore, by Theorem 4.9 (applied to functions over $\mathbb{F}_q^{n-1}$), we get $f|_{x_i=\eta} \in \mathcal{F}$. □

**Second step**

**Claim 4.21.** *For every $i \in [m]$ there exists a function $h_i : \mathbb{F}_q^n \to \mathbb{F}_q$ with $h_i \in \mathcal{F}^+$ and $h_i|_{x_i=\eta} = f|_{x_i=\eta}$ for every $\eta \in \mathbb{F}_q^*$.*

*Proof.* Let $h_i$ be defined as $h_i(x) = f(x)$ when $x_i \neq 0$ and $h_i(x) = 0$ otherwise. Clearly we have that $h_i|_{x_i=\eta} = f|_{x_i=\eta}$ for every $\eta \in \mathbb{F}_q^*$, it remains to show that $h_i \in \mathcal{F}^+$. To see this note that Claim 4.20 above implies that for every $\eta \neq 0$, $h_i|_{x_i=\eta} = f|_{x_i=\eta} \in \mathcal{F}$. Since $\mathcal{F}$ is linear we also have that the zero function is contained in $\mathcal{F}$ and hence $h_i|_{x_i=0}$ is also contained in $\mathcal{F}$. Thus we have that $h_i$ is an interpolation of functions in $\mathcal{F}$ as per Definition 4.3. Lemma 4.5 then implies that $h_i \in \mathcal{F}^+$. □

**Third step** Our final step, which is the major step of this proof, is to collect the $h_i$ together consistently to form the function $h$. Lemma 4.22 below proves that there is a function $h \in \mathcal{F}^+$ such that $h$ agrees with $f$ on all the hyperplanes $H_{x_i-\eta}$ for $\eta \neq 0$ and $i \in [m]$. We now conclude the proof by going back to the $k$ hyperplanes $H_1, \ldots, H_k$ given by the hypothesis.

For every $j \in [k]$, we first claim that $h|_{H_j} = f|_{H_j}$. To see this, let

$$S_j = H_j \cap \left( \bigcup_{i=1}^{m} \bigcup_{\eta \neq 0} H_{x_i-\eta} \right).$$

On the one hand $f$ and $h$ agree on every point in $S_j$. On the other hand, we have $|S_j| \geq q^{n-1}(1 - q^{-(m-1)})$. Finally, we also have that $h|_{H_j}, f|_{H_j} \in \mathcal{F} \subseteq \mathcal{F}^+$. Since $\delta(\mathcal{F}^+) \geq q^{-(t+q-1)} > q^{-(m-1)}$ (since $m > t+q$) we get $f|_{H_j} = h|_{H_j}$. We now have that $h \in \mathcal{F}^+$ is a function that on $k > q^{t+q^2+q+2}$ hyperplanes $h$ restricted to the hyperplane is a function in $\mathcal{F}$. By Theorem 4.9, we have $h \in \mathcal{F}$ as desired. □

**Lemma 4.22.** *Let $\mathcal{G}$ be an affine-invariant linear code and let $h_1, \ldots, h_m, f : \mathbb{F}_q^n \to \mathbb{F}_q$ be functions such that for every $\eta \neq 0$ and $i \in [m]$, we have $h_i|_{x_i=\eta} = f|_{x_i=\eta}$, and $h_i \in \mathcal{G}$ for every $i \in [m]$. Then there exists $h \in \mathcal{G}$ such that $h|_{x_i=\eta} = f|_{x_i=\eta}$ for every $i \in [m]$ and $\eta \neq 0$.*

For the proof of the above lemma we shall need the following definition of non-standard monomials.

**Definition 4.23** (Non-standard monomials)**.** For integer $j \in \{0, \ldots, q-1\}$ we define the "non-standard" monomial $N_j(t)$ to be $t^j$ if $j \neq q-1$ and $t^j - 1$ if $j = q-1$. For a vector $a \in \{0, \ldots, q-1\}^n$ we define the non-standard monomial $N_a(x)$ to be $\prod_{i=1}^{n} N_{a_i}(x_i)$.

It is simple to see that non-standard monomials do form a basis for all functions from $\mathbb{F}_q^n \to \mathbb{F}_q$. We mention this and some other properties we will be using below.

**Proposition 4.24.**

1. *For every function $f : \mathbb{F}_q^n \to \mathbb{F}_q$ there exists a unique set of coefficients denoted $\{c_a\}_{a \in \{0,\ldots,q-1\}^n}$ such that $f(x) = \sum_a c_a N_a(x)$.*

2. *For $I \subseteq [n]$, let*
$$\mathcal{A}_I = \{a \in \{0,\dots,q-1\}^n \mid a_i \neq q-1 \ \forall i \in I\} \quad \text{and let} \quad S_I = \left\{x \in \mathbb{F}_q^n \,\middle|\, x_i \neq 0 \ \forall i \in I\right\}.$$
*Then for every function $f(x) = \sum_a c_a N_a(x)$ the coefficients $\{c_a\}_{a \in \mathcal{A}_I}$ are uniquely determined by $f|_{S_I}$.*

3. *Let $\mathcal{G}$ be an affine-invariant linear code and suppose $f = \sum_a c_a N_a(x)$ is in $\mathcal{G}$. Then for every $a$ such that $c_a \neq 0$, it holds that $N_a(x) \in \mathcal{G}$.*

*Proof.* The first part of the proposition is immediate and the second part is given as Lemma 4.13 in [15] so it remains to prove the third part. For a vector $a \in \{0,\dots,q-1\}^n$ denote by $x^a$ the (standard) monomial $\prod_{i=1}^n x_i^{a_i}$. Let $a$ be such that $c_a \neq 0$ and let $x^{a'}$ be a monomial of maximal degree such that $c_{a'} \neq 0$ and $x^a \in \mathrm{supp}(N_{a'}(x))$. Since $x^{a'}$ is of maximal degree we must have that $x^{a'} \in \mathrm{supp}(f)$ which by Lemma 3.1 implies that $x^{a'} \in \mathcal{G}$.

Note that all monomials in $\mathrm{supp}(N_{a'}(x))$ are of the form $x^b$ where $b_i = a'_i$ if $a'_i \neq q-1$ and $b_i \in \{0, q-1\}$ if $a'_i = q-1$. Since $x^a \in \mathrm{supp}(N_{a'}(x))$, in particular, we have that every monomial in $\mathrm{supp}(N_a(x))$ is of this form. By Lemma 3.2 this implies in turn that $\mathrm{supp}(N_a(x)) \subseteq \mathrm{Aff}_{n\times n}(x^{a'})$. Since $x^{a'} \in \mathcal{G}$ we conclude that $\mathrm{supp}(N_a(x)) \subseteq \mathcal{G}$ so $N_a(x) \in \mathcal{G}$ as required. □

*Proof of Lemma 4.22.* We now use the non-standard monomials. For $i \in [m]$, let $\{c_a^{(i)}\}_{a \in \{0,\dots,q-1\}^n}$ be such that $h_i(x) = \sum_a c_a^{(i)} N_a(x)$. Let
$$D = \{a \in \{0,\dots,q-1\}^n \mid \exists i \in [m] \text{ s.t. } a_i \neq q-1\}.$$
For $a \in D$, let $i(a) = \min\{i \mid a_i \neq q-1\}$. We define
$$h(x) = \sum_{a \in D} c_a^{(i(a))} N_a(x).$$
We argue below that $h$ is a member of $\mathcal{G}$ and $h$ agrees with $f$ on the hyperplanes $H_{x_i-\eta}$ for every $i \in [m]$ and $\eta \neq 0$.

The first part is simple. We first notice that every term in the non-standard expansion of $h = \sum_a c_a N_a(x)$ is in $\mathcal{G}$. Suppose $N_a(x)$ has a non-zero coefficient in the expansion of $h$. Then we have that $c_a = c_a^{i(a)}$ and so $N_a(x)$ has a non-zero coefficient in the non-standard expansion of $h_{i(a)}$. Since $h_{i(a)} \in \mathcal{G}$, it follows, from Part (3) of Proposition 4.24, that $N_a(x) \in \mathcal{G}$. Thus, every term of $h$ is in $\mathcal{G}$ and by linearity of $\mathcal{G}$ it follows that $h \in \mathcal{G}$.

It remains to argue that $h$ equals $f$ on every hyperplane of the form $x_i = \eta$ for $i \in [m]$ and $\eta \neq 0$. To see this we first claim that for $i \neq j \in [m]$ and $a \in \{0,\dots,q-1\}^n$ if $a_i, a_j \neq q-1$ then $c_a^{(i)} = c_a^{(j)}$. To see this, note that
$$h_i|_{x_i\neq 0, x_j \neq 0} = f|_{x_i\neq 0, x_j \neq 0} = h_j|_{x_i\neq 0, x_j \neq 0}.$$
But now, applying Part (2) of Proposition 4.24 to the set $I = \{i, j\}$, we get that $c_a^{(i)} = c_a^{(j)}$ as claimed. Thus, as a consequence, we have that $c_a = c_a^{(i)}$ for every $a$ such that $a_i \neq q-1$. Applying Part (2) of Proposition 4.24 again, this time to the set $I = \{i\}$, we have that $h$ and $h_i$ must agree in every $x$ such that $x_i \neq 0$. The lemma follows. □

#### 4.3.3 Proof of Theorem 4.15

We are now ready to prove Theorem 4.15.

*Proof of Theorem 4.15.* We will prove the theorem for $\tau = \max\{\tau_4 - 3, q^2 + q + 1\}$ where $\tau_4$ is the constant given by Lemma 4.18 for $c = 4$.

Recall that we wish to prove that if $f$ agrees with a function from $\mathcal{F}$ on $k$ hyperplanes (where the agreeing function may be different for each hyperplane), then there is a single function in $\mathcal{F}$ with whom $f$ agrees on all the given hyperplanes. We wish to prove this when $k \geq q^{t+\tau}$, but we will prove a slightly stronger result for the induction.

**Inductive Hypothesis:** Let $n' := n - t - \tau$, let

$$C(t,n) = \frac{q^{t+\tau}}{2\prod_{i=1}^{n'-3}\left(1 - q^{-n'+i+1}\right)}$$

and let $k \geq C(t,n)$. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function such that there exist $k$ hyperplanes $H_1, \ldots, H_k$ in $\mathbb{F}_q^n$ such that $f|_{H_i} \in \mathcal{F}$ for every $i \in [k]$. Then there exists $h \in \mathcal{F}$ such that $f|_{H_i} = h|_{H_i}$ for every $i \in [k]$.

We first note that the hypothesis does imply the theorem. This is so since the denominator in the above expression is

$$\begin{aligned} 2\prod_{i=1}^{n'-3}\left(1 - q^{-n'+i+1}\right) &\geq 2\left(1 - \sum_{i=1}^{n'-3} q^{-n'+i+1}\right) = 2 - 2q^{-n'+1}\sum_{i=1}^{n'-3} q^i \\ &> 2 - 2q^{-n'+1} \cdot q^{n'-2} = 2 - 2q^{-1} \geq 1\,, \end{aligned}$$

and so $C(t,n) \leq q^{t+\tau}$.

**Base Case ($n \leq t + \tau_4$):** In this case we have

$$k \geq C(t,n) \geq q^{t+\tau}/2 \geq q^{t+\tau-1} \geq q^{t+\tau_4-4}\,.$$

Applying Lemma 4.18 with $c = 4$, we find that we have $k \geq q^{t+\tau_c-c}$ and $n \leq t + \tau_c$ and so a function $h$ as desired exists.

**Inductive step:** In Claim 4.25 below we prove that there exists a linear function $L$ such that for every $\gamma \in \mathbb{F}_q$ the hyperplane $H_{L(x)-\gamma}$ is "good" in the sense that the set

$$S_\gamma = \left\{H_i \cap H_{L(x)-\gamma} \,\middle|\, i \in [k], \dim(H_i \cap H_{L(x)-\gamma}) = n-2\right\}$$

is of size at least $C(t, n-1)$. By induction, we conclude that for every $\gamma$ the functions $f|_{H_{L(x)-\gamma}}$ belong to $\mathcal{F}$ (since each agrees with a member of $\mathcal{F}$ on at least $C(t,n-1)$ hyperplanes). Using interpolation, we conclude the existence of a function $h \in \mathcal{F}^+$ which agrees with $f$ on all hyperplanes $H_i$. Applying Theorem 4.9 (using the fact that $\tau \geq q^2 + q + 1$ and hence $k \geq q^{t^+ + q^2 + 2}$) we now conclude that $h \in \mathcal{F}$. Details follow.

**Claim 4.25.** *There exists a linear function $L \in \mathrm{Aff}_n$ such that for every $\gamma \in \mathbb{F}_q$ the set*

$$S_\gamma = \left\{H_{L(x)-\gamma} \cap H_i \,\middle|\, i \in [k], \dim\left(H_{L(x)-\gamma} \cap H_i\right) = n-2\right\}$$

*has cardinality at least $C(t, n-1)$.*

*Proof.* Without loss of generality assume $k = C(t,n)$. Let $L_i \in \mathrm{Aff}_n$ be an affine function such that $H_i = H_{L_i}$. For $L \in \mathrm{Aff}_n$ and $i \neq j \in [k]$ such that $H_i \cap H_j \neq \emptyset$ the sets $H_{L-\gamma} \cap H_i$, $H_{L-\gamma} \cap H_j$ are the same only if there exist $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$ such that $L = \alpha L_i + \beta L_j + \gamma$. Moreover, $\dim\left(H_{L-\gamma} \cap H_i\right) \neq n-2$ only if there are $\alpha, \gamma' \in \mathbb{F}_q$ such that $L = \alpha L_i + \gamma'$.

There are at most $k^2 q^3$ ways to represent a function in $\mathrm{Aff}_n$ as $L = \alpha L_i + \beta L_j + \gamma$ where $i, j \in [k]$ and $\alpha, \beta, \gamma \in \mathbb{F}_q$. Hence there is some function $L \in \mathrm{Aff}_n$ such that there are at most

$$\frac{k^2 q^3}{|\mathrm{Aff}_n|} = \frac{k^2}{q^{n-2}}$$

such different ways to represent it (we allow $\alpha, \beta$ and $\gamma \in \mathbb{F}_q$ arbitrary to be zero to deal with the case where $L = \alpha L_i + \gamma'$). As we saw, for any hyperplane that we lose in the set $S_\gamma$ there is at least one such representation for $L$. So $|S_\gamma| \geq k - (k^2/q^{n-2})$. Calculating

$$\begin{aligned}
|S_\gamma| &\geq k - \frac{k^2}{q^{n-2}} = k\left(1 - \frac{k}{q^{n-2}}\right) \\
&\geq C(t,n)\left(1 - \frac{q^{t+\tau}}{q^{n-2}}\right) = C(t,n)\left(1 - q^{-n'+2}\right) \\
&= \left(1 - q^{-n'+2}\right) \frac{q^{t+\tau}}{2\prod_{i=1}^{n'-3}\left(1 - q^{-n'+i+1}\right)} \\
&= \frac{q^{t+\tau}}{2\prod_{i=2}^{n'-3}\left(1 - q^{-n'+i+1}\right)} \\
&= \frac{q^{t+\tau}}{2\prod_{i=1}^{n'-4}\left(1 - q^{-n'+i+2}\right)} = C(t,n-1)\,.
\end{aligned}$$ □

We are ready to continue the proof of Theorem 4.15. Consider the function $L \in \mathrm{Aff}_n$ as promised by Claim 4.25 and fix some $\gamma \in \mathbb{F}_q$. Observe that there are $C(t,n-1)$ hyperplanes of the space $H_{L-\gamma}$ of the form $H_i \cap H_{L-\gamma}$ where $i \in [k]$. On each one

$$f|_{H_i \cap H_{L-\gamma}} = \left(f|_{H_i}\right)|_{H_i \cap H_{L-\gamma}} \in \mathcal{F}\,.$$

So, by the induction hypothesis there exists some function $h_\gamma \in \mathcal{F}$ such that

$$\left(f|_{H_{L-\gamma}}\right)|_{H_i \cap H_{L-\gamma}} = \left(h_\gamma\right)|_{H_i \cap H_{L-\gamma}}$$

for all $i \in [k]$ such that $\dim(H_i \cap H_{L-\gamma}) = n-2$.

Define

$$h(x) = \sum_{\gamma \in \mathbb{F}_q} \left(\prod_{\alpha \neq \gamma} \frac{L(x) - \alpha}{\gamma - \alpha}\right) \cdot h_\gamma(x)\,.$$

By Lemma 4.5, $h$ is in $\mathcal{F}^+$. Let $i \in [k]$ and $x \in H_i$. Define $\gamma' = L(x)$, so clearly $x \in H_i \cap H_{L-\gamma'}$ and hence

$$h(x) = \sum_{\gamma \in \mathbb{F}_q} \left(\prod_{\alpha \neq \gamma} \frac{\gamma' - \alpha}{\gamma - \alpha}\right) \cdot h_\gamma(x) = h_{\gamma'}(x) = f(x)\,.$$

We saw that $h|_{H_i} = f|_{H_i}$ for any $i \in [k]$. We conclude by observing that $h \in \mathcal{F}^+$ is a function such that on $k \geq q^{t+q^2+q+1}$ hyperplanes $H$, $h|_H \in \mathcal{F}$. Hence by Theorem 4.9 $h \in \mathcal{F}$ and we are done. □

#### 4.3.4 The case of general $\delta$

We finally turn to the proof of Theorem 2.1. To prove this theorem, we shall also need the following proposition whose proof appears as part of the proof of Lemma 4.16 in [15].

**Proposition 4.26.** *Let $f,g:\mathbb{F}_q^n \to \mathbb{F}_q$ be a pair of functions such that there are $k$ hyperplanes $H_1,\dots,H_k$ which satisfy $\delta(f|_{H_i},g|_{H_i}) < \delta$ for all $1 \le i \le k$. Then*

$$\delta(f,g) \le 2\delta + \frac{4(q-1)}{k}\,.$$

We include the proof below for completeness.

*Proof.* Let $S \subseteq \mathbb{F}_q^n$ be the set of points given by

$$S \triangleq \left\{ x \in \mathbb{F}_q^n \,\middle|\, \Pr_{i\in[k]}[x \in H_i] \le 1/(2q) \right\}.$$

We claim first that $\delta(f,g) \le 2\delta + |S|/q^n$. To see this consider the following experiment: Pick a random hyperplane $H_i$ by picking $i$ uniformly from $[k]$ and pick a point $x$ uniformly at random from $\mathbb{F}_q^n$ and let $I = I(i,x) = 1$ if $x$ lies on $H_i$ and $f(x) \ne g(x)$. On the one hand we have $\mathbb{E}[I] \le \delta/q$ since the probability that $x$ lies on $H_i$ is $1/q$ and conditioned on $x \in H_i$ the probability that $f$ and $g$ disagree is at most $\delta$. On the other hand, the probability that $f$ and $g$ disagree on $x$ and $x \notin S$ is at least $\delta(f,g) - |S|/q^n$ and conditioned on $x \notin S$, the probability that $x \in H_i$ is at least $1/(2q)$. We conclude that

$$\frac{1}{2q}(\delta(f,g) - |S|/q^n) \le \frac{\delta}{q}$$

and so $\delta(f,g) \le 2\delta + |S|/q^n$. Thus it suffices to show that $|S|/q^n \le 4(q-1)/k$, which we do next (by an application of Chebychev bound).

Consider picking $x \in \mathbb{F}_q^n$ at random and let $Y_i = Y_i(x) = 1$ if $x \in H_i$. Notice $x \in S$ if and only if

$$Y(x) \triangleq \sum_{i=1}^{k} Y_i(x) < k/(2q)\,.$$

We have $\mathbb{E}[Y_i] = 1/q$ and $\mathbb{E}[Y_iY_j] \le 1/q^2$ (we have $\mathbb{E}[Y_iY_j] = 1/q^2$ if the hyperplanes are not parallel and $\mathbb{E}[Y_iY_j] = 0$ if they are). Thus $Y = \sum_{i=1}^{k} Y_i$ has expectation $k/q$ and variance

$$E[Y^2] - E[Y]^2 \le \frac{k}{q} + \frac{k(k-1)}{q^2} - \frac{k^2}{q^2} = k\frac{1}{q}\left(1 - \frac{1}{q}\right).$$

By the Chebychev bound it follows that

$$\Pr\left[Y < \frac{k}{2q}\right] \le \Pr\left[|Y - E[Y]| \ge \frac{k}{2q}\right] \le \frac{(2q)^2 k(1/q)(1-1/q)}{k^2} = \frac{4(q-1)}{k}\,.$$

The proposition follows. $\square$

We can now prove Theorem 2.1 as a corollary of Theorem 4.15 and Proposition 4.26.

*Proof of Theorem 2.1.* For all $i \in [k]$ let $g_i$ be a function in $\mathcal{F}$ such that $\delta(g_i|_{H_i}, f|_{H_i}) \le \delta$. We will show that the functions $g_1, \ldots, g_k$ are consistent with each other, namely that

$$g_i|_{H_i \cap H_j} = g_j|_{H_i \cap H_j}$$

for all $1 \le i, j \le k$.

For any $i, j \in [k]$, if $H_i \cap H_j = \emptyset$ then there is nothing to prove. Else,

$$\delta\big(g_i|_{H_i \cap H_j}, g_j|_{H_i \cap H_j}\big) \le \delta\big(g_i|_{H_i \cap H_j}, f|_{H_i \cap H_j}\big) + \delta\big(f|_{H_i \cap H_j}, g_j|_{H_i \cap H_j}\big) \le q\delta + q\delta < q^{-t}.$$

But by Corollary 3.6, the distance of $\mathcal{F}$ is at least $q^{-t}$, so $g_i$ and $g_j$ must agree on $H_i \cap H_j$. Theorem 4.15 then implies the existence of a function $g \in \mathcal{F}$ such that $g|_{H_i} = g_i|_{H_i}$ for every $i \in [k]$. By Proposition 4.26, $\delta(g, f) \le 2\delta + 4(q-1)/k$ and so $\delta_{\mathcal{F}}(f) \le 2\delta + 4(q-1)/k$ as required. □

## 5 Proof of Main Theorem 1.1, $Q = q$ case

In this section we prove our Main Theorem 1.1 for the special case in which $Q = q$. In order to prove Theorem 1.1 in this case, we first show in Lemma 5.1 below, using probabilistic arguments, bounds on the rejection probability of the $\ell$-dimensional test for the case in which $f$ is relatively close to $\mathcal{F}$ and $\ell \ge t+1$. In Lemma 5.2 we then use our Main Technical Theorem 2.1 to bound the rejection probability of the $\ell$-dimensional test for the case in which $f$ is relatively far from $\mathcal{F}$ and $\ell \ge t+c$ for some absolute constant $c$. Combining Lemmas 5.1 and 5.2 one can bound the rejection probability of the $\ell$-dimensional test when $\ell = t+c$. Relating this to the rejection probability of the $t$-dimensional test requires some extra work given in Lemma 5.3 and Corollary 5.4 below.

We start by analyzing the rejection probability of the $\ell$-dimensional test for the case in which $f$ is relatively close to $\mathcal{F}$ and $\ell \ge t+1$. Recall that $\mathrm{Rej}_\ell(f)$ denotes the probability that the $\ell$-dimensional test rejects the function $f : \mathbb{F}_q^n \to \mathbb{F}_q$.

**Lemma 5.1.** *Let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ for an affine-invariant linear base code $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$. Then for every $n \ge \ell \ge t+1$, and every $f : \mathbb{F}_q^n \to \mathbb{F}_q$, if $\delta_{\mathcal{F}}(f) \le q^{-(t+1)}/2$ then*

$$\mathrm{Rej}_\ell(f) \ge \min\left\{\frac{1}{4q}, \frac{q^\ell \delta_{\mathcal{F}}(f)}{2}\right\}.$$

*Proof.* The proof is similar to the proof of Lemma 5.1 in [15]. We will use the monotonicity of the rejection probability and prove a bound on $\mathrm{Rej}_{\ell'}(f)$ for some $\ell' \le \ell$.

Let $\ell'$ be such that $t+1 \le \ell' \le \ell$ and let $A$ be an $\ell'$-dimensional subspace. Let $g \in \mathcal{F}$ be the function closest to $f$, so that $\delta(f, g) = \delta \triangleq \delta_{\mathcal{F}}(f)$. We now use the fact that $\delta(f|_A, g|_A)$ is the average of $N = q^{\ell'}$ random $\{0,1\}$-valued variables of expectation $\delta$ that are roughly pairwise independent to derive a lower bound on the probability that $f|_A$ and $g|_A$ disagree on exactly one point. Note that if $f|_A$ and $g|_A$ disagree on exactly one point, then $\delta(f|_A, g|_A) = q^{-\ell'} < q^{-t}$ due to our assumption that $\ell' \ge t+1$. But by Corollary 3.6 we have that $\delta(\mathcal{F}) \ge q^{-t}$ and consequently $f|_A \notin \mathcal{F}$ in this case. Thus the $\ell'$-dimensional test rejects whenever $f|_A$ and $g|_A$ disagree on exactly one point and this will imply a lower bound on $\mathrm{Rej}_{\ell'}(f)$.

Let $A$ be specified by $\alpha_0,\dots,\alpha_{\ell'} \in \mathbb{F}_q^n$ such that

$$A = \left\{ A(\theta) \triangleq \alpha_0 + \sum_{i=1}^{\ell'} \theta_i \alpha_i \;\middle|\; \theta = (\theta_1,\dots,\theta_{\ell'}) \in \mathbb{F}_q^{\ell'} \right\}.$$

Fix $\theta \in \mathbb{F}_q^{\ell'}$, and let $X(\theta)$ denote the random variable that is 1 if $f(A(\theta)) \neq g(A(\theta))$ and 0 otherwise, where $A$ is a uniform $\ell'$-dimensional affine subspace. We note that for every $\theta \in \mathbb{F}_q^{\ell'}$, we have $\mathbb{E}_A[X(\theta)] = \delta$. Furthermore, for every pair of distinct points $\theta,\eta \in \mathbb{F}_q^{\ell'}$ we have $\mathbb{E}_A[X(\theta)X(\eta)] \leq \delta^2$. (If the points $\alpha_1,\dots,\alpha_{\ell'}$ were not required to be linearly independent, this expectation would be exactly $\delta^2$. But because we insist that they are independent we get that $A(\theta)$ and $A(\eta)$ are two distinct random points in $\mathbb{F}_q^n$ and so the bound above is a (strict) inequality.) Furthermore we have

$$\delta(f|_A, g|_A) = q^{-\ell'} \sum_{\theta} X(\theta).$$

Thus we have

$$\Pr\left[\delta(f|_A,g|_A) = q^{-\ell'}\right] = \Pr_A\left[q^{-\ell'}\sum_{\theta} X(\theta) = q^{-\ell'}\right] \geq q^{\ell'}\delta(1-(q^{\ell'}-1)\delta) \geq q^{\ell'}\delta(1-q^{\ell'}\delta).$$

When $\delta \leq (1/2)q^{-\ell}$ the bound above implies that $\mathrm{Rej}_{\ell}(f) \geq (1/2)q^{\ell}\delta$. Else, let $\ell'$ be the largest integer such that $\delta \leq (1/2)q^{-\ell'}$ (and so $\delta > (1/2q)q^{-\ell'}$). Note that the assumption that $\delta_{\mathcal{F}}(f) \leq q^{-(t+1)}/2$ implies that $\ell' \geq t+1$. We then get

$$\mathrm{Rej}_{\ell}(f) \geq \mathrm{Rej}_{\ell'}(f) \geq \frac{1}{2}q^{\ell'}\delta > \frac{1}{4q}.$$

The lemma follows. □

Next we bound the rejection probability of the $\ell$-dimensional test in the case in which $f$ is relatively far from $\mathcal{F}$ and $\ell \geq t+c$ for some absolute constant $c$.

**Lemma 5.2.** *Let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ for an affine-invariant linear base code $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$. Then for every $q$ there exist $\varepsilon > 0$ and $c$ such that if $n \geq \ell \geq t+c$ we have the following: For every $f : \mathbb{F}_q^n \to \mathbb{F}_q$ with $\delta_{\mathcal{F}}(f) \geq q^{-\ell}$ we have*

$$\mathrm{Rej}_{\ell}(f) \geq \varepsilon + \frac{1}{16}q^{\ell}\sum_{i=n+1}^{\infty} q^{-i}.$$

*Proof.* The proof is identical to the proof of Lemma 5.2 in [15]. Let $c = \max\{\tau+3, 9\}$ where $\tau$ is the constant from Theorem 2.1.

We prove the lemma by induction on $n$. The base case $n = \ell$ is straightforward since in this case $\mathrm{Rej}_{\ell}(f) = 1$ and

$$\frac{1}{16}q^{\ell}\sum_{i=n+1}^{\infty} q^{-i} \leq \frac{1}{16(q-1)} \leq \frac{1}{16}$$

and so this case holds for every $\varepsilon \leq 15/16$.

For the inductive step, let $H_1,\ldots,H_k$ be all hyperplanes which satisfy $\delta_{\mathcal{L}_{n-1}}(f|_{H_i}) \leq q^{-\ell}$. If $k < (1/16)q^{\ell}$ then we are done by induction since

$$\mathrm{Rej}_\ell(f) = \mathbb{E}_H[\mathrm{Rej}_\ell(f|_H)] \geq \varepsilon + \frac{1}{16}q^{\ell}\sum_{i=n}^{\infty} q^{-i} - \frac{k}{q^n} \geq \varepsilon + \frac{1}{16}q^{\ell}\sum_{i=n+1}^{\infty} q^{-i}$$

as desired.

Finally we are left with the case where $k \geq (1/16)q^{\ell}$. In this case we use Theorem 2.1 to show that $\delta_{\mathcal{F}}(f)$ is small and then use Lemma 5.1 to show that $\mathrm{Rej}_\ell(f)$ is large. Specifically, by Theorem 2.1 we have

$$\delta_{\mathcal{F}}(f) \leq 2q^{-\ell} + \frac{4(q-1)}{k} \leq (2+64q)\cdot q^{-\ell} \leq (66q)\cdot q^{-\ell}.$$

Since $\ell \geq t+c$ and $c \geq 9$ we have $\delta_{\mathcal{F}}(f) < q^{-t}/2$ and so by Lemma 5.1 we have

$$\mathrm{Rej}_\ell(f) \geq \min\left\{\frac{1}{4q}, \frac{q^{\ell}\delta_{\mathcal{F}}(f)}{2}\right\} \geq \frac{1}{4q} \geq \varepsilon + \frac{1}{16(q-1)} = \varepsilon + \frac{1}{16}q^{\ell}\sum_{i=\ell+1}^{\infty} q^{-i}$$

for every $\varepsilon < 1/(32q)$. So the lemma is true for $\varepsilon = 1/(32q)$. □

As noted above, Lemmas 5.1 and 5.2 suffice to analyze the rejection probability of a sufficiently high dimensional test ($\ell = t+c$), but not the $t$-dimensional test. To relate the two we use a lemma similar to Lemma 4.7 from [15]. We note that the proof again gets new complications since our result is more general.

**Lemma 5.3.** *Let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ for an affine-invariant linear code $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function such that $f \notin \mathcal{F}$. Then $\Pr_H[f|_H \notin \mathcal{F}] \geq 1/q$ where the probability is over a hyperplane $H$ chosen uniformly in $\mathbb{F}_q^n$.*

*Proof.* Since $f \notin \mathcal{F}$ there exists an affine transformation $T \in \mathrm{Aff}_{n\times n}$ such that

$$f \circ T|_{x_{t+1}=\cdots=x_n=0}$$

is not in $\mathcal{B}$. To simplify notation, assume $T$ is the identity. We now bound the number of hyperplanes $H$ such that $f|_H \in \mathcal{F}$. Each hyperplane can be written as

$$H_\alpha = \left\{ x \in \mathbb{F}_q^n \;\middle|\; x_c = \sum_{i=c+1}^{n} \alpha_i x_i + \alpha_0 \right\}$$

for $\alpha = (\alpha_0,\ldots,\alpha_n) \in \mathbb{F}_q^{n+1}$, where $c \geq 1$ is the first coordinate such that $\alpha_c \neq 0$. For such a hyperplane define

$$f_\alpha := f\left(x_1,\ldots,x_{c-1}, \sum_{i=c+1}^{n} \alpha_i x_i + \alpha_0, x_{c+1},\ldots,x_n\right).$$

Observe that $f|_{H_\alpha} \in \mathcal{F}$ if and only if $f_\alpha \in \mathcal{F}$.

We divide into cases according to the value of $c$. For any hyperplane $H_\alpha$ for which $c > t$ we will show the existence of a hyperplane $H_{\alpha'}$, where $\alpha'$ may differ from $\alpha$ only by the 0-th coordinate, such that $f|_{H_{\alpha'}} \notin \mathcal{F}$. Similarly, for any hyperplane $H_\alpha$ for which $1 \le c \le t$ we will show the existence of a hyperplane $H_{\alpha'}$, where $\alpha'$ may differ from $\alpha$ only by the $n$-th coordinate, such that $f|_{H_{\alpha'}} \notin \mathcal{F}$. This will prove the claim since it will map at most $q$ different hyperplanes to one "good" hyperplane.

First, consider the case where $c > t$. In this case consider $\alpha'$ such that $\forall i > 0 : \alpha'_i = \alpha_i$ and $\alpha'_0 = 0$. Then

$$f_{\alpha'}|_{x_{t+1}=\cdots=x_n=0} = f|_{x_{t+1}=\cdots=x_n=0} \notin \mathcal{B},$$

hence $f_{\alpha'} \notin \mathcal{F}$ which implies in turn that $f|_{H_{\alpha'}} \notin \mathcal{F}$.

Next assume that $1 \le c \le t$ and for a variable $z$, let $\alpha(z) \in \mathbb{F}_q^{n+1}$ denote the vector which satisfies $\alpha(z)_i = \alpha_i$ for all $i \ne n$ and $\alpha(z)_n = z$. Our goal will be to show that there exists an assignment $\beta \in \mathbb{F}_q$ to $z$ for which $f_{\alpha(\beta)} \notin \mathcal{F}$. In order to do so we shall show that there exists a monomial $M$ in variables $x_1, \ldots, x_n$ in $\mathrm{supp}(f_{\alpha(z)})$ such that $M \notin \mathcal{F}$ and the coefficient of $M$ is a non-zero polynomial in the variable $z$. This will imply in turn that there exists an assignment $\beta \in \mathbb{F}_q$ to $z$ such that $M$ has a non-zero coefficient in $f_{\alpha(\beta)}$ and consequently $f_{\alpha(\beta)} \notin \mathcal{F}$.

Consider the affine transformation $B \in \mathrm{Aff}_{n\times n}$ which satisfies

$$\forall i \ne c : B(e_i) = e_i \quad \text{and} \quad B(e_c) = e_c + \sum_{i=c+1}^{n-1} \alpha_i e_i + \alpha_0$$

and the affine transformation $B' \in \mathrm{Aff}_{t\times t}$ which satisfies

$$\forall i \ne c : B'(e_i) = e_i \quad \text{and} \quad B'(e_c) = e_c + \sum_{i=c+1}^{t} \alpha_i e_i + \alpha_0 .$$

Observe that

$$f \circ B|_{x_{t+1}=\cdots=x_n=0} = \left(f|_{x_{t+1}=\cdots=x_n=0}\right) \circ B' \notin \mathcal{B} .$$

Therefore, there exists a monomial $M = \prod_{i=1}^{t} x_i^{a_i}$, containing only the variables $x_1, \ldots, x_t$, that is in $\mathrm{supp}(f \circ B)$ but not in $\mathrm{supp}(\mathcal{B})$. By Claim 3.4, we also have that $M \notin \mathrm{supp}(\mathcal{F})$. Note next that the function $f_{\alpha(z)}$ is obtained from $f \circ B$ by substituting $x_c$ with $zx_n$. This implies in turn that the monomial

$$z^{a_c} x_n^{a_c} \prod_{i\in[t]\setminus\{c\}} x_i^{a_i}$$

is a monomial of $f_{\alpha(z)}$ when viewed as a function of the variables $\{x_i\}_{i\ne c}$ and $z$.

Now view $f_{\alpha(z)}$ as a function of $\{x_i\}_{i\ne c}$ with coefficients that are functions of $z$. Then the coefficient of the monomial

$$M' = x_n^{a_c} \prod_{i\in[t]\setminus\{c\}} x_i^{a_i}$$

is a non-zero polynomial in $z$. Hence, there is some value $\beta \in \mathbb{F}_q$ such that if we substitute $z = \beta$ then the coefficient of $M'$ will be non-zero. In particular, $f_{\alpha(\beta)}$ has the monomial $M'$ in its support. The proof is completed by noting that $M \in \mathrm{Aff}_{n\times n}(M')$ and hence the fact that $M \notin \mathcal{F}$ implies that $M' \notin \mathcal{F}$. Consequently, $f_{\alpha(\beta)} \notin \mathcal{F}$. □

By applying the above lemma iteratively we obtain the following corollary.

**Corollary 5.4.** *Let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$ for an affine-invariant linear code $\mathcal{B} \subseteq \{\mathbb{F}_q^t \to \mathbb{F}_q\}$ and let $n \geq \ell \geq k \geq t$. Let $f : \mathbb{F}_q^n \to \mathbb{F}_q$ be a function such that $f \notin \mathcal{F}$. Then $\mathrm{Rej}_k(f) \geq \mathrm{Rej}_\ell(f) \cdot q^{-(\ell-k)}$.*

*Proof.* The proof is by induction on $k$. The base case, where $k = \ell$ is trivial. Now assume the corollary holds for $k = r+1$ and we will prove it for $k = r$. Consider the following way of choosing a random $r$-dimensional affine subspace. First choose a random $(r+1)$-dimensional affine subspace $V' \subseteq \mathbb{F}_q^n$ and then choose a random $r$-dimensional affine subspace $V \subseteq V'$. Then

$$\begin{aligned}\mathrm{Rej}_r(f) = \Pr\left[f|_V \notin \mathcal{F}\right] &\geq \Pr\left[f|_V \notin \mathcal{F} \;\middle|\; f|_{V'} \notin \mathcal{F}\right] \Pr\left[f|_{V'} \notin \mathcal{F}\right] \\ &\geq \frac{1}{q} \cdot \mathrm{Rej}_\ell(f) \cdot q^{-(\ell-(r+1))} = \mathrm{Rej}_\ell(f) \cdot q^{-(\ell-r)},\end{aligned}$$

where the last inequality is obtained by the induction hypothesis and Lemma 5.3. □

*Proof of Theorem 1.1, $Q = q$ case.* Follows immediately from Lemmas 5.1 and 5.2 and Corollary 5.4. □

## 6 Proof of Main Theorem 1.1, general $Q$

In this section we prove Theorem 1.1 for the case in which $Q \neq q$ via a simple reduction to the $Q = q$ case. For this we shall need several facts concerning affine-invariant linear codes from $\mathbb{F}_Q^n$ to $\mathbb{F}_q$. The following lemma is a generalization of the monomial extraction lemma (Lemma 3.1) for such codes.

**Lemma 6.1** ([13, Proposition 2.2])**.** *Let $\mathcal{F} \subseteq \left\{\mathbb{F}_Q^n \to \mathbb{F}_q\right\}$ be an affine-invariant linear code. Then*

$$\mathcal{F} = \left\{ f : \mathbb{F}_Q^n \to \mathbb{F}_q \mid \mathrm{supp}(f) \subseteq \mathrm{supp}(\mathcal{F}) \right\}.$$

Let $Q = q^s$ for an integer $s$, and let Trace denote the trace function from $\mathbb{F}_Q$ to $\mathbb{F}_q$ given by

$$\mathrm{Trace}(x) = x + x^q + \cdots + x^{q^{s-1}}.$$

The following lemma says that if a monomial belongs to the support of an affine-invariant linear code then its trace belongs to the code.

**Lemma 6.2** ([13, Lemma A.7.])**.** *Let $\mathcal{F} \subseteq \{\mathbb{F}_Q^n \to \mathbb{F}_q\}$ be an affine-invariant linear code, and suppose that $M \in \mathrm{supp}(\mathcal{F})$. Then $\mathrm{Trace}(\alpha M) \in \mathcal{F}$ for every $\alpha \in \mathbb{F}_Q$.*

The above lemma yields the following corollary.

**Corollary 6.3.** *Let $\mathcal{F} \subseteq \{\mathbb{F}_Q^n \to \mathbb{F}_q\}$ be an affine-invariant linear code, and suppose that $f \in \mathcal{F}$. Then $\mathrm{Trace}(\alpha f) \in \mathcal{F}$ for every $\alpha \in \mathbb{F}_Q$.*

*Proof.* Let $f = \sum_{M\in\mathcal{M}_n} c_M M$ for $c_M \in \mathbb{F}_Q$. Lemma 6.2 implies that $\mathrm{Trace}(\alpha c_M M) \in \mathcal{F}$ for every $M \in \mathcal{M}_n$ and $\alpha \in \mathbb{F}_Q$. By linearity of the trace function, we have that

$$\mathrm{Trace}(\alpha f) = \sum_{M\in\mathcal{M}_n} \mathrm{Trace}(\alpha c_M M),$$

and hence $\mathrm{Trace}(\alpha f) \in \mathcal{F}$ by linearity of $\mathcal{F}$. □

*Proof of Theorem 1.1, $Q \neq q$ case.* Let $\mathcal{B}'$ be the $\mathbb{F}_Q$-span of $\mathcal{B}$, i. e.,

$$\mathcal{B}' = \left\{ \sum_i \alpha_i f_i \;\middle|\; f_i \in \mathcal{B}, \alpha_i \in \mathbb{F}_Q \right\},$$

and let $\mathcal{F}' = \mathrm{Lift}_n(\mathcal{B}')$. Note that $\mathcal{B}'$ is an affine-invariant linear code from $\mathbb{F}_Q^t$ to $\mathbb{F}_Q$.

We start by showing that $\mathcal{B}' \neq \left\{\mathbb{F}_Q^t \to \mathbb{F}_Q\right\}$. To see this note that our assumption that $\mathcal{B} \neq \left\{\mathbb{F}_Q^t \to \mathbb{F}_q\right\}$, together with Lemma 6.1, imply that there exists a monomial $M \in \mathcal{M}_t$ such that $M \notin \mathrm{supp}(\mathcal{B})$. Since $\mathcal{B}$ and $\mathcal{B}'$ have the same set of monomials in their support, we have that $M \notin \mathrm{supp}(\mathcal{B}')$ and hence $\mathcal{B}' \neq \left\{\mathbb{F}_Q^t \to \mathbb{F}_Q\right\}$.

We have just shown that $\mathcal{B}' \subsetneq \left\{\mathbb{F}_Q^t \to \mathbb{F}_Q\right\}$ is an affine-invariant linear code. Hence Theorem 1.1 for the $Q = q$ case implies a local tester $T$ for $\mathcal{F}'$ which makes $Q^t$ queries, accepts every function $f \in \mathcal{F}'$ and rejects every function $f \in \left\{\mathbb{F}_Q^n \to \mathbb{F}_Q\right\} \setminus \mathcal{F}'$ with probability at least $\varepsilon_Q \delta_{\mathcal{F}'}(f)$.

We claim that $T$ is also a local tester for $\mathcal{F}$ with the same soundness parameter $\varepsilon_Q$ and consequently $\mathcal{F}$ is $(Q^t, \varepsilon_Q, Q^{-t})$-locally testable. For this it suffices to show that $\delta_{\mathcal{F}'}(f) = \delta_{\mathcal{F}}(f)$ for every function $f : \mathbb{F}_Q^n \to \mathbb{F}_q$.

Fix $f : \mathbb{F}_Q^n \to \mathbb{F}_q$. Since $\mathcal{B} \subseteq \mathcal{B}'$, we clearly have that $\mathcal{F} \subseteq \mathcal{F}'$, and consequently $\delta_{\mathcal{F}'}(f) \leq \delta_{\mathcal{F}}(f)$. It remains to show that $\delta_{\mathcal{F}'}(f) \geq \delta_{\mathcal{F}}(f)$. To see this, let $g \in \mathcal{F}'$ be such that $\delta_{\mathcal{F}'}(f) = \delta(f, g)$. Then clearly $\delta(f, \mathrm{Trace}(g)) \leq \delta(f, g)$. Next we show that $\mathrm{Trace}(g) \in \mathcal{F}$ and so $\delta_{\mathcal{F}'}(f) \geq \delta_{\mathcal{F}}(f)$.

We need to show that $\mathrm{Trace}(g)|_A \in \mathcal{B}$ for every $t$-dimensional affine subspace $A$. Let $A$ be a $t$-dimensional affine subspace. Since $g \in \mathcal{F}'$ we have that $g|_A \in \mathcal{B}'$, so $g|_A = \sum_i \alpha_i f_i$ for $f_i \in \mathcal{B}$ and $\alpha_i \in \mathbb{F}_Q$. Hence $\mathrm{Trace}(g)|_A = \mathrm{Trace}(g|_A) = \sum_i \mathrm{Trace}(\alpha_i f_i)$ by linearity of the trace function. By Corollary 6.3 we have that $\mathrm{Trace}(\alpha_i f_i) \in \mathcal{B}$ for all $i$. Finally, by linearity of $\mathcal{B}$, this implies that $\mathrm{Trace}(g)|_A \in \mathcal{B}$ which completes the proof of the Theorem. □

## 7 New testable codes

In this section, we give some examples of codes with "nice" parameters that are testable with absolute soundness based on our main theorem (Theorem 1.1).

The need for such codes is motivated by the work of Barak et al. [3]. Their work used appropriate Reed–Muller codes over the domain $\mathbb{F}_2^n$. Our work gives the second family of codes that is known to satisfy their requirements. We point out that Guo et al. [14] also give codes motivated by the work of [3], but their codes are not, thus far, known to be testable with absolute soundness and so fail to meet all the requirements of [3]. Our codes fall within the class of "lifted" codes studied by [14], but were not analyzed there. Here we use analysis similar to their to analyze the rate and distance of our codes, while the testing follows from our main theorem.

**The code.** Our codes are defined by three parameters: a real number $\varepsilon > 0$ and a pair of integers $s$ and $n$. The code $\mathcal{F} = \mathcal{F}_{\varepsilon,s,n}$ is obtained as follows: Let $Q = 2^s$, $q = 2$ and let $\ell = \lfloor (1/s) \log 1/\varepsilon \rfloor$. Let

$$\mathcal{B} = \left\{ f : \mathbb{F}_Q^{n-\ell} \to \mathbb{F}_q \;\middle|\; \sum_{\vec{x} \in \mathbb{F}_Q^{n-\ell}} f(\vec{x}) = 0 \right\}.$$

Let $\mathcal{F} = \mathrm{Lift}_n(\mathcal{B})$.

**Basic parameters:**

**Proposition 7.1.** *For every $\varepsilon, s$ and $n$ the code $\mathcal{F} = \mathcal{F}_{\varepsilon,s,n}$ has block length $N = 2^{sn}$, (absolute, non-normalized) distance at least $1/\varepsilon$ and dimension at least*

$$2^{sn} - \left( \binom{n}{\ell}^s + \sum_{i=0}^{s\ell-1} \binom{ns}{i} \right).$$

*Proof.* The block length can be easily verified and the distance follows from Proposition 3.5 and Lemmas 3.11 and 3.12 in Guo et al. [14] Lemmas 3.11 and 3.12 from Guo et al. [14] who analyzed the dimension of the code $\mathcal{F}_{\varepsilon,s,n}$ for the case in which $s = \log(1/\varepsilon)$ (so $\ell = 1$). More specifically, given a degree pattern $a = (a_1, \dots, a_n)$ with $\{a_i\}_{i=1}^n \subseteq \{0, \dots, Q-1\}$, let $a_i^{(j)}$ denote the $j$-th bit of the binary expansion of $a_i$. Let $M(a)$ denote the $n \times s$ matrix with entries $M(a)_{i,j} = a_i^{(j)}$. Guo et al. show that in the special case in which $\ell = 1$ the code $\mathcal{F}_{\varepsilon,s,n}$ contains in its support all monomials with degree pattern $a = (a_1, \dots, a_n)$ such that there exists a column in $M(a)$ with at least two zeroes. This readily implies a bound of $2^{sn} - (n+1)^\ell$ on the dimension of their code.

A similar analysis shows that our code $\mathcal{F}_{\varepsilon,s,n}$ contains all monomials with degree pattern $a = (a_1, \dots, a_n)$ where the matrix $M(a)$ has at least $s\ell + 1$ zeroes, or the matrix has $s\ell$ zeroes and there exists a column in $M(a)$ with at least $\ell + 1$ zeros. The lower bound on the dimension follows. □

**Testability:** The following is an immediate application of Theorem 1.1.

**Proposition 7.2.** *For every $s$ there exists a constant $\tau > 0$ such that for every $\varepsilon$ and $n$ the code $\mathcal{F} = \mathcal{F}_{\varepsilon,s,n}$ is testable by a test that makes $\varepsilon N$ queries, accepts codewords with probability one, while rejecting all functions $f : \mathbb{F}_Q^n \to \mathbb{F}_q$ with probability at least $\tau \cdot \delta_{\mathcal{F}}(f)$.*

We remark that the dimension of our codes, for any choice of $N$ and $\varepsilon$ is strictly better than that of the codes used in [3] which have dimension

$$2^{sn} - \sum_{i=0}^{s\ell} \binom{sn}{i} \approx 2^{sn} - \frac{1}{\sqrt{2\pi s\ell}} (en/\ell)^{s\ell}.$$

An important parameter for them is the codimension of their code (block length minus the dimension, or the dimension of the dual code), which thus turns out to be roughly

$$\frac{1}{\sqrt{2\pi s\ell}} (en/\ell)^{s\ell}$$

from the above expression. (A smaller codimension is better for their application.) Simplifying the dimension of our code from Proposition 7.1, we see that the codimension of our code is smaller by a multiplicative factor of roughly $O(\ell^{s/2-1})$, making our codes noticeably better. Unfortunately such changes do not alter the essential relationship between $N = 2^{sn}$, the parameter $\varepsilon$ (which determines the locality of the tester) and the codimension of the code. The following theorem summarizes the performance of our codes.

**Theorem 7.3.** *For every positive $s$ there exists a constant $\tau$ such that for every sufficiently small $\varepsilon$ and sufficiently large $N$ there exists a binary code of block length $N$, codimension*

$$\left(\log \frac{1}{\varepsilon}\right)^{-s} \cdot \left(\frac{e \log N}{\log \frac{1}{\varepsilon}}\right)^{\log \frac{1}{\varepsilon}}$$

*that is testable with a tester that makes $\varepsilon \cdot N$ queries accepting codewords with probability one, while rejecting words at distance $\delta$ from the code with probability at least $\tau \cdot \delta$.*

To contrast, the corresponding result in [3] would assert the existence of a positive constant $s$ for which the above held.

## References


[1] NOGA ALON, TALI KAUFMAN, MICHAEL KRIVELEVICH, SIMON LITSYN, AND DANA RON: Testing Reed-Muller codes. *IEEE Trans. Inform. Theory*, 51(11):4032–4039, 2005. prrr RANDOM'03. [doi:10.1109/TIT.2005.856958] 302

[2] SANJEEV ARORA AND MADHU SUDAN: Improved low-degree testing and its applications. *Combinatorica*, 23(3):365–426, 2003. Preliminary version in STOC'97 and ECCC. [doi:10.1007/s00493-003-0025-0] 302

[3] BOAZ BARAK, PARIKSHIT GOPALAN, JOHAN HÅSTAD, RAGHU MEKA, PRASAD RAGHAVENDRA, AND DAVID STEURER: Making the long code shorter, with applications to the unique games conjecture. In *Proc. 53rd FOCS*. IEEE Comp. Soc. Press, 2012. Preliminary version in ECCC. [doi:10.1109/FOCS.2012.83] 301, 303, 333, 334, 335

[4] ELI BEN-SASSON, ELENA GRIGORESCU, GHID MAATOUK, AMIR SHPILKA, AND MADHU SUDAN: On sums of locally testable affine invariant properties. In *Proc. 15th Internat. Workshop on Randomization and Computation (RANDOM'11)*, pp. 400–411. Springer, 2011. Available at author's website and ECCC. [doi:10.1007/978-3-642-22935-0_34] 300, 306

[5] ELI BEN-SASSON, GHID MAATOUK, AMIR SHPILKA, AND MADHU SUDAN: Symmetric LDPC codes are not necessarily locally testable. In *Proc. 26th IEEE Conf. on Computational Complexity (CCC'11)*, pp. 55–65. IEEE Comp. Soc. Press, 2011. Preliminary version in ECCC. [doi:10.1109/CCC.2011.14] 300, 301, 306

[6] ELI BEN-SASSON AND MADHU SUDAN: Limits on the rate of locally testable affine-invariant codes. In *Proc. 15th Internat. Workshop on Randomization and Computation (RANDOM'11)*, volume 6845 of *Lecture Notes in Computer Science*, pp. 412–423. Springer, 2011. Preliminary version in ECCC. [doi:10.1007/978-3-642-22935-0_35] 300, 306

[7] ARNAB BHATTACHARYYA, ELDAR FISCHER, HAMED HATAMI, POOYA HATAMI, AND SHACHAR LOVETT: Every locally characterized affine-invariant property is testable. In *Proc. 45th STOC*, pp. 429–436. ACM Press, 2013. Preliminary version in ECCC. [doi:10.1145/2488608.2488662] 303

[8] ARNAB BHATTACHARYYA, SWASTIK KOPPARTY, GRANT SCHOENEBECK, MADHU SUDAN, AND DAVID ZUCKERMAN: Optimal testing of Reed-Muller codes. In *Proc. 51st FOCS*, pp. 488–497. IEEE Comp. Soc. Press, 2010. Available at ITCS'10 and ECCC. [doi:10.1109/FOCS.2010.54] 301, 303, 304, 305, 306

[9] MANUEL BLUM, MICHAEL LUBY, AND RONITT RUBINFELD: Self-testing/correcting with applications to numerical problems. *J. Comput. System Sci.*, 47(3):549–595, 1993. Preliminary version in STOC'90. [doi:10.1016/0022-0000(93)90044-W] 302

[10] HILLEL FURSTENBERG AND YITZHAK KATZNELSON: A density version of the Hales-Jewett theorem. *J. d'Analyse Math.*, 57(1):64–119, 1991. [doi:10.1007/BF03041066] 320

[11] ELENA GRIGORESCU, TALI KAUFMAN, AND MADHU SUDAN: Succinct representation of codes with applications to testing. *SIAM J. Discrete Math.*, 26(4):1618–1634, 2012. Preliminary versions in RANDOM'09 and ECCC. [doi:10.1137/100818364] 300, 306

[12] ELENA GRIGORESCU, TALI KAUFMAN, AND MADHU SUDAN: 2-Transitivity is insufficient for local testability. *Comput. Complexity*, 22(1):137–158, 2013. Preliminary version in CCC'08. [doi:10.1007/s00037-012-0055-3] 300, 306

[13] ALAN GUO, SWASTIK KOPPARTY, AND MADHU SUDAN: New affine-invariant codes from lifting. *Electron. Colloq. on Comput. Complexity (ECCC)*, TR12-019, 2012. 309, 332

[14] ALAN GUO, SWASTIK KOPPARTY, AND MADHU SUDAN: New affine-invariant codes from lifting. In *ITCS'13*, pp. 529–540, 2013. Preliminary version in ECCC. [doi:10.1145/2422436.2422494] 300, 301, 302, 303, 333, 334

[15] ELAD HARAMATY, AMIR SHPILKA, AND MADHU SUDAN: Optimal testing of multivariate polynomials over small prime fields. *SIAM J. Comput.*, 42(2):536–562, 2013. Preliminary versions in FOCS'11 and ECCC. [doi:10.1137/120879257] 301, 302, 303, 304, 305, 306, 307, 312, 319, 320, 321, 324, 327, 328, 329, 330

[16] CHARANJIT S. JUTLA, ANINDYA C. PATTHAK, ATRI RUDRA, AND DAVID ZUCKERMAN: Testing low-degree polynomials over prime fields. *Random Structures Algorithms*, 35(2):163–193, 2009. Preliminary version in FOCS'04. [doi:10.1002/rsa.20262] 302

[17] TALI KAUFMAN AND DANA RON: Testing polynomials over general fields. *SIAM J. Comput.*, 36(3):779–802, 2006. Preliminary verison found in FOCS'04. [doi:10.1137/S0097539704445615] 302

[18] TALI KAUFMAN AND MADHU SUDAN: Algebraic property testing: The role of invariance. *Electron. Colloq. on Comput. Complexity (ECCC)*, TR07-111, 2007. 300, 302, 303, 306, 308, 310

[19] TALI KAUFMAN AND MADHU SUDAN: Algebraic property testing: the role of invariance. In *Proc. 40th STOC*, pp. 403–412. ACM Press, 2008. Expanded version in ECCC. [doi:10.1145/1374376.1374434] 303, 304

[20] D. H. J. POLYMATH: A new proof of the density Hales-Jewett theorem. *Ann. Math.*, 175(3):1283–1327, 2012. Preliminary version in CoRR. [doi:10.4007/annals.2012.175.3.6] 320

[21] RAN RAZ AND SHMUEL SAFRA: A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP. In *Proc. 29th STOC*, pp. 475–484. ACM Press, 1997. [doi:10.1145/258533.258641] 302, 304

[22] NOGA RON-ZEWI AND MADHU SUDAN: A new upper bound on the query complexity of testing generalized Reed-Muller codes. *Theory of Computing*, 9(25):783–807, 2013. Preliminary version in RANDOM'12. [doi:10.4086/toc.2013.v009a025] 302

[23] RONITT RUBINFELD AND MADHU SUDAN: Robust characterizations of polynomials with applications to program testing. *SIAM J. Comput.*, 25(2):252–271, 1996. [doi:10.1137/S0097539793255151] 302

## AUTHORS

Elad Haramaty
Northeastern University
eladh@cs.technion.ac.il

Noga Ron-Zewi
Institute for Advanced Study, Princeton, and
Rutgers University
nogazewi@ias.edu
https://sites.google.com/site/nogazewi/

Madhu Sudan
Microsoft Research New England, Cambridge, MA
madhu@mit.edu
http://people.csail.mit.edu/madhu/

## ABOUT THE AUTHORS

ELAD HARAMATY is a postdoctoral researcher at Northeastern University in the College of Computer and Information Science, hosted by Emanuele Viola. He earned his Ph. D. from the Technion - Israel Institute of Technology under the guidance of Amir Shpilka. His research interests lie in a broad range of areas of theoretical computer science, especially in algebraic complexity. In his work he has studied mostly the structure, testability and applications of polynomials and algebraic codes. This paper was written while Elad was a Ph. D. student at the Technion.

NOGA RON-ZEWI is an IAS-DIMACS postdoc with a joint postdoctoral position at the Institute for Advanced Study (IAS) at Princeton and the Center for Discrete Mathematics and Theoretical Computer Science (DIMACS) at Rutgers. Her hosts are Avi Wigderson and Michael Saks. She received her Ph. D. from the Department of Computer Science at the Technion in 2014, under the supervision of Eli Ben-Sasson. Her research interests are in the theory of computation, with a focus on computational aspects of communication and coding. This paper was written while Noga was a Ph. D. student at the Technion.

MADHU SUDAN received his Ph. D. from the University of California at Berkeley in 1992. From 1992 to 1997 he was a research staff member at IBM's Thomas J. Watson Research Center. From 1997 to 2009 he was a faculty member at the Electrical Engineering and Computer Science Department at the Massachusetts Institute of Technology. He is currently a Principal Researcher at Microsoft Research New England. His research has focused on Probabilistic Checking of Proofs, List-Decoding, Property Testing, and Semantic Communication.