Electronic Colloquium on Computational Complexity, Report No. 104 (2022)

On One-Sided Testing Affine Subspaces

Nader H. Bshouty
Dept. of Computer Science
Technion, Haifa, Israel.

July 18, 2022

Abstract

We study the query complexity of one-sided ϵ-testing the class of Boolean functions $f:\mathcal{F}^n\to\{0,1\}$ that describe affine subspaces and Boolean functions that describe axis-parallel affine subspaces, where $\mathcal{F}$ is any finite field. We give a polynomial-time ϵ-testers that ask $\tilde{O}(1/\epsilon)$ queries. This improves the query complexity $\tilde{O}(|\mathcal{F}|/\epsilon)$ in [16].

We then show that any one-sided ϵ-tester with proximity parameter $\epsilon<1/|\mathcal{F}|^d$ for the class of Boolean functions that describe $(n-d)$-dimensional affine subspaces and Boolean functions that describe axis-parallel $(n-d)$-dimensional affine subspaces must make at least $\Omega(1/\epsilon+|\mathcal{F}|^{d-1}\log n)$ and $\Omega(1/\epsilon+|\mathcal{F}|^{d-1}n)$ queries, respectively. This improves the lower bound $\Omega(\log n/\log\log n)$ that is proved in [16] for $\mathcal{F}=\mathrm{GF}(2)$. We also give testers for those classes with query complexity that almost match the lower bounds.[1]

1 Introduction

Property testing of Boolean function was first considered in the seminal works of Blum, Luby, and Rubinfeld [3] and Rubinfeld and Sudan [22] and has recently become a very active research area. See, for example, the works referenced in the surveys and books [12, 14, 20, 21].

Let $\mathcal{F}$ be a finite field. A Boolean function $f:\mathcal{F}^n\to\{0,1\}$ describes a $(n-d)$-dimensional affine subspace if $f^{-1}(1)\subseteq\mathcal{F}^n$ is a $(n-d)$-dimensional affine subspace. We denote the class of all such functions by d-**AS**. The class **AS**$=\cup_k k$-**AS** and $(\le d)$-**AS**$=\cup_{k\le d}k$-**AS**. A Boolean function $f:\mathcal{F}^n\to\{0,1\}$ describes an axis-parallel $(n-d)$-dimensional affine subspace if $f^{-1}(1)\subseteq\mathcal{F}^n$ is an axis parallel $(n-d)$-dimensional affine subspace, i.e., there are d entries $1\le i_1<i_2<\cdots<i_d\le n$ and constants $\lambda_i\in\mathcal{F}$, $i\in[d]$, such that $f^{-1}(1)=\{a\in\mathcal{F}^n|a_{i_1}=\lambda_1,\ldots,a_{i_d}=\lambda_d\}$. We denote the class of all such functions by d-**APAS**. In the same way, we define the class **APAS** and $(\le d)$-**APAS**. If in the above definitions, instead of "affine subspace" we have "linear subspace", then we get the classes d-**LS**, **LS**, $(\le d)$-**LS**, d-**APLS**, **APLS** and $(\le d)$-**APLS**. Those classes are studied in [13, 16, 19].

A related classes of Boolean functions $f:\{0,1\}^n\to\{0,1\}$ that are studied in the literature, [4, 6, 7, 8, 10, 13, 16, 19], are d-**Monomial** (conjunction of d negated Boolean variables)[2], **Monomial** (conjunction of negated Boolean variables), $(\le d)$-**Monomial** (conjunction of at most d negated

[1] See the definitions of the classes in the introduction and many other results in Tables 1 and 2.

[2] In the literature, this class is defined as conjunction of d (non-negated) variables. Testability of f for this class is equivalent to testability of $f(x+1^n)$ of d-**Monomial** as defined in this paper. The same applies to the classes $(\le d)$-**Monomial** and **Monomial**.

ISSN 1433-8092

Boolean variables), d-**Term** (conjunction of d literals[3]), **Term** (conjunction of literals), ($\le d$)-**Term** (conjunction of at most d literals). Those are equivalent to the two family of classes **APLS** (for **Monomial**) and **APAS** (for **Term**) over the binary field GF(2).

In property testing a class C of Boolean functions, a *tester* for C is a randomized algorithm T that has access to a Boolean function f via a black-box oracle that returns $f(x)$ when a point x is queried. Given a proximity parameter, ϵ, if $f \in C$, the tester T accepts with probability at least 2/3, and if f is ϵ-far from C (i.e., for every $g \in C$, $\mathbf{Pr}_x[f(x) \neq g(x)] > \epsilon$) then it rejects with probability at least 2/3. We say that T is a *one-sided* tester if it always accepts when $f \in C$; otherwise, it is called a *two-sided* tester.

Testers for the above classes were studied in [4, 6, 8, 10, 13, 16, 19]. In [19], Parnas et al. gave two-sided testers for the above classes that make $O(1/\epsilon)$ queries. See also [4, 13]. The one-sided testers were studied by Goldreich and Ron in [16]. They gave a polynomial-time one-sided testers for the classes **AS**, **APAS**, **LS**, ($\le d$)-**LS**, **APLS** and ($\le d$)-**APLS** that make $\tilde{O}(|\mathcal{F}|/\epsilon)$ queries[4]. In this paper, we give a polynomial-time[5] testers for these classes that make $\tilde{O}(1/\epsilon)$ queries.

For the classes d-**AS** and d-**APAS**, Goldreich and Ron gave the lower bound $\Omega(1/\epsilon + \log n/\log\log n)$ for the query complexity of any tester when $\mathcal{F} = \mathrm{GF}(2)$ and $\epsilon \le 2^{-d}$. In this paper, we give the lower bounds $\Omega(1/\epsilon + |\mathcal{F}|^{d-1}n)$ and $\Omega(1/\epsilon + |\mathcal{F}|^{d-1}\log n)$, respectively, for the proximity parameter $\epsilon < 1/|\mathcal{F}|^d$. We also give testers for those classes with query complexity that almost match the lower bounds.

See other results in Table 1 and 2 and the tester with self-corrector in the Appendix.

2 Overview of the Testers and the Lower Bounds

2.1 The Algorithm for Functions that describe Affine and Linear Subspace

In this section, we give the one-sided testers for **AS**, **LS** and ($\le d$)-**LS**.

Our tester that tests whether a function describes an affine subspace, **AS**, is built on the reduction of Goldreich and Ron's [16] and four stages. For completeness, we first present Goldreich and Ron's reduction. They show that testing whether a function $f(x)$ describes an affine subspace (resp. axis-parallel affine subspace) can be randomly reduced to testing whether $h(x) = f(x+a)$ describes a linear subspace (resp. axis-parallel linear subspace) where $a \in f^{-1}(1)$. This follows from the fact that if $f^{-1}(1) = u + L$ for some linear subspace $L \subseteq \mathcal{F}^n$, then for any $a \in f^{-1}(1)$, $f^{-1}(1) = a + L$ and, therefore, $h^{-1}(1) = L$.

Thus, in the reduction, the tester accepts if f is evaluated to 0 on uniformly at random $O(1/\epsilon)$ points[6]. Otherwise, let a be a point such that $f(a) = 1$. Then they run the tester for functions that describe linear subspaces to test $f(x+a)$. See more details in [16] Section 4.

The above reduction reduces the problem of testing **AS** to testing **LS**. Now, for testing **LS** we have four stages. In the following three stages, we show how to test whether the function describes a *well-structured* $(n-d)$*-dimensional subspace*. A function describes a well-structured $(n-d)$-dimensional subspace if $f^{-1}(1) = \{(a, \phi(a)) | a \in \mathcal{F}^{n-d}\}$, where $\phi : \mathcal{F}^{n-d} \to \mathcal{F}^d$ is a linear function.

[3] A literal is a variable or its negation.

[4] They also gave a tester for ($\le d$)-**AS**$\cup\{z(x)\}$ and ($\le d$)-**APAS**$\cup\{z(x)\}$ with the same query complexity where $z(x)$ is the zero function.

[5] Goldreich and Ron algorithm and our algorithm run in time linear in the number of queries

[6] If f is ϵ-far from **AS**, then it is ϵ-far from the function $h(x)$ that satisfies $h^{-1}(1) = \{0^n\}$. Therefore, whp, some point a satisfies $f(a) = 1$. This is not true for ($\le d$)-**AS** because $h \notin$ ($\le d$)-**AS**.

Class/Theo.	Lower Bound	Upper Bound	ϵ
AS	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$< \frac{1}{2}$
1,27	0	0	$> \frac{1}{2}$
($\le d$)-**AS**	$\Omega(1/\epsilon + \lvert\mathcal{F}\rvert^{d-1}n)$	$\tilde{O}(1/\epsilon) + \tilde{O}(\lvert\mathcal{F}\rvert^{d})n$ †	$< \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon) + O(1/(\epsilon - 1/\lvert\mathcal{F}\rvert^{d}))$	$> \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
6,13,24,27	0	0	$> \frac{1}{2}$
d-**AS**	$\Omega(1/\epsilon + \lvert\mathcal{F}\rvert^{d-1}n)$	$\tilde{O}(1/\epsilon) + \tilde{O}(\lvert\mathcal{F}\rvert^{d})n$ †	$< \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1/\epsilon + n)$	$\tilde{O}(1/\epsilon) + \tilde{O}(\lvert\mathcal{F}\rvert^{d})n$ †	$< 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1)$	$O(1/(\epsilon - 1 + \lvert\mathcal{F}\rvert^{-d}))$	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
6,7,13,22,27	0	0	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}} +^{\ddagger}$
APAS	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$> \frac{1}{2}$
3,27	0	0	$> \frac{1}{2}$
($\le d$)-**APAS**	$\Omega(1/\epsilon + \lvert\mathcal{F}\rvert^{d-1}\log n)$	$\tilde{O}(1/\epsilon) + \lvert\mathcal{F}\rvert^{d+o(d)}\log n$	$< \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon) + O(1/(\epsilon - 1/\lvert\mathcal{F}\rvert^{d}))$	$> \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
8,18,24,27	0	0	$> \frac{1}{2}$
d-**APAS**	$\Omega(1/\epsilon + \lvert\mathcal{F}\rvert^{d-1}\log n)$	$O(1/\epsilon) + \lvert\mathcal{F}\rvert^{d+o(d)}\log n$	$< \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega\left(\frac{1}{\epsilon} + \min\left(\frac{\log(1/\epsilon)}{\log\lvert\mathcal{F}\rvert}, d\right)\cdot\log\frac{n}{d}\right)$	$O(1/\epsilon) + \lvert\mathcal{F}\rvert^{d+o(d)}\log n$	$< 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1)$	$O(1/(\epsilon - 1 + \lvert\mathcal{F}\rvert^{-d}))$	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
8,10,18,22,27	0	0	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}} +$
LS	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$< \frac{1}{2}$
1,27	0	0	$> \frac{1}{2}$
($\le d$)-**LS**	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$< \frac{1}{2}$
2,27	0	0	$> \frac{1}{2}$
d-**LS**	$\Omega(1/\epsilon + n)$	$\tilde{O}(1/\epsilon) + O(\lvert\mathcal{F}\rvert^{d}n)$	$< 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1)$	$O(1/(\epsilon - 1 + \lvert\mathcal{F}\rvert^{-d}))$	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
7, 12,20,27	0	0	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}} +$
APLS	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$> \frac{1}{2}$
3,27	0	0	$> \frac{1}{2}$
($\le d$)-**APLS**	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$> \frac{1}{2}$
4,27	0	0	$> \frac{1}{2}$
d-**APLS**	$\Omega\left(\frac{1}{\epsilon} + \min\left(\frac{\log(1/\epsilon)}{\log\lvert\mathcal{F}\rvert}, d\right)\cdot\log\frac{n}{d}\right)$	$O\left(\frac{1}{\epsilon} + \min\left(\frac{\log(1/\epsilon)}{\log\lvert\mathcal{F}\rvert}, d\right)\cdot\log\frac{n}{d}\right)$	$< \frac{1}{\lvert\mathcal{F}\rvert} - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1)$	$O(1/(\epsilon - \lvert\mathcal{F}\rvert^{-1} + \lvert\mathcal{F}\rvert^{-d}) + \log n)$	$> \frac{1}{\lvert\mathcal{F}\rvert} - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
	$\Omega(1)$	$O(1/(\epsilon - 1 + \lvert\mathcal{F}\rvert^{-d}))$	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}}$
10,14,16,20,27	0	0	$> 1 - \frac{1}{\lvert\mathcal{F}\rvert^{d}} +$

Figure 1: A table of the lower bounds and upper bounds achieved in this paper. Any upper bound (resp. lower bound) for the proximity parameter ϵ is also an upper bound for $\epsilon' \ge \epsilon$ (resp. $\epsilon' \le \epsilon$). † Those testers are exponential time testers. ‡ $\lvert\mathcal{F}\rvert^{-d}+$ means $\lvert\mathcal{F}\rvert^{-d} + o(\lvert\mathcal{F}\rvert^{-d})$. See Th. 26 and Lem. 19

Class/Corollary	Lower Bound	Upper Bound	ϵ
Term	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$< \frac{1}{2}$
5,28	0	0	$> \frac{1}{2}$
$(\le d)$-**Term**	$\Omega(1/\epsilon + 2^d \log n)$	$\tilde{O}(1/\epsilon) + 2^{d+o(d)} \log n$	$< \frac{1}{2^d}$
	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon) + O(1/(\epsilon - 1/2^d))$	$> \frac{1}{2^d}$
9,19,25,28	0	0	$> \frac{1}{2}$
d-**Term**	$\Omega(1/\epsilon + 2^d \log n)$	$O(1/\epsilon) + 2^{d+o(d)} \log n$	$< \frac{1}{2^d}$
	$\Omega\left(\frac{1}{\epsilon} + \min\left(\log(1/\epsilon), d\right) \cdot \log \frac{n}{d}\right)$	$O(1/\epsilon) + 2^{d+o(d)} \log n$	$< 1 - \frac{1}{2^d}$
	$\Omega(1)$	$O(1/(\epsilon - 1 + 2^{-d}))$	$> 1 - \frac{1}{2^d}$
9,11,19,23,28	0	0	$> 1 - \frac{1}{2^d} +^{\ddagger}$
Monomial	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$< \frac{1}{2}$
5,28	0	0	$> \frac{1}{2}$
$(\le d)$-**Monom.**	$\Omega(1/\epsilon)$	$\tilde{O}(1/\epsilon)$	$< \frac{1}{2}$
	$\Omega(1/\epsilon)$	$O(1/\epsilon) + \tilde{O}(2^{2d})$	$< \frac{1}{2}$
5,28,29	0	0	$> \frac{1}{2}$
d-**Monomial**	$\Omega\left(\frac{1}{\epsilon} + \min\left(\log(1/\epsilon), d\right) \cdot \log \frac{n}{d}\right)$	$O\left(\frac{1}{\epsilon} + \min\left(\log(1/\epsilon), d\right) \cdot \log \frac{n}{d}\right)$	$< \frac{1}{2} - \frac{1}{2^d}$
	$\Omega(1)$	$O(1/(\epsilon - 1/2 + 2^{-d}) + \log n)$	$> \frac{1}{2} - \frac{1}{2^d}$
	$\Omega(1)$	$O(1/(\epsilon - 1 + 2^{-d}))$	$> 1 - \frac{1}{2^d}$
11,15,17,21,28	0	0	$> 1 - \frac{1}{2^d} +$

Figure 2: A table of the lower bounds and upper bounds achieved in this paper for **Term** and **Monomial**.
‡ $2^{-d}+$ means $2^{-d} + o(2^{-d})$. See Theorem 26 and Lemma 19

Then, in the fourth stage, we show how to test whether a function describes a linear subspace using the first three stages.

In the first stage, we give a tester that tests whether f is a function that *describes a well-structured* $(n-d)$*-dimensional injective relation*. That is, it satisfies: For every $a \in \mathcal{F}^{n-d}$, there is *at most one* $b \in \mathcal{F}^d$ such that $f(a,b) = 1$. The class of such functions is denoted by d-$\mathbf{R}$. We show that if f is ϵ-far from d-$\mathbf{R}$, then there are $\alpha, \beta < 1$ such that $\alpha\beta = O(\epsilon/\log(1/\epsilon))$ and $\mathbf{Pr}_{a \in \mathcal{F}^{n-d}}[\mathbf{Pr}_{b \in \mathcal{F}^d}[f(a,b) = 1] \ge \beta] \ge \alpha$. Then with a proper double search, the tester, with high probability, can find $a, b^{(1)} \ne b^{(2)}$ such that $f(a, b^{(1)}) \ne f(a, b^{(2)})$ and reject. If $f \in d$-$\mathbf{R}$, then no such $a, b^{(1)} \ne b^{(2)}$ can be found. Therefore, this is a one-sided tester. The query complexity of this stage is $\tilde{O}(\log^2(1/\epsilon)/\epsilon) = \tilde{O}(1/\epsilon)$.

In the second stage, we give a tester that tests whether f *describes a well-structured* $(n-d)$*-dimensional bijection*. That is: For every $a \in \mathcal{F}^{n-d}$, there is *exactly one* $b \in \mathcal{F}^d$ such that $f(a,b) = 1$. The class of such functions is denoted by d-$\mathbf{F}$. The tester for d-$\mathbf{F}$ first runs the above tester for d-$\mathbf{R}$ with proximity parameter $\epsilon/2$ and rejects if it rejects. So, we may assume that f is $\epsilon/2$-close to d-$\mathbf{R}$. Define the function $R_f : \mathcal{F}^{n-d} \to \mathcal{F}^d \cup \{\perp\}$ where $R_f(a)$ is equal to the first $b \in \mathcal{F}^d$ (in some total order) that satisfies $f(a,b) = 1$ and $\perp$ if no such b exists. We show that if f is $\epsilon/2$-close to d-$\mathbf{R}$ and ϵ-far from d-$\mathbf{F}$ then[7] $\mathbf{Pr}[R_f(a) = \perp] \ge \epsilon|\mathcal{F}|^d/2$. See details in Section 3. Since computing $R_f(a)$

[7] if $|\mathcal{F}|^d\epsilon > 2$, the tester accepts. This is because any function in d-$\mathbf{R}$ is $|\mathcal{F}|^{n-d}/|\mathcal{F}|^n \le 1/|\mathcal{F}|^d \le \epsilon/2$ close to any function in d-$\mathbf{F}$. Therefore, if f is $\epsilon/2$-close to d-$\mathbf{R}$, and $|\mathcal{F}|^d\epsilon > 2$ then it is ϵ-close to d-$\mathbf{F}$.

takes $|\mathcal{F}|^d$ queries, the query complexity of testing whether $\mathbf{Pr}[R_f(a) =\perp] \geq \epsilon|\mathcal{F}|^d/2$ is $O(1/\epsilon)$. This is also a one-sided tester because when $f \in d$-$\mathbf{F}$, $\mathbf{Pr}[R_f(a) =\perp] = 0$. The query complexity of this stage is $\tilde{O}(1/\epsilon)$.

In the third stage, we give a tester that tests whether a function f describes a well-structured $(n-d)$-dimensional linear subspace. The class of such functions is denoted by d-**WSLS**. First, the tester runs the tester for d-$\mathbf{F}$ with proximity parameter $\epsilon/2$ and rejects if it rejects. Now define a function $F_f : \mathcal{F}^{n-d} \to \mathcal{F}^d$ where $F_f(a) = R_f(a)$ if $R_F(a) \neq \perp$ and $f(a, b) = 0^d$ otherwise. We show that if f is ϵ-far from d-**WSLS** and $\epsilon/2$-close to d-$\mathbf{F}$, then F_f is $(|\mathcal{F}|^d\epsilon/2)$-far from linear functions. See details in Section 3. The tester then uses the testers in [3, 22] to test if F_f is $(|\mathcal{F}|^d\epsilon/2)$-far from linear functions. Since computing $F_f(a)$ takes $|\mathcal{F}|^d$ queries and the testers in [3, 22] make $O(2/(\epsilon|\mathcal{F}|^d)$ queries, the query complexity of this test is $O(1/\epsilon)$. Since the testers in [3, 22] are one-sided, this tester is also one-sided. The query complexity of this tester is $\tilde{O}(1/\epsilon)$.

Now, in the fourth stage, we give a tester that tests whether f describes a linear subspace. Recall that the class of such functions is denoted by **LS**. The tester at the $(d+1)$-th iteration uses a non-singular $n \times n$ matrix M such that $f_d(x) := f(xM)$ satisfies

1. If f is ϵ-far from **LS** then f_d is ϵ-far from **LS**.
2. If $f \in$ **LS** then $f_d \in$ **LS**.
3. If $f \in$ **LS** then $f_d^{-1}(1) = \{(a, \phi(a))|a \in L\}$ for some linear subspace $L \subseteq \mathcal{F}^{n-d}$ and linear function $\phi : \mathcal{F}^{n-d} \to \mathcal{F}^d$.

Items 1 and 2 are true for any non-singular matrix M. At the $(d+1)$-th iteration, the tester runs the tester that tests whether $f_d \in d$-**WSLA** with proximity parameter $\epsilon/2$ and accepts if it accepts. We show that if $f_d \in$ **LS** and the tester rejects, then it is because some $a \in \mathcal{F}^{n-d}$ has no $b \in \mathcal{F}^d$, such that $f_d(a, b) = 1$. In that case, the tester does not reject and uses the point $(a, 0^d) \in \mathcal{F}^d$ to construct a new non-singular matrix M' such that $f_{d+1} = f(xM')$ satisfies the above items 1-3. Items 1 and 2 hold for f_{d+1} because M' is non-singular. For item 3, we will have, if $f \in$ **LS**, then $f_{d+1}^{-1}(1) = \{(a, \phi'(a))|a \in L'\}$ for some linear subspace $L' \subseteq \mathcal{F}^{n-d-1}$ and a linear function $\phi' : \mathcal{F}^{n-d-1} \to \mathcal{F}^{d+1}$. The tester then continues to the $(d+2)$-th iteration if $d < (2 + \log(1/\epsilon)/\log|\mathcal{F}|)$; otherwise, it accepts.

If $f \in$ **LS**, then at each iteration, the tester either accepts or moves to the next iteration. Also, when $d = (2 + \log(1/\epsilon)/\log|\mathcal{F}|)$, the tester accepts. So, this tester is one-sided.

On the other hand, if f is ϵ-far from **LS**, then it is ϵ-far from the function h that satisfies $h^{-1}(1) = \{0^n\}$ (which is in **LS**). Therefore,[8], $\mathbf{Pr}[f \neq 0] \geq \epsilon/2$. Now since for $d = 2 + \log(1/\epsilon)/\log|\mathcal{F}|$, every function g in d-$\mathbf{R}$ satisfies $\mathbf{Pr}[g(x) = 1] \leq |\mathcal{F}|^{-d} \leq \epsilon/4$, the tester of d-**WSLA**, with high probability, rejects when it calls the tester of d-$\mathbf{R}$.

Therefore, this tester is one-sided, and its query complexity is $\tilde{O}(1/\epsilon)$. This completes the description of the tester of the class **LS**.

The above tester also works for testing the class $(\leq k)$-**LS**. The only change is that the tester rejects if $d > k$.

2.2 The Algorithm for Functions that describe Axis-Parallel Affine Subspace

The class of functions that describe axis-parallel affine subspace and the class of functions that describe axis-parallel linear subspace are denoted by **APAS** and **APLS**, respectively. Then d-

[8] This is true since $\mathbf{Pr}[f \neq 0] \geq \mathbf{Pr}[f \neq h] - \mathbf{Pr}[h \neq 0] \geq \epsilon - 1/|\mathcal{F}|^n$. Now we may assume that $\epsilon \geq 2/|\mathcal{F}|^n$ because, otherwise, we can query f in all the points using $O(|\mathcal{F}|^n) = O(1/\epsilon)$ queries.

APAS, d-**APLS**, ($\leq d$)-**APAS**, and ($\leq d$)-**APLS** are defined similarly to those in the previous subsection. When the field is $\mathcal{F} = \mathrm{GF}(2)$, those classes are equivalent to **Term**, **Monomial**, d-**Term**, d-**Monomial**, ($\leq d$)-**Term**, and ($\leq d$)-**Monomial**, respectively.

We first give an overview of the testers for **APAS** and **APLS**. As in the previous section, the reduction of Goldreich and Ron reduces the problem of testing whether the function describes an axis-parallel affine subspace (**APAS**) to testing whether the function describes an axis-parallel linear subspace (**APLS**).

The tester for testing whether the function describes an axis-parallel linear subspace, first runs the tester for **LS** with proximity parameter $\epsilon/100$ and rejects if it rejects. Then it draws uniformly at random $x, y, z \in f^{-1}(1)$ and tests if $f(w^{x,y} + z) = 1$ where for every $i \in [n]$, $w_i^{x,y} = 0$ if $x_i = y_i = 0$ and $w_i^{x,y} \in \{0, 1\}$ drawn uniformly at random, otherwise. If $f(w^{x,y} + z) = 1$, then the tester accepts; otherwise, it rejects.

We show that if $f \in$ **APLS**, then with probability 1, $f(w^{x,y} + z) = 1$. This fact is obvious. We also show that if f is ϵ-far from **APLS** and $\epsilon/100$-close to **LS**, then with constant probability $f(w^{x,y} + z) \neq 1$. Obviously, this tester is one-sided and makes $\tilde{O}(1/\epsilon)$ queries.

We give some intuition for why the latter is true. Let f be ϵ-far from **APLS** and $\epsilon/100$-close to **LS**. If $f^{-1}(1)$ is very close to a linear subspace L, then, for a uniformly at random $x, y, z \in f^{-1}(1)$, with high probability, x, y, z are in L. Then, since $f^{-1}(1)$ is ϵ-far from **APLS**, L is also $\Omega(\epsilon)$-far from **APLS**. So assuming $x, y \in L$, with high probability, $w^{x,y}$ is not in L. This follows from the fact that, if $L \in$ **LS**$\backslash$**APLS**, then some entry in the points in L is a *non-zero* linear combination of the other entries; therefore this entry is, whp, uniformly at random in $w^{x,y}$. Thus, whp, $w^{x,y} \notin L$, but not necessarily (whp) not in $f^{-1}(1)$ because $w^{x,y}$ is not a uniformly random point. So we need to add some randomness to $w^{x,y}$, which is why we add a random z to $w^{x,y}$. Then, assuming $x, y, z \in L$, whp, $w^{x,y} + z$ is not L. Now since z is almost random uniform in L and $w^{x,y}$ is not in L, whp, $w^{x,y} + z$ is an almost random uniform point in some coset outside L. Then again, since $f^{-1}(1)$ is very close to L, we get, whp, $w^{x,y} + z \notin f^{-1}(1)$. This implies that, whp, $f(w^{x,y} + z) \neq 1$. See details in Section 6.

Now for testing the class ($\leq d$)-**APLS**, we prove that if f is ($\epsilon/100$)-close to **APLS** and ($\epsilon/100$)-close to ($\leq d$)-**LS**, then it is ϵ-close to ($\leq d$)-**APLS**. So we run the tester for **APLS** and ($\leq d$)-**LS**, with proximity parameter $\epsilon/100$, and accept if both accept.

2.3 Lower Bound for Testing Classes with Fixed/Bounded Dimension

For the class of Boolean functions that describe $(n-d)$-dimensional affine/linear subspaces (d-**AS** and d-**LS**) and Boolean functions that describe axis-parallel $(n-d)$-dimensional affine/linear subspaces (d-**APAS** and d-**APLS**), we give lower bounds that depend on n, the number of variables. See Tables 1 and 2 and the proofs in Section 7.

Here we will give the technique used to prove the lower bound for the class d-**APLS**. For this class, we give the lower bound

$$\Omega\left(\frac{1}{\epsilon} + \min\left(\frac{\log(1/\epsilon)}{\log|\mathcal{F}|}, d\right) \cdot \log\frac{n}{d}\right)$$

for the query complexity.

First, the lower bound $\Omega(1/\epsilon)$ follows from [5]. Then any tester for the above classes can distinguish between functions in the class d-**APLS** and d'-**APLS** for $d' = \min(\log(1/\epsilon)/\log|\mathcal{F}|, d) - 1$. This is because the distance between any function in d'-**APLS** and a function in d-**APLS** is at least ϵ. Since the tester is one-sided, using Yao's principle, we show that there is a deterministic algorithm that can distinguish between all the functions in d-**APLS** and a subclass $C \subseteq d'$-**APLS** of size $|C| \geq (2/3)|d'\text{-}\mathbf{APLS}|$. We then show that for any $f \in C$, this algorithm asks queries that eliminate all possible entries in the points of $f^{-1}(1)$ that are not identically zero, except for at most d entries. Therefore, with d more queries, we get an exact learning algorithm for C. Thus, the number of queries of the tester must be at least the information-theoretic lower bound for learning C minus d, which is $\log|C| - d$. This gives the lower bound.

3 Definitions and Preliminary Results

Let $\mathcal{F}$ be a finite field of $q = |\mathcal{F}|$ elements, and $B(\mathcal{F})$ be the set of all Boolean functions $f : \mathcal{F}^n \to \{0,1\}$. We say that $f \in B(\mathcal{F})$ *describes a well-structured* $(n-d)$*-dimensional injective relation* if for every $a \in \mathcal{F}^{n-d}$, there is at most one element $b \in \mathcal{F}^d$ such that[9] $f(a,b) = 1$. The class of such functions is denoted by d-$\mathbf{R}$. Here $\mathcal{F}^0 = \{()\}$, so every Boolean function describes a well-structured n-dimensional injective relation. That is 0-$\mathbf{R}$$= B(\mathcal{F})$.

For a class $C \subseteq B(\mathcal{F})$ and functions $f, g \in B(\mathcal{F})$ we define $\text{dist}(f,g) = \mathbf{Pr}[f(x) \neq g(x)]$ and $\text{dist}(f,C) = \min_{h \in C} \text{dist}(f,h)$. For any $f \in B(\mathcal{F})$ define the function $R_f : \mathcal{F}^{n-d} \to \mathcal{F}^d \cup \{\perp\}$, $\perp \notin \mathcal{F}^d$, where $R_f(a)$ is equal to the minimum $b \in \mathcal{F}^d$ (in some total order over $\mathcal{F}^d$) that satisfies $f(a,b) = 1$ and $R_f(a) = \perp$ if no such b exists. If $d = 0$, we have $R_f : \mathcal{F}^n \to \{(), \perp\}$, where $R_f(a) = ()$ if $f(a) = 1$ and $R_f(a) = \perp$ if $f(a) = 0$. For any $f \in B(\mathcal{F})$ define $f_{\mathbf{R}} \in B(\mathcal{F})$ as $f_{\mathbf{R}}(a,b) = 1$ if $b = R_f(a)$ and $f_{\mathbf{R}}(a,b) = 0$ otherwise. The proof of the following lemma is straightforward.

Lemma 1. *We have*

1. *$R_f(a)$ can be computed using q^d queries to f.*
2. *$f_{\mathbf{R}}(a,b)$ can be computed using q^d queries to f.*
3. *$f_{\mathbf{R}} \in d$-$\mathbf{R}$.*
4. *If $f \in d$-$\mathbf{R}$ then $f_{\mathbf{R}} = f$.*
5. *$\text{dist}(f, d\text{-}\mathbf{R}) = \text{dist}(f, f_{\mathbf{R}})$.*

We now show

Lemma 2. *Let $q = |\mathcal{F}|$ and $r = \max(0, d\log q - \log(2/\epsilon))$. If f is ϵ-far from d-$\mathbf{R}$ then there is ℓ_0, $r + 1 \leq \ell_0 \leq d \log q$ such that for*

$$\alpha = \frac{\epsilon q^d}{2^{\ell_0+1}\min(d\log q - 1, \log(1/\epsilon))} \quad , \quad \beta = \frac{2^{\ell_0-1}}{q^d}$$

we have $\mathbf{Pr}_{a\in\mathcal{F}^{n-d}}[\mathbf{Pr}_{b\in\mathcal{F}^d}[f(a,b) \neq f_{\mathbf{R}}(a,b)] \geq \beta] \geq \alpha$.

In particular,

$$\alpha\beta \geq \frac{\epsilon}{4\log(1/\epsilon)}.$$

[9] By $f(a,b)$, we mean the following: If $a = (a_1, \ldots, a_{n-d})$ and $b = (b_1, \ldots, b_d)$, then $f(a,b) = f(a_1, \ldots, a_{n-d}, b_1, \ldots, b_d)$.

Proof. For every $a \in \mathcal{F}^{n-d}$, let $m_a = |\{b \in \mathcal{F}^d | f(a,b) = 1\}|$. Let $N_a = 0$ if $m_a = 0$ and $N_a = m_a - 1$ if $m_a \geq 1$. Then $N_a = q^d \mathbf{Pr}_{b \in \mathcal{F}^d}[f(a,b) \neq f_{\mathbf{R}}(a,b)]$. Since, by Lemma 1, $\text{dist}(f, f_{\mathbf{R}}) = \text{dist}(f, d\text{-}\mathbf{R}) \geq \epsilon$,

$$\mathbf{E}_a[N_a] = \frac{\sum_a N_a}{q^{n-d}} \geq \frac{\epsilon q^n}{q^{n-d}} = \epsilon q^d.$$

Since $N_a < q^d$, we have

$$\begin{aligned} \epsilon q^d &\leq \mathbf{E}_a[N_a] \leq \sum_{i=1}^{d \log q} 2^i \mathbf{Pr}_a[2^{i-1} \leq N_a < 2^i] \\ &= \sum_{i=1}^{r} 2^i \mathbf{Pr}_a[2^{i-1} \leq N_a < 2^i] + \sum_{i=r+1}^{d \log q} 2^i \mathbf{Pr}_a[2^{i-1} \leq N_a < 2^i] \\ &\leq 2^r \min(r,1) + (d \log q - r - 1) \max_{r+1 \leq i \leq d \log q} 2^i \mathbf{Pr}_a[2^{i-1} \leq N_a < 2^i]. \end{aligned}$$

Therefore, there is $r + 1 \leq \ell_0 \leq d \log q$ such that

$$\mathbf{Pr}_a[2^{\ell_0 - 1} \leq N_a < 2^{\ell_0}] \geq \frac{\epsilon q^d - 2^r \min(r,1)}{2^{\ell_0}(d \log q - r - 1)} \geq \frac{(\epsilon/2) q^d}{2^{\ell_0}(\min(d \log q - 1, \log(1/\epsilon)))} = \alpha.$$

Therefore,

$$\mathbf{Pr}_{a \in \mathcal{F}^{n-d}}[\mathbf{Pr}_{b \in \mathcal{F}^d}[f(a,b) \neq f_{\mathbf{R}}(a,b)] \geq \beta] = \mathbf{Pr}\left[\frac{N_a}{q^d} \geq \beta\right] \geq \mathbf{Pr}[N_a \geq 2^{\ell_0 - 1}] \geq \alpha.$$

□

We say that $f \in B(\mathcal{F})$ *describes a well-structured* $(n-d)$*-dimensional bijection*, if for every $a \in \mathcal{F}^{n-d}$, there is exactly one $b \in \mathcal{F}^d$ such that $f(a,b) = 1$. This class is denoted by d-$\mathbf{F}$. In particular, $f \in 0$-$\mathbf{F}$ if it is the constant 1 function.

We define $F_f : \mathcal{F}^{n-d} \to \mathcal{F}^d$ where $F_f(a) = R_f(a)$ if $R_f(a) \neq \perp$ and $F_f(a) = 0^d$ otherwise. Define $f_{\mathbf{F}} \in B(\mathcal{F})$ as $f_{\mathbf{F}}(a,b) = 1$ if $b = F_f(a)$ and $f_{\mathbf{F}}(a,b) = 0$ otherwise. The following lemma is straightforward.

Lemma 3. *We have*

1. d-$\mathbf{F} \subset d$-$\mathbf{R}$.
2. $F_f(a)$ *can be computed using* q^d *queries to* f.
3. $f_{\mathbf{F}}(a,b)$ *can be computed using* q^d *queries to* f.
4. $f_{\mathbf{F}} \in d$-$\mathbf{F}$.
5. *If* $f \in d$-$\mathbf{F}$ *then* $f_{\mathbf{F}} = f$.
6. $\text{dist}(f, d\text{-}\mathbf{F}) = \text{dist}(f, f_{\mathbf{F}})$.
7. $\text{dist}(f_{\mathbf{R}}, f_{\mathbf{F}}) = q^{-d} \mathbf{Pr}_x[R_f(x) = \perp]$.

We now prove

Lemma 4. *If* f *is* $\epsilon/2$*-close to* d-$\mathbf{R}$ *and* ϵ*-far from* d-$\mathbf{F}$*, then* $\mathbf{Pr}[R_f(a) = \perp] \geq \epsilon q^d / 2$.

Proof. By item 5 in Lemma 1, we have $\text{dist}(f, f_{\mathbf{R}}) \le \epsilon/2$. By item 6 in Lemma 3, $\text{dist}(f, f_{\mathbf{F}}) \ge \epsilon$. Therefore, $\text{dist}(f_{\mathbf{R}}, f_{\mathbf{F}}) \ge \epsilon/2$. By item 7 in Lemma 3, $\mathbf{Pr}_x[R_f(x) = \perp] \ge \epsilon q^d/2$. □

We say that $L \subseteq \mathcal{F}^n$ is a *well-structured* $(n-d)$*-dimensional linear subspace* if there is a linear function $\phi : \mathcal{F}^{n-d} \to \mathcal{F}^d$ such that

$$L = \{(a, \phi(a)) \mid a \in \mathcal{F}^{n-d}\}.$$

We say that $f \in B(\mathcal{F})$ *describes a well-structured* $(n-d)$*-dimensional linear subspace* if $f^{-1}(1)$ is a well-structured $(n-d)$-dimensional linear subspace. We denote by d-**WSLS** the class of Boolean functions that describes a well-structured $(n-d)$-dimensional linear subspace. Consider the class **Linear** of linear functions $\Lambda : \mathcal{F}^{n-d} \to \mathcal{F}^d$. We show

Lemma 5. *We have*

1. d-**WSLS**$\subset d$-**F**.
2. *If* $f \in d$-**WSLS** *then* $R_f(x) = F_f(x) \in$**Linear**.
3. $\text{dist}(f_{\mathbf{F}}, d\text{-}\mathbf{WSLS}) = q^{-d} \cdot \text{dist}(F_f(x), \mathbf{Linear})$.

Proof. Items 1 and 2 are obvious. For an event X, denote by $[X]$ the indicator random variable of X. We now prove item 3.

We have

$$\begin{aligned}
\text{dist}(f_{\mathbf{F}}, d\text{-}\mathbf{WSLS}) &= \min_{g \in d\text{-}\mathbf{WSLS}} \text{dist}(f_{\mathbf{F}}, g) \\
&= \min_{g \in d\text{-}\mathbf{WSLS}} \frac{1}{q^n} \sum_{a \in \mathcal{F}^{n-d}} \sum_{b \in \mathcal{F}^d} [f_{\mathbf{F}}(a,b) \ne g(a,b)] \\
&= \min_{g \in d\text{-}\mathbf{WSLS}} \frac{1}{q^n} \sum_{a \in \mathcal{F}^{n-d}} [F_f(a) \ne F_g(a)] \\
&= \min_{\Lambda \in \mathbf{Linear}} \frac{1}{q^n} \sum_{a \in \mathcal{F}^{n-d}} [F_f(a) \ne \Lambda(a)] \\
&= q^{-d} \text{dist}(F_f(x), \mathbf{Linear}).
\end{aligned}$$

□

We now prove

Lemma 6. *If* f *is* ϵ*-far from* d-**WSLS** *and* $\epsilon/2$*-close to* d-**F**, *then* F_f *is* $(q^d\epsilon/2)$*-far from* **Linear**.

Proof. If f is $\epsilon/2$-close from d-**F**, then by item 6 in Lemma 3, $\text{dist}(f, f_{\mathbf{F}}) \le \epsilon/2$. Since $\text{dist}(f, d\text{-}\mathbf{WSLS}) \ge \epsilon$ we have $\text{dist}(f_{\mathbf{F}}, d\text{-}\mathbf{WSLS}) \ge \epsilon/2$. The by item 3 in Lemma 5, $\text{dist}(F_f, \mathbf{Linear}) \ge q^d\epsilon/2$. □

We say that $f \in B(\mathcal{F})$ *describes an* $(n-d)$*-dimensional affine/linear subspace* if $f^{-1}(1) \subseteq \mathcal{F}^n$ is $(n-d)$-dimensional affine/linear subspace. The classes of such functions are denoted by d-**AS** and d-**LS**, respectively. Denote $(\le d)$-**AS**$= \cup_{d \ge k \ge 0}(k$-**AS**$)$ and **AS**$= \cup_{k \ge 0}(k$-**AS**$)$. Similarly, we define $(\le d)$-**LS**$= \cup_{d \ge k \ge 0}(k$-**LS**$)$ and **LS**$= \cup_{k \ge 0}(k$-**LS**$)$.

We now prove.

Lemma 7. *For any function $f \in B(\mathcal{F})$ and any nonsinglar $n \times n$-matrix M we have*

1. *If $f \in \mathbf{LS}$ and $h(x) = f(xM)$, then $h \in \mathbf{LS}$ and $\dim(h^{-1}(1)) = \dim(f^{-1}(1))$*
2. $\mathrm{dist}(f(x), \mathbf{LS}) = \mathrm{dist}(f(xM), \mathbf{LS})$.

Proof. For the proof, we use the fact that the map $x \to xM$ is a bijection. We have $h^{-1}(1) = \{a|h(a) = 1\} = \{a|f(aM) = 1\} = \{aM|f(aM) = 1\}M^{-1} = f^{-1}(1)M^{-1}$. This implies item 1.

We now prove item 2. Let $g(x) \in \mathbf{LS}$. Then, for $h(x) = g(xM^{-1})$, we have $h^{-1}(1) = g^{-1}(1)M$. Therefore $g(xM^{-1}) \in \mathbf{LS}$. This also implies that if $g(xM^{-1}) \in \mathbf{LS}$, then $g(x) = g(xM^{-1}M) \in \mathbf{LS}$. Therefore $g(x) \in \mathbf{LS}$ iff $g(xM^{-1}) \in \mathbf{LS}$. Now we have

$$\begin{aligned} \mathrm{dist}(f(x), \mathbf{LS}) &= \min_{g(x)\in\mathbf{LS}} \mathrm{dist}(f(x), g(x)) = \min_{g(x)\in\mathbf{LS}} \mathrm{dist}(f(x), g(xM^{-1})) \\ &= \min_{g(x)\in\mathbf{LS}} \mathrm{dist}(f(xM), g(x)) = \mathrm{dist}(f(xM), \mathbf{LS}). \end{aligned}$$

□

We say that $f \in B(\mathcal{F})$ is $(n-d)$*-dimensional axis-parallel linear/affine subspace* if there are d entries $i_1 < i_2 < \cdots < i_d$ such that $f^{-1}(1) = \{a \in \mathcal{F}^n | a_{i_1} = a_{i_2} = \cdots = a_{i_d} = 0\}$ (resp. there are $\xi_i \in \mathcal{F}$, $i \in [d]$ such that $f^{-1}(1) = \{a \in \mathcal{F}^n | a_{i_1} = \xi_1, a_{i_2} = \xi_2, \cdots, a_{i_d} = \xi_d\}$). The class of such functions are denoted by d-**APLS** and d-**APAS**, respectively. Similarly, as above, we define $(\leq d)$-**APLS**$= \cup_{d\geq k\geq 0}(k$-**APLS**$)$, **APLS**$= \cup_{k\geq 0}(k$-**APLS**$)$, $(\leq d)$-**APAS**$= \cup_{d\geq k\geq 0}(k$-**APAS**$)$, and **APAS**$= \cup_{k\geq 0}(k$-**APAS**$)$. Obviously, d-**APLS**$\subset d$-**LS** and d-**APAS**$\subset d$-**AS**.

4 Three Testers

In this section, we give testers for d-**R**, d-**F** and d-**WSLS**.

Test-d-R(f, ϵ)
Input: Oracle that accesses a Boolean function $f : \mathcal{F}^n \to \{0, 1\}$.
Output: Either "Accept" or "Reject"

1. For $\ell = \max(1, d\log q - \log(1/\epsilon))$ to $d \log q$
2. Let $\alpha(\ell) = \frac{\epsilon q^d}{2^{\ell+1}\min(d\log q-1,\log(1/\epsilon))}$, $\beta(\ell) = \frac{2^{\ell-1}}{q^d}$
3. Draw uniformly at random $r = 10/\alpha(\ell)$ assignments $a^{(1)}, \ldots, a^{(r)} \in \mathcal{F}^{n-d}$
   Draw uniformly at random $s = 10/\beta(\ell)$ assignments $b^{(1)}, \ldots, b^{(s)} \in \mathcal{F}^d$
   If there is $a^{(i)}$ and two $b^{(j_1)} \neq b^{(j_2)}$ such that $f(a^{(i)}, b^{(j_1)}) = f(a^{(i)}, b^{(j_2)}) = 1$ then Reject
4. Accept.

Figure 3: A tester for d-**R**.

We first prove

Lemma 8. *There is a polynomial-time one-sided tester for d-**R** that makes*

$$O(\min(\log(1/\epsilon), d\log q)^2/\epsilon) = O(\log^2(1/\epsilon)/\epsilon) = \tilde{O}(1/\epsilon).$$

queries.

Proof. Consider the tester **Test-d-R** in Figure 3. When $d = 0$, 0-**R** $= B(\mathcal{F})$. Since the commands in the For loop in **Test-0-R** are not executed, the tester accepts all functions. Now suppose $d \geq 1$. If $f \in d$-**R** then, (see step 3) there are no a and $b^{(1)} \neq b^{(2)}$ such that $f(a, b^{(1)}) = f(a, b^{(2)}) = 1$. Therefore, the tester accepts with probability 1.

Now suppose f is ϵ-far from d-**R**. By Lemma 2, there is ℓ_0 where $\max(1, d\log q - \log(1/\epsilon)) \leq \ell_0 \leq d\log q$ such that $\mathbf{Pr}_a[\mathbf{Pr}_b[f(a,b) \neq f_{\mathbf{R}}(a,b)] \geq \beta(\ell_0)] \geq \alpha(\ell_0)$. For such ℓ_0 in the For loop, the probability that one of the assignments $a^{(i)}$ satisfies $\mathbf{Pr}_b[f(a^{(i)},b) \neq f_{\mathbf{R}}(a^{(i)},b)] \geq \beta(\ell_0)$ is at least $1 - (1-\alpha(\ell_0))^{10/\alpha(\ell_0)} \geq 99/100$. For such an $a^{(i)}$, the probability that there are two $b^{(j_1)} \neq b^{(j_2)}$ such that $f(a^{(i)}, b^{(j_1)}) = f(a^{(i)}, b^{(j_2)}) = 1$ is at least

$$1 - (1-\beta(\ell_0))^{10/\beta(\ell_0)} - \frac{10}{\beta(\ell_0)}\beta(\ell_0)(1-\beta(\ell_0))^{10/\beta(\ell_0)-1} \geq \frac{99}{100}.$$

Therefore, with probability at least $98/100 > 2/3$, the tester rejects.

Since for every ℓ, $\alpha(\ell)\beta(\ell) \geq \epsilon/(4\log(1/\epsilon))$, the query complexity is $\min(d\log q - 1, \log(1/\epsilon)) \cdot 100/(\alpha(\ell)\beta(\ell)) = \tilde{O}(1/\epsilon)$. □

Test-d-F(f, ϵ)
Input: Oracle that accesses a Boolean function $f : \mathcal{F}^n \to \{0,1\}$.
Output: Either "Accept" or "Reject" with v =empty or $v \in \mathcal{F}^{n-d}$ s.t. $R_f(v) = \perp$

1. If **Test-d-R**$(f, \epsilon/2)$ =Reject then Reject; Return v = empty.
2. For $i = 1$ to $\lfloor 10/(q^d\epsilon) \rfloor$
3. Draw uniformly at random $a \in \mathcal{F}^{n-d}$
4. If $R_f(a) = \perp$ then Reject: Return $v = a$
5. Accept

Figure 4: A Tester for d-**F**.

We now give a tester for d-**F**. See Figure 4. Notice that when the tester rejects, it also returns $v \in \{\textit{empty}\} \cup \mathcal{F}^d$. We will use this in the next section. So, we can ignore that for this section.

Lemma 9. *There is a polynomial-time one-sided tester for d-**F** that makes $\tilde{O}(1/\epsilon)$ queries.*

Proof. Consider the tester **Test-d-F**. By Lemma 8 and (1) in Lemma 1, the query complexity is $\tilde{O}(1/\epsilon) + (10/(q^d\epsilon))q^d = \tilde{O}(1/\epsilon)$.

If $f \in d$-**F** then by item 1 in Lemma 3, $f \in d$-**R** and therefore Test-d-R in step 1 accepts. For every a, $R_f(a) \neq \perp$, so the tester accepts in step 5.

Now suppose f is ϵ-far from d-**F**. If f is $\epsilon/2$-far from d-**R**, then with probability at least 2/3, the tester rejects in step 1. If f is $\epsilon/2$-close to d-**R** then by Lemma 4, $\mathbf{Pr}_a[R_f(a) = \perp] \geq \epsilon q^d/2$. Therefore, with probability at least $1 - (1-\epsilon q^d/2)^{10/(q^d\epsilon)} \geq 2/3$, the tester rejects in the "For" loop. □

We now prove

Test-d-WSLS(f,ϵ)
Input: Oracle that accesses a Boolean function $f:\mathcal{F}^n\to\{0,1\}$.
Output: Either "Accept" or "Reject" with v =empty or $v\in\mathcal{F}^{n-d}$ s.t. $R_f(v)=\perp$
Test-Linear(F,ϵ) tests whether $F:\mathcal{F}^{n-d}\to\mathcal{F}^d$ is linear or ϵ-far from linear

1. If **Test-d-F**$(f,\epsilon/2)$ =Reject then Reject; Return v (that **Test-d-F** returns).
2. If **Test-Linear**$(F_f,q^d\epsilon/2)$ =Reject then
   If for some query a that **Test-Linear** asks $R_f(a)=\perp$ then Reject; Return $v=a$
   Otherwise, Reject; Return v =empty.
3. Accept

Figure 5: A Tester for d-**WSLS**.

Lemma 10. *There is a polynomial-time one-sided tester for d-**WSLS** that makes $\tilde{O}(1/\epsilon)$ queries.*

Proof. Consider the tester **Test-d-WSLS** in Figure 5. If $f\in d$-**WSLS**, then, by (1) in Lemma 5, $f\in d$-**F** and therefore the algorithm does not reject in step 1. By (2) in Lemma 5, $F_f(x)\in$**Linear**, and therefore, the tester does not reject in step 2. Thus, the tester accepts with probability 1.

Suppose f is ϵ-far from d-**WSLS**. If f is $\epsilon/2$-far from d-**F**, then with probability at least 2/3, **Test-d-F**$(f,\epsilon/2)$ rejects in step 1. If f is $\epsilon/2$-close to d-**F**, then by Lemma 6, F_f is $q^d\epsilon/2$-far from **Linear.** Therefore, with probability at least 2/3, **Test-Linear**$(F_f,q^d\epsilon)$ rejects.

The query complexity of **Test-d-F** is $\tilde{O}(1/\epsilon)$, and the query complexity of **Test-Linear**$(F_f,q^d\epsilon/2)$ is $O(1/\epsilon)$. The latter follows from item 2 in Lemma 3 and the fact that the testers for linear functions in [3, 22] have query complexity $O(1/\epsilon)$. □

5 A Tester for AS

We recall the definitions of the classes. We say that $f\in B(\mathcal{F})$ *describes an $(n-d)$-dimensional affine/linear subspace* if $f^{-1}(1)\subseteq\mathcal{F}^n$ is $(n-d)$-dimensional affine/linear subspace. The class of such functions is denoted by d-**AS** and d-**LS**, respectively. Denote $(\le d)$-**AS**$=\cup_{d\ge k\ge 0}(k$-**AS**$)$ and **AS**$=\cup_{k\ge 0}(k$-**AS**$)$. Similarly, we define $(\le d)$-**LS**$=\cup_{d\ge k\ge 0}(k$-**LS**$)$ and **LS**$=\cup_{k\ge 0}(k$-**LS**$)$.

In this section, we prove.

Theorem 1. *There are polynomial-time one-sided testers for **AS** and **LS** that make $\tilde{O}(1/\epsilon)$ queries.*

Theorem 2. *There is a polynomial-time one-sided tester for $(\le d)$-**LS** that makes $\tilde{O}(1/\epsilon)$ queries.*

In this section, we give the proofs of the above theorems for **LS** and $(\le d)$-**LS**. The reduction of Goldreich and Ron in [16] section 4 gives the result for **AS**.

Consider the tester **Test-LS** in Figure 6. In this tester, I_n is the $n\times n$ identity matrix, and $e_j=(0,0,\cdots,0,1)\in\mathcal{F}^j$. We first prove the following.

Lemma 11. *Let $L\subseteq\mathcal{F}^m$ be a linear subspace such that $e_m\notin L$. Then there is a linear function $\phi:\mathcal{F}^{m-1}\to\mathcal{F}$ such that $L=\{(a,\phi(a))|a\in L'\}$ for some linear subspace $L'\subseteq\mathcal{F}^{m-1}$.*

Test-LS(f,ϵ)
Input: Oracle that accesses a Boolean function $f:\mathcal{F}^n \to \{0,1\}$.
Output: Either "Accept" or "Reject".

1. If $f(0^n)=0$ then Reject.
2. $k \leftarrow 0; N = I_n$;
3. While $k \le m := \log(1/\epsilon)/\log(q)+2$ do
4. $\quad v \leftarrow$ **Test-k-WSLS**$(f(xN),\epsilon,\delta = 1-1/(10m))$; If Accept, then Accept.
5. $\quad$ If Reject and v =empty then Reject.
6. $\quad$ If Reject and $v \neq$empty $(R_{f_k}(v) = \perp)$ then
7. $\quad\quad$ Find a non-singular $(n-k)\times(n-k)$ matrix M s.t. $v = e_{n-k}M$
   $\quad\quad N \leftarrow N \cdot diag(M, I_k)$.
   $\quad\quad k \leftarrow k+1$
8. Accept

Figure 6: A Tester for **LS**.

Proof. Suppose, for the contrary, that there are no linear function ϕ and linear subspace $L' \subseteq \mathcal{F}^{m-1}$ such that $L = \{(a,\phi(a))|a \in L'\}$. For $u = (u_1,\ldots,u_m) \in \mathcal{F}^m$, denote $u' = (u_1,\ldots,u_{m-1})$. Let $t = \dim L$ and $\{b_1,\ldots,b_t\} \subset \mathcal{F}^m$ be a basis for L. Consider the $t \times m$ matrix H that has b_i in its ith row. We have $rank(H) = t$. The last column in H is independent of the other columns. Otherwise, L can be expressed as $L = \{(a,\phi(a))|a \in L'\}$ for some linear subspace $L' \subseteq \mathcal{F}^{m-1}$ and linear function ϕ, and we get a contradiction. Therefore, if we remove the last column of H, we get a matrix H' of rank $t-1$. Since $b'_1,\ldots,b'_t$ are the rows of H', there are $\lambda_i \in \mathcal{F}$, not all zero, such that $\sum_i \lambda_i b'_i = 0^{m-1}$. Since $b = \sum_i \lambda_i b_i \neq 0^m$, $b \in L$, and $b' = \sum_i \lambda_i b'_i = 0^{m-1}$, we must have that $b = \lambda e_m$ for some $\lambda \neq 0$. Therefore $\lambda^{-1} b = e_m \in L$. A contradiction. □

We are now ready to prove Theorem 1.

Proof. Consider the tester **Test-LS** in Figure 6. Notice that we added the confidence parameter $\delta = 1-1/(10m)$ to the tester **Test-k-WSLS** in step 4. We can achieve this confidence by running **Test-k-WSLS** with confidence $2/3$, $O(\log m) = O(\log\log(1/\epsilon))$ times.
Completeness: Suppose $f \in$**LS**. Since $f^{-1}(1)$ is a linear subspace, we have $0^n \in f^{-1}(1)$ and $f(0^n) = 1$. Therefore, the tester does not reject in step 1. If $f^{-1}(1) = \mathcal{F}^n$, then $f \in 0$-**WSLA** and **Test-0-WSLA**$(f(x),\epsilon,\delta)$ in step 4 accepts, and therefore **Test-LS** accepts. So, we may assume that $\dim(f^{-1}(1)) < n$.

Consider the "While" loop in the tester and denote by N_k the value of the matrix N in the $(k+1)$th iteration. Let $f_k(x) = f(xN_k)$. We now prove by induction the following claim, which implies the completeness of the tester.

Claim 1. *We have.*

1. *As long as $n-k > \dim(f^{-1}(1))$ and the tester does not accept, we have N_k is a non-singular matrix, $\dim(f_k^{-1}(1)) = \dim(f^{-1}(1))$, $\text{dist}(f_k,\mathbf{LS}) = \text{dist}(f,\mathbf{LS})$, and*

$$f_k^{-1}(1) = \{(u,\phi_k(u)) \mid u \in L_k\}$$

for some linear subspace $L_k \subseteq \mathcal{F}^{n-k}$ and a linear function $\phi_k : L_k \to \mathcal{F}^k$.

2. *If $n-k = \dim(f^{-1}(1))$, then $L_k = \mathcal{F}^{n-k}$, and the tester accepts.*
3. *If $n-k = n - \log(1/\epsilon)/\log q - 3$, the tester accepts.*

Proof. We prove 1. Obviously, the claim is true for $k=0$. We assume it is true for k and prove it for $k+1$.

Since, by item 1 in Lemma 7, $n-k > \dim(f^{-1}(1)) = \dim(f_k^{-1}(1))$, we have $L_k \neq \mathcal{F}^{n-k}$ and therefore $\dim(L_k) < n-k$.

We now show that either **Test-k-WSLA**$(f_k(x), \epsilon, \delta)$ accepts or returns $v \neq$empty, $v \neq 0^{n-k}$, and therefore $R_{f_k}(v) = \perp$.

In step 4, **Test-k-WSLA** first calls **Test-k-F**, which calls **Test-k-R** on f_k. See Figures 5, 4, and 3. Since[10] $f_k \in k$-**R**, **Test-k-R** does not reject. Therefore, if **Test-k-F** rejects, it is because some v satisfies $R_{f_k}(v) = \perp$. Then **Test-k-WSLA** tests the linearity of F_{f_k}. Since $R_{f_k}(a) = \phi_k(a)$ is linear for $a \in L_k$, the linearity test fails only if some $v \in \mathcal{F}^{n-k} \backslash L_k$ is queried in the linearity test, in which case $R_{f_k}(v) = \perp$. So, the tester either accepts or returns v, which satisfies $R_{f_k}(v) = \perp$. We now show that $v \neq 0^{n-k}$. Since $R_{f_k}(v) = \perp$, $f_k(v,u) = 0$ for every $u \in \mathcal{F}^k$. In particular, $f_k(v, 0^k) = 0$. Since $f_k(0^n) = f(0^n) = 1$, we have $v \neq 0^{n-k}$.

We now show that N_{k+1} is non-singular. Consider step 7 in the tester. Since $v \neq 0^{n-k}$, there is a non-singular matrix M that satisfies $v = e_{n-k}M$. Since, by the induction hypothesis, N_k is non-singular, we have $N_{k+1} = N_k \cdot diam(M, I_k)$ is a non-singular matrix. By Lemma 7, we have $\dim(f_{k+1}^{-1}(1)) = \dim(f^{-1}(1))$ and $\mathrm{dist}(f_{k+1}, \mathbf{LS}) = \mathrm{dist}(f, \mathbf{LS})$.

Now

$$f_{k+1}^{-1}(1) = f_k^{-1}(1) \cdot diag(M, I_k)^{-1} = \{(uM^{-1}, \phi_k(u)) | u \in L_k\} = \{(w, \phi_k(wM)) | w \in L_k M^{-1}\}.$$

Since[11] $v \notin L_k$, $e_{n-k} = vM^{-1} \notin L_k M^{-1}$ and by Lemma 11, $L_k M^{-1} = \{(z, \pi(z)) | z \in L'\}$ for some linear subspace $L' \subseteq \mathcal{F}^{n-(k+1)}$ and a linear function $\pi : \mathcal{F}^{n-(k+1)} \to \mathcal{F}$. Let $\phi'(z) = (\pi(z), \phi_k((z, \pi(z))M))$. Then $\phi' : \mathcal{F}^{n-(k+1)} \to \mathcal{F}^{k+1}$ is a linear function, and

$$f_{k+1}^{-1}(1) = \{(w, \phi_k(wM)) | w \in LM^{-1}\} = \{(z, \phi'(z)) | z \in L'\}.$$

This completes the proof of 1.

We now prove item 2. Since $\dim(f_k^{-1}(1)) = \dim(f^{-1}(1)) = n-k$ and $L_k \subseteq \mathcal{F}^{n-k}$, we have $L_k = \mathcal{F}^{n-k}$. Now when $L_k = \mathcal{F}^{n-k}$, $f_k \in k$-**WSLA** and therefore, the tester accepts.

Item 3 follows from steps 3 and 7 in the tester.

This completes the proof of the claim. □

Soundness: Let f be ϵ-far from **LS**. Then, by item 2 in Lemma 7, for any non-singular matrix N, $f(xN)$ is ϵ-far from **LS**. In particular, $f(xN)$ is ϵ-far from **Test-k-WSLS**. Therefore, with probability at least $1 - m/(10m) = 9/10$, it does not accept in the "While" loop. Now, we show that with probability at least $2/3$, it rejects in the "While" loop.

Since f is ϵ-far from **LS**, it is ϵ-far from the function h that satisfies $h^{-1}(1) = \{0^n\}$ (which is in **LS**). Therefore, $\mathbf{Pr}[f \neq 0] \geq \epsilon - 1/q^n \geq \epsilon/2$. Now since for $k = 2 + \log(1/\epsilon)/\log|\mathcal{F}|$, every function g in k-**R** satisfies $\mathbf{Pr}[g(x) = 1] \leq |\mathcal{F}|^{-k} \leq \epsilon/4$, the tester of k-**WSLA**, with probability at least $2/3$, rejects when it calls the tester of k-**R** when it reaches $k = 2 + \log(1/\epsilon)/\log|\mathcal{F}|$. Therefore, with probability at least $1 - 1/3 - 1/10 > 1/2$, the tester rejects. □

[10] This follows from the fact that if $a \in L_k$, then $f(a, \phi_k(a)) = 1$, otherwise no b satisfies $f(a,b) = 1$.

[11] If $v \in L_k$ then $(v, \phi_k(v)) \in f_k^{-1}(1)$ and $f_k(v, \phi_k(v)) = 1$ which implies $R_{f_k}(v) \neq \perp$. A contradiction.

For the proof of Theorem 2, we add to the tester in Figure 6, the command
"If $k = d + 1$ then Reject."
between steps 3 and 4. The proof is the same as above.

6 A Tester for APAS

We recall the definitions of the classes. We say that $f \in B(\mathcal{F})$ is $(n-d)$-*dimensional axis-parallel linear/affine subspace* if there are d entries $i_1 < i_2 < \cdots < i_d$ such that $f^{-1}(1) = \{a \in \mathcal{F}^n | a_{i_1} = a_{i_2} = \cdots = a_{i_d} = 0\}$ (resp. there are $\xi_i \in \mathcal{F}$, $i \in [d]$ such that $f^{-1}(1) = \{a \in \mathcal{F}^n | a_{i_1} = \xi_1, a_{i_2} = \xi_2, \cdots, a_{i_d} = \xi_d\}$). The class of such functions are denoted by d-**APLS** and d-**APAS**, respectively. Similarly, as in the previous section, we define $(\le d)$-**APLS**$= \cup_{d \ge k \ge 0}(k$-**APLS**$)$, **APLS**$= \cup_{k \ge 0}(k$-**APLS**$)$, $(\le d)$-**APAS**$= \cup_{d \ge k \ge 0}(k$-**APAS**$)$, and **APAS**$= \cup_{k \ge 0}(k$-**APAS**$)$. Obviously, d-**APLS**$\subset$ d-**LS** and d-**APAS**$\subset$ d-**AS**.

In this section, we prove.

Theorem 3. *There are polynomial-time one-sided testers for* **APAS** *and* **APLS** *that make* $\tilde{O}(1/\epsilon)$ *queries.*

Theorem 4. *There is a polynomial-time one-sided tester for* $(\le d)$-**APLS** *that makes* $\tilde{O}(1/\epsilon)$ *queries.*

Since **Term**=**APAS** and **Monomial**=**APLS** over $\mathcal{F} = \mathrm{GF}(2)$, we have.

Corollary 5. *There are polynomial-time one-sided testers for* **Term**, **Monomial**, *and* $(\le d)$-**Monomial** *that make* $\tilde{O}(1/\epsilon)$ *queries.*

Test-APLS(f, ϵ)
Input: Oracle that accesses a Boolean function $f : \mathcal{F}^n \to \{0, 1\}$.
Output: Either "Accept" or "Reject".

1. If **Test-LS**$(f, \epsilon/200)$ rejects then Reject.
2. For $i = 1$ to 30.
3. Draw $m = O(1/\epsilon)$ elements $U \subseteq \mathcal{F}^n$ uniformly at random
4. If there are three distinct $x, y, z \in U$ such that $f(x) = f(y) = f(z) = 1$ then
5. Define $w \in \mathcal{F}^n$ such that for every $i \in [n]$,
   $w_i = 0$ if $x_i = y_i = 0$ and $w_i \in \mathcal{F}$ random uniform otherwise.
6. If $f(w + z) = 0$ then Reject.
7. Accept.

Figure 7: A Tester for **APLS**.

In this section, we prove the theorems for **APLS** and $(\le d)$-**APLS**. The reduction of Goldreich and Ron in [16] section 4 gives the result for **APAS**.

When we write $\mathbf{Pr}_{x \in H}$, we mean x is drawn uniformly at random from H. By $\mathbf{Pr}_x$, we mean $\mathbf{Pr}_{x \in \mathcal{F}^n}$.

We first prove

Lemma 12. *Let L be a linear subspace that is not an axis-parallel linear subspace. Let $H \subseteq \mathcal{F}^n$ be any set that is $\epsilon/100$-close to L and $\mathbf{Pr}_x[x \in H] \geq \epsilon$. For any $x, y \in \mathcal{F}^n$, define the random variable $w^{x,y} \in \mathcal{F}^n$ where $w_i^{x,y} = 0$ if $x_i = y_i = 0$; otherwise $w_i^{x,y}$ is drawn uniformly at random from $\mathcal{F}$. Then*

$$\mathbf{Pr}_{x,y,z \in H, w^{x,y}}[w^{x,y} + z \in H] \leq 0.95.$$

Proof. In this proof, we omit the subscript $w^{x,y}$ from all the probabilities. Since $\mathbf{Pr}_x[x \in H] \geq \epsilon$ and $\mathbf{Pr}_x[x \in H \Delta L] \leq \epsilon/100$, we have $\mathbf{Pr}_x[x \in L] \geq 99\epsilon/100$. Since L is a linear subspace that is not an axis-parallel linear space, by permuting the coordinates, we may assume that wlog, $L = \{(u, \phi(u)) | u \in \mathcal{F}^{n-d}\}$, where $d \in [n]$ and $\phi : \mathcal{F}^{n-d} \to \mathcal{F}^d$ is a non-zero linear function. Then wlog, $\phi_1(u) := \phi(u)_1$ is a non-zero linear function. For $x = (u, \phi(u)) \in L$ and $y = (v, \phi(v)) \in L$ let X be the event that $\phi_1(u) \neq 0$ or $\phi_1(v) \neq 0$. If the event X occurs, then $w_{n-d+1}^{x,y}$ is uniformly random in $\mathcal{F}$. Let $w' = (w_1^{x,y}, \ldots, w_{n-d}^{x,y})$. Therefore

$$\begin{aligned}
\mathbf{Pr}_{x,y \in L}[w^{x,y} \notin L] &\geq \mathbf{Pr}_{x,y \in L}[w_{n-d+1}^{x,y} \neq \phi(w')] \\
&\geq \mathbf{Pr}_{x,y \in L}[w_{n-d+1}^{x,y} \neq \phi(w') | X] \cdot \mathbf{Pr}_{u,v \in \mathcal{F}^{n-d}}[X] \\
&= \left(1 - \frac{1}{q}\right)^3 \geq \frac{1}{8}.
\end{aligned}$$

Now, for the event[12] $A = [w^{x,y} + z \in H]$

$$\begin{aligned}
\mathbf{Pr}_{x,y,z \in H}[A] &\leq \mathbf{Pr}_{x,y,z \in H \cap L}[A] + \mathbf{Pr}_{x,y,z \in H}[(x \notin H \cap L) \vee (y \notin H \cap L) \vee (z \notin H \cap L)] \\
&\leq \mathbf{Pr}_{x,y,z \in H \cap L}[A] + \frac{3\mathbf{Pr}_x[x \in H \Delta L]}{\mathbf{Pr}_x[x \in H]} \\
&\leq \mathbf{Pr}_{x,y,z \in H \cap L}[A] + \frac{3(\epsilon/100)}{\epsilon}. \\
&\leq \mathbf{Pr}_{x,y,z \in L}[A] + \mathbf{Pr}_{x,y,z \in L}[(x \notin H \cap L) \vee (y \notin H \cap L) \vee (z \notin H \cap L)] + \frac{3}{100} \\
&\leq \mathbf{Pr}_{x,y,z \in L}[A] + \frac{3\mathbf{Pr}_x[x \in H \Delta L]}{\mathbf{Pr}_x[x \in L]} + \frac{3}{100} \\
&\leq \mathbf{Pr}_{x,y,z \in L}[A] + \frac{3 \cdot (\epsilon/100)}{99\epsilon/100} + \frac{3}{100} = \mathbf{Pr}_{x,y,z \in L}[A] + \frac{3}{99} + \frac{3}{100}
\end{aligned}$$

[12] We are using the facts that for any two events W and V, $\mathbf{Pr}[U] \leq \mathbf{Pr}[U|V] + \mathbf{Pr}[\neg V]$ and $\mathbf{Pr}[U|V] \leq \mathbf{Pr}[U] + \mathbf{Pr}[\neg V]$.

Now, since for every $w \notin L$, $L \cap (w + L) = \emptyset$,

$$\begin{aligned}
\mathbf{Pr}_{x,y,z\in L}[A] &= \mathbf{Pr}_{x,y,z\in L}[w^{x,y} + z \in H] \\
&\le \mathbf{Pr}_{x,y,z\in L}[w^{x,y} + z \in H | w^{x,y} \notin L] + \mathbf{Pr}_{x,y,z\in L}[w^{x,y} \in L] \\
&\le \mathbf{Pr}_{x,y,z\in L}[w^{x,y} + z \in H | w^{x,y} \notin L] + \frac{7}{8} \\
&\le \max_{w\notin L} \mathbf{Pr}_{z\in L}[w + z \in H] + \frac{7}{8} \\
&\le \max_{w\notin L} \frac{\mathbf{Pr}_z[z \in L, w + z \in H]}{\mathbf{Pr}_z[z \in L]} + \frac{7}{8} \\
&= \max_{w\notin L} \frac{\mathbf{Pr}_{z'}[z' \in (w + L) \cap H]}{\mathbf{Pr}_z[z \in L]} + \frac{7}{8} \\
&\le \frac{\mathbf{Pr}_{z'}[z' \in L\Delta H]}{\mathbf{Pr}_z[z \in L]} + \frac{7}{8} \\
&\le \frac{\epsilon/100}{99\epsilon/100} + \frac{7}{8} = \frac{1}{99} + \frac{7}{8}.
\end{aligned}$$

Therefore,

$$\mathbf{Pr}_{x,y,z\in H}[w^{x,y} + z \in H] \le \frac{4}{99} + \frac{3}{100} + \frac{7}{8} \le 0.95.$$

□

We are now ready to prove Theorem 3.

Proof. Consider the tester in Figure 7.
Soundness: If $f \in \mathbf{APLS}$, then it is in $\mathbf{LS}$. So, the tester does not reject in step 1. There is $d \in [n]$ and d entries $i_1 < i_2 < \cdots < i_d$ such that $f^{-1}(1) = \{a \in \mathcal{F}^n | a_{i_1} = a_{i_2} = \cdots = a_{i_d} = 0\}$. Therefore, for any $x, y, z \in f^{-1}(1)$, we have $w^{x,y} + z \in f^{-1}(1)$, and the tester does not reject in the "For" loop. So, it accepts.
Completeness: Suppose f is ϵ-far from $\mathbf{APLS}$. If f is $\epsilon/200$-far from $\mathbf{LS}$, then with probability at least $2/3$, the tester rejects in step 1. So, we may assume that f is $\epsilon/200$-close to $\mathbf{LS}$. Since f is ϵ-far from $\mathbf{APLS}$, it is ϵ-far from the function $h \in \mathbf{APLS}$ that satisfies $h^{-1}(1) = \{0^n\}$. Therefore, $\mathbf{Pr}[f = 1] \ge \epsilon - 1/q^n \ge \epsilon/2$. By Lemma 12, for $H = f^{-1}(1)$, we have

$$\mathbf{Pr}_{x,y,z,w^{x,y}}[f(w^{x,y} + z) = 1 | f(x) = f(y) = f(z) = 1] \le 0.95.$$

Since $\mathbf{Pr}[f = 1] \ge \epsilon/2$, there is a constant c such that for $m = c/\epsilon$, the algorithm, with probability at least $99/100$, at every iteration of the "For" loop, finds three points $x, y, z \in U$ such that $f(x) = f(y) = f(z) = 1$.[13] Therefore, the probability that the tester rejects is $1 - 0.95^{30} - 1/100 \ge 2/3$. □

Before proving Theorem 4, we give the following result.

[13] If $\mathbf{Pr}[f = 1] = \epsilon' \ge \epsilon/2$, then the probability that at every iteration of the "For" loop, the tester finds three points $x, y, z \in U$ such that $f(x) = f(y) = f(z) = 1$ is $\left(1 - (1-\epsilon')^{c/\epsilon} - \binom{c/\epsilon}{1}\epsilon'(1-\epsilon')^{c/\epsilon-1} - \binom{c/\epsilon}{2}\epsilon'^2(1-\epsilon')^{c/\epsilon-2}\right)^{30}$. This is greater than $99/100$ for a large enough constant c.

Lemma 13. *If f is $(\epsilon/100)$-close to* **APLS** *and $(\epsilon/100)$-close to $(\le d)$-***LS***, then it is ϵ-close to $(\le d)$-***APLS***.*

Proof. Suppose $f_1' \in d_1$-**LS**, $f_2' \in d_2$-**LS**, and $d_1 < d_2$. Then $\mathbf{Pr}[f_i'(x) = 1] = q^{-d_i}$ and therefore

$$3q^{-d_1}/2 \ge q^{-d_1} + q^{-d_2} \ge \mathrm{dist}(f_1', f_2') \ge q^{-d_1} - q^{-d_2} \ge q^{-d_1}/2. \tag{1}$$

Now assume, for the contrary, f is ϵ-far from $(\le d)$-**APLS**. Since f is $\epsilon/100$-close to **APLS**, there is $d' > d$ such that f is $\epsilon/100$-close to d'-**APLS**. Let $f_1 \in d'$-**APLS** be such that $\mathrm{dist}(f_1, f) \le \epsilon/100$. Choose any $f_2 \in d$-**APLS**. Since f is ϵ-far from f_2 we get that f_1 is $99\epsilon/100$-far from f_2. Therefore, by (1), $3q^{-d}/2 \ge \mathrm{dist}(f_1, f_2) \ge 99\epsilon/100$. This implies

$$q^{-d} \ge \frac{33}{50}\epsilon.$$

Since f is $(\epsilon/100)$-close to $(\le d)$-**LS**, there is $f_3 \in (\le d)$-**LS** such that $\mathrm{dist}(f, f_3) \le \epsilon/100$. Therefore, $\mathrm{dist}(f_1, f_3) \le \epsilon/50$. Now again, by (1), $\epsilon/50 \ge \mathrm{dist}(f_1, f_3) \ge q^{-d}/2$. This implies

$$q^{-d} \le \frac{1}{25}\epsilon < \frac{33}{50}\epsilon.$$

A contradiction. □

We are now ready to prove Theorem 4.

Proof. The tester simply runs the tester for **APLS** with proximity parameter $\epsilon/100$. Then it runs the tester for $(\le d)$-**LS** with proximity parameter $\epsilon/100$ and accepts if both testers accept.
Soundness. If $f \in (\le d)$-**APLS**, then $f \in$ **APLS** and $f \in (\le d)$-**LS**. Therefore, the tester accepts.
Completeness. If f is ϵ-far from $(\le d)$-**APLS**, then by Lemma 13, it is either $\epsilon/100$-far from **APLS** or $\epsilon/100$-far from $(\le d)$-**LS**. Therefore, with probability of at least 2/3 the tester rejects. □

7 Lower Bounds

In this section, we give all the other lower bounds in Table 1.

7.1 Preliminary Results

We first give some preliminary results.

Throughout this section, $z(x)$ will denote the zero function and $q = |\mathcal{F}|$. We will also assume that $d < cn$ for some constant $c < 1$.

Let $C \subset B(\mathcal{F})$ be a class of Boolean functions and $h \in B(\mathcal{F})$. We say that $U \subset \mathcal{F}^n$ is a *hitting set* for C *with respect to* h if, for every $f \in C$, there is $u \in U$ such that $f(u) \ne h(u)$. When $h = z$, the zero function, we say that $U \subset \mathcal{F}^n$ is a *hitting set* for C. The minimal size of a hitting set for C (resp. with respect to h) is denoted by $\mathcal{H}(C)$ (resp. $\mathcal{H}(C, h)$). Obviously, if $C' \subseteq C$, then $\mathcal{H}(C) \ge \mathcal{H}(C')$.

We now prove

Lemma 14. *Let $C \subseteq B(\mathcal{F})$ be a class of Boolean functions. Let $\epsilon_0 = \mathrm{dist}(C, h) := \min_{f\in C} \mathrm{dist}(f, h)$. Any one-sided tester for C with proximity parameter $\epsilon < \epsilon_0$ must make at least $\mathcal{H}(C, h)$ queries.*

Proof. Let T be a one-sided tester for C with proximity $\epsilon < \epsilon_0$. Since $\text{dist}(C,h)=\epsilon_0$, the tester T can distinguish between $h(x)$ and any function in C. The tester accepts with probability 1 when $f \in C$ and with probability at least 2/3 rejects when $f = h$; therefore, there is a deterministic algorithm[14] A with the same query complexity as T such that

1. If $f \in C$, then $A(f) = 1$.
2. $A(h) = 0$.

We now run the algorithm A and answer $h(a)$ for every query a. Let U be the set of queries. Then $|U|$ is at most the query complexity of A (and of T). We now show that U is a hitting set for C with respect to h. If U is not a hitting set for C with respect to h, then there is $g \in C$ such that $g(u) = h(u)$ for all $u \in U$. Then A cannot distinguish between h and g, and we get a contradiction. Therefore, U is a hitting set for C with respect to h. Thus, the query complexity of T is at least $|U| \geq \mathcal{H}(C,h)$. □

We now prove

Lemma 15. *Let $d' < d$. Then* $\text{dist}(d\text{-}\mathbf{AS}, d'\text{-}\mathbf{AS}) = \text{dist}(d\text{-}\mathbf{APLS}, d'\text{-}\mathbf{APLS}) = q^{-d'} - q^{-d}$.

Proof. Obviously, $\text{dist}(d\text{-}\mathbf{AS}, d'\text{-}\mathbf{AS}) \leq \text{dist}(d\text{-}\mathbf{APLS}, d'\text{-}\mathbf{APLS})$. For every $g \in d\text{-}\mathbf{AS}$, $\mathbf{Pr}[g=1] = q^{-d}$. Therefore, for $h \in d'\text{-}\mathbf{AS}$, we have $\mathbf{Pr}[g \neq h] \geq \mathbf{Pr}[h=1] - \mathbf{Pr}[g=1] = q^{-d'} - q^{-d}$. Therefore, $\text{dist}(d\text{-}\mathbf{AS}, d'\text{-}\mathbf{AS}) \geq q^{-d'} - q^{-d}$.

Now for g, h that satisfy $g^{-1}(1) = \{(a, 0^d) | a \in \mathcal{F}^{n-d}\}$ and $h^{-1}(1) = \{(b, 0^{d'}) | b \in \mathcal{F}^{n-d'}\}$, we have: $g \in d\text{-}\mathbf{APLS}$, $h \in d'\text{-}\mathbf{APLS}$ and $\text{dist}(g,h) = q^{-d'} - q^{-d}$. Therefore $\text{dist}(d\text{-}\mathbf{APLS}, d'\text{-}\mathbf{APLS}) \leq q^{-d'} - q^{-d}$, and the result follows. □

The following is an information-theoretic lower bound.

Lemma 16. *Any deterministic algorithm that exactly learns*[15] *a class C of Boolean functions $f : \mathcal{F}^n \to \{0,1\}$ must ask at least* $\log |C|$ *black-box queries.*

7.2 Lower Bound for $(\leq d)$-AS

Theorem 6. *Any one-sided testers for $(\leq d)$-$\mathbf{AS}$ and d-$\mathbf{AS}$ with proximity parameter $\epsilon < q^{-d}$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + q^{d-1}n\right)$$

queries.

Proof. The lower bound $\Omega(1/\epsilon)$ follows from [5]. For $\xi = (\xi_1, \ldots, \xi_{d-1}) \in \mathcal{F}^{d-1}$ and an affine subspace $L \subset \mathcal{F}^{n-d+1}$ of dimension $n-d$, let $f_{\xi,L}$ be the function that satisfies $f^{-1}(1) = \{\xi\} \times L$. Obviously, $f_{\xi,L} \in d\text{-}\mathbf{AS}$. Let $C \subseteq d\text{-}\mathbf{AS}$ be the class of such functions. We have $\text{dist}(d\text{-}\mathbf{AS}, z) = q^{-d}$. We now prove that $\mathcal{H}(C) \geq q^{d-1}(n-d+1)$. Since $\mathcal{H}(d\text{-}\mathbf{AS}) \geq \mathcal{H}(C)$, by Lemma 14, the result follows.

To this end, let H be a hitting set for C. Suppose, on the contrary, that $|H| < q^{d-1}(n-d+1)$. For $\xi \in \mathcal{F}^{d-1}$ let $H_\xi = \{a \in H | (a_1, \ldots, a_{d-1}) = \xi\}$. By the pigeonhole principle, there

[14] Just choose a seed that accepts h and use it for the algorithm T.

[15] For $f \in C$ and access to a black-box to f, the algorithm returns a function equivalent to f.

is $\xi' \in \mathcal{F}^{d-1}$, such that $|H_{\xi'}| \leq n-d$. Let $H_{\xi'} = \{b^{(1)}, \ldots, b^{(t)}\} \subseteq \mathcal{F}^n$, $t \leq n-d$. Consider $S = \{(b_d, \ldots, b_n) | b \in H_{\xi'}\} \subseteq \mathcal{F}^{n-d+1}$. If $\dim(Span(S)) < n-d$, we add to S elements from $\mathcal{F}^{n-d+1}$ to make $\dim(Span(S)) = n-d$. Let $L = Span(S) + v$ for some $v \in \mathcal{F}^{n-d+1} \backslash Span(S)$. Now consider the function $h := f_{\xi',L} \in C$. We will show that $h(u) = 0$ for all $u \in H$; therefore H is not a hitting set for C. A contradiction.

Let $u \in H$. Then either $(u_1, \ldots, u_{d-1}) \neq \xi'$ or $(u_1, \ldots, u_{d-1}) = \xi'$ and $(u_d, \ldots, u_n) \in Span(S)$. Since $Span(S) \cap L = \emptyset$ and $h^{-1}(1) = \{\xi'\} \cup L$, we have $u \notin \{\xi'\} \times L$ and therefore $h(u) = 0$. □

7.3 Lower Bound for d-AS and d-LS

In this subsection, we prove

Theorem 7. *Let $d > 0$. Any one-sided tester for d-**AS** and d-**LS** with proximity parameter $\epsilon < 1 - q^{-d}$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + n\right)$$

*queries, and for d-**AS** with proximity $\epsilon < q^{-d}$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + q^{d-1} n\right)$$

queries.

Proof. The second bound is from Theorem 6. We now prove the first bound for d-**AS**. The same proof holds for d-**LS**.

We use Lemma 14 with $h(x) = \alpha(x) = 1$, the constant function 1. We have $\epsilon_0 := \text{dist}(d\text{-}\mathbf{AS}, \alpha) = 1 - q^{-d}$. Let U be a hitting set for d-**AS** with respect to α. Suppose, on the contrary, $|U| \leq n-d$. If $\dim(Span(U)) < n-d$, then add elements to U such that $\dim(Span(U)) = n-d$. Let $L = Span(U)$ and let $h \in d$-**AS** be a function such that $h^{-1}(1) = L$. Then $h(u) = \alpha(u)$ for every $u \in U$, and therefore U is not a hitting set for d-**AS** with respect to α. A contradiction. Therefore $\mathcal{H}(d\text{-}\mathbf{AS}, \alpha) \geq |U| \geq n-d$. □

7.4 Lower Bound for $(\leq d)$-APAS

In this subsection, we prove.

Theorem 8. *Any one-sided tester for $(\leq d)$-**APAS** and d-**APAS** with proximity parameter $\epsilon < 1/q^d$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + q^{d-1} \log n\right)$$

queries.

In particular, we have.

Corollary 9. *Any one-sided tester for $(\leq d)$-**Term** and d-**Term** with proximity parameter $\epsilon < 1/2^d$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + 2^d \log n\right)$$

queries.

Proof. We give the proof for d-**APAS**. The same proof holds for $(\leq d)$-**APAS**. The lower bound $\Omega(1/\epsilon)$ follows from [5]. We use Lemma 14. First, we have $\text{dist}(d\text{-}\mathbf{APAS}, z) = q^{-d}$.

Let $U \subseteq \mathcal{F}^n$ be a hitting set for d-**APAS**. Since the function g that satisfies $g^{-1}(1) = \{x \in \mathcal{F}^n | x_{i_1} = \xi_1, \ldots, x_{i_d} = \xi_d\}$ is in d-**APAS**, there is $u \in U$ such that $u_{i_1} = \xi_1, \ldots, u_{i_d} = \xi_d$. Therefore, for every $1 \leq i_1 < i_2 < \cdots < i_d \leq n$ and $\xi_1, \xi_2, \ldots, \xi_d \in \mathcal{F}$, there is $u \in U$, such that $u_{i_1} = \xi_1, \ldots, u_{i_d} = \xi_d$. Such a set is called an (n, d)-*universal set over* $\mathcal{F}$[16]. It is well known, [9, 17, 23][17], that such a set has a size of at least $\Omega(q^{d-1} \log n)$. □

7.5 Lower Bounds for d-APLS

In this section, we prove.

Theorem 10. *Any one-sided tester for d-**APLS** and d-**APAS** with proximity parameter $\epsilon \leq q^{-1} - q^{-d}$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + \min\left(\frac{\log(1/\epsilon)}{\log|\mathcal{F}|}, d\right) \cdot \log\frac{n}{d}\right)$$

queries.

In particular,

Corollary 11. *Any one-sided tester for d-**Monomial** and d-**Term** with proximity parameter $\epsilon \leq 1/2 - 2^{-d}$ must make at least*

$$\Omega\left(\frac{1}{\epsilon} + \min\left(\log(1/\epsilon), d\right) \cdot \log\frac{n}{d}\right)$$

queries.

Proof. The lower bound $\Omega(1/\epsilon)$ follows from [5].

Let T be a tester for d-**APLS** (resp. d-**APAS**) with proximity parameter $\epsilon \leq 1 - q^{-d}$, which makes Q queries. Consider the class d'-**APLS** where $d' = \min(\lfloor \log(1/(\epsilon + q^{-d}))/\log q)\rfloor, d-1)$. Then, by Lemma 15, $\text{dist}(d\text{-}\mathbf{APLS}, d'\text{-}\mathbf{APLS}) = q^{-d'} - q^{-d} \geq \epsilon$ (resp. $\text{dist}(d\text{-}\mathbf{APAS}, d'\text{-}\mathbf{APLS}) \geq \epsilon$). Therefore

1. If $f \in d$-**APLS** then $T(f)$ =Accept.
2. If $f \in d'$-**APLS** then with probability at least $2/3$, $T(f)$ =Reject.

Using Yao's principle[18], there is a deterministic algorithm A that has query complexity Q (as T) and a class $C \subseteq d'$-**APLS** such that $|C| \geq (2/3)|d'\text{-}\mathbf{APLS}|$ and

1. If $f \in d$-**APLS** then $A(f)$ =Accept.
2. If $f \in C$ then $A(f)$ =Reject.

---

[16] Also called covering arrays.

[17] The lower bound follows from combining the lower bound in [9] for $d = 2$ with the lower bound in [17] or [23].

[18] For a random uniform $g \in d'$-**APLS**, we have $\mathbf{E}_s[\mathbf{E}_g[T(g)]] = \mathbf{E}_g[\mathbf{E}_s[T(g)]] \geq 2/3$ where s is the random seed of T. Then there is s_0 such that $\mathbf{E}_g[T(g)] \geq 2/3$.

We will show in the following how to change A to an exact learning algorithm for C that makes $Q+d$ queries, and then, by Lemma 16, the query complexity of T is at least[19]

$$\log|C|-d\geq \log\left(\frac{2}{3}|d'\text{-}\mathbf{APLS}|\right)-d=\log\left(\frac{2}{3}\binom{n}{d'}\right)-d=\Omega\left(\min\left(\frac{\log(1/\epsilon)}{\log|\mathcal{F}|},d\right)\cdot\log\frac{n}{d}\right).$$

It remains to show how to change A to an exact learning algorithm for C that makes $Q+d$ queries. To this end, consider the following algorithm (e_i is the point that contains 1 in the i-th coordinate and zero elsewhere)

1. Given access to a black-box for $f\in C$.
2. Let $X=[n]$.
3. Run A and for every query b that A asks such that $f(b)=1$, define $X\leftarrow X\backslash\{i|b_i=1\}$.
4. For every $i\in X$ if $f(e_i)=1$ then remove i from X.
5. Return the function h that satisfies $h^{-1}(1)=\{a\in\mathcal{F}^n|(\forall i\in X)a_i=0\}$.

Now, suppose $f^{-1}(1)=\{a\in\mathcal{F}^n|a_{i_1}=\cdots=a_{i_{d'}}=0\}$. We now show

Claim 2. *After step 3, we have $|X|\leq d$ and $\{i_1,\ldots,i_{d'}\}\subseteq X$.*

Proof. If, on the contrary, some $j\in[d']$, $i_j\notin X$, there is b such that $b_{i_j}=1$ and $f(b)=1$. Then $b\in f^{-1}(1)$ and therefore $b_{i_j}=0$. A contradiction.

Suppose, on the contrary, X contains more than d elements. Let $i_{d'+1},\ldots,i_d\in X$ be distinct and distinct from $i_1,\ldots,i_{d'}$. Consider the function g such that $g^{-1}(1)=\{a\in\mathcal{F}^b|a_{i_1}=\cdots=a_{i_d}=0\}$. Since A accepts $g\in d\text{-}\mathbf{APLS}$ and rejects $f\in C$, there must be a query b that A makes such that $g(b)\neq f(b)$. Since $g^{-1}(1)\subset f^{-1}(1)$, we have $b\in f^{-1}(1)\backslash h^{-1}(1)$, and then for some $j>d'$, we have $b_{i_j}=1$ and $f(b)=1$. Therefore, $i_j\notin X$ after step 3. A contradiction. This finishes the proof of the claim. □

By the above claim, step 5 makes at most d queries; therefore, the query complexity of the learning algorithm is $Q+d$. If, after step 3, $i\in\{i_1,\ldots,i_{d'}\}$, then $f(e_i)=0$, and then i is not removed from X after step 4. If after step 3, $i\notin\{i_1,\ldots,i_{d'}\}$ and $i\in X$, then the query e_i satisfies $f(e_i)=1$, and then i is removed from X after step 4. So, after step 4, we have $X=\{i_1,\ldots,i_{d'}\}$ and hence $h=f$. □

8 Upper Bounds

In this section, we prove the upper bounds in the table.

The following theorems cover all the upper bounds in the table.

We first prove.

Theorem 12. *There is a polynomial-time one-sided tester for d-**LS** with proximity parameter ϵ that makes*

$$\tilde{O}\left(\frac{1}{\epsilon}\right)+O(q^dn)$$

queries.

[19]Here, we assume that $d\ll n$. For large d, we can replace step 4 in the learning algorithm that makes at most d queries with the algorithm in [24] that makes $d'\log(d/d')-O(d')$ queries. This changes $\log|C|-d$ to $\log|C|-d'\log(d/d')-O(d')$, and we get the lower bound for any d.

Proof. Let $e_{n-k,i} \in \mathcal{F}^{n-k}$ be the point that has 1 in the i-th coordinate and zero elsewhere. Before we give the tester, notice that if we run the tester of $(\le d)$-**LS** (that makes $\tilde{O}(1/\epsilon)$ queries) on f, the only case where it fails to test d-**LS** is when $f \in k$-**LS** where $k < d$, and f is ϵ-far from d-**LS**. This happens when the tester of $(\le d)$-**LS** calls **Test-k-WSLS** (for $f(xM)$), and it accepts. So we need to change the tester **Test-k-WSLS** so that when $k < d$ and $f \in k$-**LS**, it rejects.

To solve this, the following modification is made. In **Test-k-WSLS** between step 2 and step 3 (before the tester accepts), we add the following step when $k < d$:

• If for some $i \in [n-k]$ we have $R_f(e_{n-k,i}) = \perp$, then Return $v = e_{n-k,i}$, Otherwise Reject. Given that $f^{-1}(1) = \{(a,b)|a \in L, \phi\}$ for some linear subspace $L \subseteq \mathcal{F}^{n-k}$ and linear function $\phi : \mathcal{F}^{n-k} \to \mathcal{F}^k$, this step tests whether $L = \mathcal{F}^{n-k}$. That is, the tester is the same as $(\le d)$-**LS** but does not accept when $f \in k$-**LS** and $k < d$. The following claim finishes the proof.

Claim 3. *$L = \mathcal{F}^{n-k}$ if and only for every i, $R_f(e_{n-k,i}) \neq \perp$.*

Proof. If $L = \mathcal{F}^{n-k}$, then $f(e_{n-k,i}, \phi(e_{n-k,i})) = 1$ and therefore $R_f(e_{n-k,i}) \neq \perp$ for every $i \in [n-k]$.

If for every i, $R_f(e_{n-d,i}) \neq \perp$, then for every i, there is $b^{(i)} \in \mathcal{F}^d$ such that $f(e_{n-d,i}, b^{(i)}) = 1$. Therefore for every i, $e_{n-d,i} \in L$, Since L is a linear space we get $L = \mathcal{F}^{n-d}$. □

This step has query complexity at most $q^d(n-d) = O(q^d n)$. □

Before we prove the following theorem, we give some preliminary results.

By [11], we have

$$|d\text{-}\mathbf{LS}| = \binom{n}{n-d}_q := \frac{(q^n-1)\cdots(q^{d+1}-1)}{(q^{n-d}-1)\cdots(q-1)} \le (2q)^{d(n-d)} \tag{2}$$

and therefore

$$|d\text{-}\mathbf{AS}| = q^d \binom{n}{n-d}_q \le q^d (2q)^{d(n-d)}. \tag{3}$$

By the probabilistic method, we show

Lemma 17. *There is a hitting set for d-**AS** (and d-**LS**) of size*

$$O(d(\log q)q^d n).$$

Proof. We choose uniformly at random $m = O(d(\log q)q^d n)$ points $a_1, \ldots, a_m \in \mathcal{F}^n$. The probability that there is $f \in d$-**AS** such that for all $i \in [m]$, $f(a_i) = 0$ is at most

$$|d\text{-}\mathbf{AS}| \left(1 - \frac{1}{|\mathcal{F}|^d}\right)^m < 1.$$

So a hitting set of size m exists. □

Theorem 13. *There is an exponential time one-sided tester for d-**AS** (and $(\le d)$-**AS**) with proximity parameter ϵ that makes*

$$\tilde{O}\left(\frac{1}{\epsilon}\right) + O(d(\log q)q^d n)$$

queries.

Proof. We use the hitting set to find a such that $f(a) = 1$ and then tests $f(x+a)$ using the tester of d-**LS** in Theorem 12. □

We now prove.

Theorem 14. *There is a polynomial-time one-sided tester for d-**APLS** with proximity parameter $\epsilon < 1/q$ that makes*

$$O\left(\frac{1}{\epsilon} + \min\left(\frac{\log(1/\epsilon)}{\log q}, d\right) \cdot \log \frac{n}{d}\right)$$

queries.

In particular,

Corollary 15. *There is a polynomial-time one-sided tester for d-**Monomial** with proximity parameter $\epsilon < 1/2$ that makes*

$$O\left(\frac{1}{\epsilon} + \min\left(\log(1/\epsilon), d\right) \cdot \log \frac{n}{d}\right)$$

queries.

Proof. If $d < 3\log(1/\epsilon)/\log|\mathcal{F}|$, the tester learns the function exactly with $O(d\log(n/d))$ queries using the algorithm in [24]. Then it tests if the output hypothesis is equal to the target on uniformly at random $O(1/\epsilon)$ points. If this occurs, then the tester accepts; otherwise, it rejects. The correctness of this case is obvious. See the reduction from learning to testing in [15].

If $d > d' := 3\log(1/\epsilon)/\log|\mathcal{F}|$, then the tester learns d' entries $1 \le i_1 < i_2 < \cdots < i_{d'} \le n$ such that $f^{-1}(1) \subseteq A := \{a \in \mathcal{F}^n | a_{i_1} = \cdots = a_{i_{d'}} = 0\}$ using $d'\log(n/d)$ queries [24]. Then for uniformly at random $O(1/\epsilon)$ points B, and for every point $b \in B$ it tests if "$f(b) = 1$ implies $b \in A$". If this occurs, then the tester accepts; otherwise, it rejects.

We now prove the correctness of the second case ($d > d'$). If $f \in d$-**APLS**, then the learning algorithm indeed learns d' entries $1 \le i_1 < i_2 < \cdots < i_{d'} \le n$ such that $f^{-1}(1) \subseteq A := \{a \in \mathcal{F}^n | a_{i_1} = \cdots = a_{i_{d'}} = 0\}$. Therefore, for every other point b, if $f(b) = 1$, then $b \in f^{-1}(1) \subseteq A$, which implies $b \in A$.

Now suppose f is ϵ-far from d-**APLS**. Since every $g \in d$-**APLS** satisfies $\mathbf{Pr}[g(x) \ne 0] \le q^{-d} \le \epsilon^3$, f is $(\epsilon - \epsilon^3)$-far from 0. Since $\mathbf{Pr}_b[b \in A] \le q^{-d'} \le \epsilon^3$, $f^{-1}(1)$ is $(\epsilon - 2\epsilon^3)$-far from A. Since $\epsilon - 2\epsilon^3 > \epsilon/4$, with constant probability, some $b \in B$ satisfies $f(b) = 1$ and $b \notin A$, and the tester rejects. □

We now prove.

Theorem 16. *There is a polynomial-time one-sided tester for d-**APLS** with proximity parameter $\epsilon > q^{-1} - q^{-d}$ that makes*

$$O\left(\frac{1}{\epsilon + q^{-d} - q^{-1}} + \log n\right)$$

queries.

In particular,

Corollary 17. *There is a polynomial-time one-sided tester for* d-**Monomial** *with proximity parameter* $\epsilon > 1/2 - 2^{-d}$ *that makes*

$$O\left(\frac{1}{\epsilon + 2^{-d} - 1/2} + \log n\right)$$

queries.

Proof. As in Theorem 14, the tester learns one entry $1 \le i_1 \le n$ such that $f^{-1}(1) \subseteq A := \{a \in \mathcal{F}^n | a_{i_1} = 0\}$ using $\log n$ queries [24]. Then for uniformly at random $O(1/(\epsilon + q^{-d} - q^{-1}))$ points B, and for every point $b \in B$ it tests if "$f(b) = 1$ implies $b \in A$". If this occurs, then the tester accepts; otherwise, it rejects.

If $f \in d$-**APLS**, then as in Theorem 14, the tester accepts.

Now suppose f is ϵ-far from d-**APLS**. Since, by Lemma 15, d-**APLS** is $(q^{-1} - q^{-d})$-far from 1-**APLS**, $f^{-1}(1)$ is $(\epsilon + q^{-d} - q^{-1})$-far from A. Therefore, with constant probability, some $b \in B$ satisfies $f(b) = 1$ and $b \notin A$, and the tester rejects. □

We now prove.

Theorem 18. *There is a polynomial-time one-sided tester for* d-**APAS** *(and* $(\le d)$-**APAS***) with proximity parameter* ϵ *that makes*

$$O\left(\frac{1}{\epsilon} + q^{d+o(d)} \log n\right)$$

queries.

In particular,

Corollary 19. *There is a polynomial-time one-sided tester for* d-**Term** *(and* $(\le d)$-**Term***) with proximity parameter* ϵ *that makes*

$$O\left(\frac{1}{\epsilon} + 2^{d+o(d)} \log n\right)$$

queries.

Proof. The tester builds an (n, d)-universal set U over $\mathcal{F}$ of size $O(q^{d+o(d)} \log n)$. This can be done in polynomial time [18] (in the number of queries). For every $a \in U$, it asks a black-box query until it finds a such that $f(a) = 1$. Such a exists. See the proof of Theorem 8. Then $f(x + a)$ is either in d-**APLS** or ϵ-far from d-**APLS**. So it runs the tester of d-**APLS** on $f(x + a)$. □

The rest of this section deals with the cases when ϵ is close to one.

Theorem 20. *There is a polynomial-time one-sided tester for* d-**LS** *(*d-**APLS***) with proximity parameter* $\epsilon > 1 - 1/q^d$ *that makes*

$$O\left(\frac{1}{\epsilon - 1 + 1/q^d}\right)$$

queries.

In particular,

Corollary 21. *There is a polynomial-time one-sided tester for d-***Monomial** *with proximity parameter $\epsilon > 1 - 1/2^d$ that makes*

$$O\left(\frac{1}{\epsilon - 1 + 1/2^d}\right)$$

queries.

Proof. If $d = 1$ and $q = 2$, the tester accepts. Otherwise, the tester chooses $O(1/(\epsilon - 1 + 1/q^d))$ uniformly at random points B. If f is identically one on B, the tester accepts. If for some point $a \in B$, $f(a) = 0$, then it chooses $b \in \mathcal{F}^n$ uniformly at random. If $f(b) = 1$ and $f(a + b) = 1$, then it rejects. Otherwise, it accepts.

Let $f \in d$-**LS** and $L = f^{-1}(1)$. If f is identically one on the points of B or $f(b) = 0$, then it accepts. If for some $a \in B$, $f(a) = 0$ and $f(b) = 1$, then $a \notin L$ and $b \in L$ and since L is a linear subspace, $a + b \notin L$. Therefore, $f(a + b) = 0$, and the tester accepts.

Now suppose f is ϵ-far from d-**LS**. Let α be the one function. Since α is $1 - q^{-d}$ far from d-**LS**, we get that f is $\epsilon - 1 + q^{-d}$ far from α. Therefore, with high probability, one of the points $a \in B$ satisfies $f(a) = 0$. Now

$$\begin{aligned}
\mathbf{Pr}[Rejects] &= \mathbf{Pr}_b[f(b) = 1, f(a + b) = 1] \\
&\geq 1 - \mathbf{Pr}_b[f(b) = 0] - \mathbf{Pr}_b[f(a + b) = 0] \\
&\geq 1 - 2\left(\epsilon - 1 + \frac{1}{q^d}\right) \geq 1 - \frac{2}{q^d}.
\end{aligned}$$

Therefore, for $d > 1$ or $q > 2$, with constant probability, the tester rejects.

The only case that remains is when[20] $d = 1$ and $q = 2$. For $\lambda \in \{0, 1\}^{n-1}$, consider the linear subspace $L_\lambda = \{(a, \phi_\lambda(a))\}$, where $\phi_\lambda(a) = \sum_{i=1}^{n-1} \lambda_i a_i$. Let $g_\lambda \in 1$-**LS** be the boolean function that satisfies $g_\lambda^{-1}(1) = L_\lambda$. It is easy to see that $g_\lambda(x) = \phi_\lambda(x_1, \ldots, x_{n-1}) + x_n + 1$. Let f be any boolean function. We have (Here, $[f(x) \neq g_\lambda(x)]$ is the indicator random variable of the event $f(x) \neq g_\lambda(x)$)

$$\mathbf{E}_\lambda[\mathbf{E}_x[f \neq g_\lambda]] = \mathbf{E}_x[\mathbf{E}_\lambda[f \neq g_\lambda]] \leq \frac{1}{2} + \frac{1}{2^{n-1}}.$$

Therefore, for every boolean function f, there is $g \in 1$-**LS** such that $\mathbf{Pr}_x[f \neq g] \leq 1/2 + 1/2^{n-1}$. Therefore, the tester, in this case, for $\epsilon > 1/2(+1/2^{n-1})$, accepts for any f. □

Theorem 22. *There is a polynomial-time one-sided tester for d-***AS** *(d-***APAS***) with proximity parameter $\epsilon > 1 - 1/q^d$ that makes*

$$O\left(\frac{1}{\epsilon - 1 + 1/q^d}\right)$$

queries.

In particular,

Corollary 23. *There is a polynomial-time one-sided tester for d-***Term** *with proximity parameter $\epsilon > 1 - 1/2^d$ that makes*

$$O\left(\frac{1}{\epsilon - 1 + 1/2^d}\right)$$

queries.

[20] Notice that for $d = 0$, 0-**LS**=(≤ 0)-**LS**. See the results for (≤ 0)-**LS** in the Table.

Proof. The tester chooses 10 points uniformly at random. If f is zero on all the points, then it accepts. Otherwise, let a be a point such that $f(a) = 1$. The tester then runs the tester of d-**LS** on $f(x + a)$.

If $f \in d$-**AS**, then the tester accepts.

If f is ϵ-far from d-**AS**, then f is $\epsilon - q^{-d} \geq 1 - 2q^{-d}$ far from z (the zero function). Therefore, with high probability, some point a satisfies $f(a) = 1$. Then $f(x + a)$ is ϵ-far from d-**LS**, and the result follows.

Again here, the tester for $q = 2$ and $d = 1$ accepts all functions. □

Theorem 24. *There is a polynomial-time one-sided tester for* $(\leq d)$-**AS** *(*$(\leq d)$-**APAS***) with proximity parameter* $\epsilon > 1/q^d$ *that makes*

$$\tilde{O}\left(\frac{1}{\epsilon}\right) + O\left(\frac{1}{\epsilon - 1/q^d}\right)$$

queries.

In particular,

Corollary 25. *There is a polynomial-time one-sided tester for* $(\leq d)$-**Term** *with proximity parameter* $\epsilon > 1/2^d$ *that makes*

$$\tilde{O}\left(\frac{1}{\epsilon}\right) + O\left(\frac{1}{\epsilon - 1/2^d}\right)$$

queries.

Proof. The tester chooses $O(1/(\epsilon - q^{-d}))$ uniformly at random points. If f is zero on all the points, then it accepts. Otherwise, let a be a point such that $f(a) = 1$. The tester then runs the tester of $(\leq d)$-**LS** on $f(x + a)$.

If $f \in (\leq d)$-**AS**, then it is obvious that the tester accepts.

If f is ϵ-far from $(\leq d)$-**AS**, then since $(\leq d)$-**AS** is q^{-d} far from z, we get that f is $(\epsilon - q^{-d})$-far from z. Therefore, with high probability, the tester finds a such that $f(a) = 1$. □

We now investigate the value of ϵ, where the tester does need to ask any queries.

We define the *isolation factor* of a class C as

$$\text{IF}(C) := \max_{f \in B(\mathcal{F})} \text{dist}(f, C).$$

Obviously.

Lemma 18. *If* $C_1 \subseteq C_2$*, then* $\text{IF}(C_1) \geq \text{IF}(C_2)$*.*

The following is obvious,

Theorem 26. *There is a one-sided tester for* C *with proximity parameter* $\epsilon > \text{IF}(C)$ *that makes no queries.*

Proof. Since any $f \in B(\mathcal{F})$ satisfies $\text{dist}(f, C) \leq \text{IF}(C) < \epsilon$, the tester does not ask any query and just accepts. □

We now prove

Lemma 19. *We have*

1. $\frac{1}{2} \geq \text{IF}(\mathbf{APLS}) \geq \text{IF}(\mathbf{LS}) \geq \frac{1}{2} - o_n(1)$.
2. $\frac{1}{2} \geq \text{IF}(\mathbf{APAS}) \geq \text{IF}(\mathbf{AS}) \geq \frac{1}{2} - o_n(1)$.
3. $\frac{1}{2} + \frac{1}{2q^d} \geq \text{IF}((\leq d)\text{-}\mathbf{APLS}) \geq \text{IF}((\leq d)\text{-}\mathbf{LS}) \geq \frac{1}{2} - o_n(1)$.
4. $\frac{1}{2} + o_n(1) \geq \text{IF}((\leq d)\text{-}\mathbf{APAS}) \geq \text{IF}((\leq d)\text{-}\mathbf{AS}) \geq \frac{1}{2} - o_n(1)$.
5. $1 - \frac{1}{q^d} + \Theta\left(\frac{1}{q^{3d/2}}\right) \geq \text{IF}(d\text{-}\mathbf{APLS}) \geq \text{IF}(d\text{-}\mathbf{LS}) \geq 1 - \frac{1}{q^d}$.
6. $1 - \frac{1}{q^d} + \Theta\left(\frac{1}{q^{2d}}\right) \geq \text{IF}(d\text{-}\mathbf{APAS}) \geq \text{IF}(d\text{-}\mathbf{AS}) \geq 1 - \frac{1}{q^d}$.

Proof. By Chernoff's bound, it is easy to show that for all the above classes C, for a random uniform function $f \in B(\mathcal{F})$, with probability greater than zero, we have $\text{dist}(f, C) \geq 1/2 - o_n(1)$. Therefore, $\text{IF}(C) \geq 1/2 - o_n(1)$. This gives the lower bounds in items 1-4.

Let C be one of the classes **APAS**, **APLS**, **LS**, or **AS**, and let $f \in B(\mathcal{F})$. Since $1 \in C$ (the one function) and the function h that satisfies $h^{-1}(1) = \{0^n\}$ is in C, we have

$$\begin{aligned} 1 = \mathbf{Pr}[f \neq 0] + \mathbf{Pr}[f \neq 1] &\geq \mathbf{Pr}[f \neq h] - \mathbf{Pr}[h \neq 0] + \mathbf{Pr}[f \neq 1] \\ &= \mathbf{Pr}[f \neq h] - \frac{1}{q^n} + \mathbf{Pr}[f \neq 1]. \end{aligned} \tag{4}$$

Therefore, $\min(\mathbf{Pr}[f \neq h], \mathbf{Pr}[f \neq 1]) \leq 1/2 + 1/(2q^n)$. Since the probability of each point is $1/q^n$, we get $\text{IF}(\mathbf{APLS}) \leq 1/2$. This gives the upper bounds in items 1-2. Applying (4) with any $h \in d\text{-}\mathbf{APLS}$, we get the upper bound in item 3.

We now prove the upper bound in item 4. For $\lambda \in \mathcal{F}^d$, let g_λ be such that $g_\lambda^{-1}(1) = L_\lambda := \{a \in \mathcal{F}^n | a_i = \lambda_i, i \in [d]\}$. Let C be the class that contains the 1 function (which is in 0-**APAS**) and all g_λ. Obviously, $C \subseteq (\leq d)\text{-}\mathbf{APAS}$. Therefore, by Lemma 18, an upper bound for $\text{IF}(C)$ gives an upper bound for $\text{IF}((\leq d)\text{-}\mathbf{APAS})$.

Consider a function that satisfies $\text{dist}(f, C) = \text{IF}(C)$. For $\lambda \in \mathcal{F}^d$, Let $M_\lambda = L_\lambda \cap f^{-1}(1)$. Suppose there are $\lambda^{(1)} \neq \lambda^{(2)}$ such that $m := |M_{\lambda^{(1)}}| - |M_{\lambda^{(2)}}| \geq 2$. We now define the following function f_0. Take any $\lceil m/2 \rceil$ elements B_1 from $M_{\lambda^{(1)}}$ and $\lceil m/2 \rceil$ elements B_2 from $L_{\lambda^{(2)}} \backslash M_{\lambda^{(2)}}$. Define f_0 to be equal to f on all L_λ where $\lambda \neq \lambda^{(1)}, \lambda^{(2)}$. Then f_0 is 1 on $M_{\lambda^{(1)}} \backslash B_1$ and $M_{\lambda^{(2)}} \cup B_2$ and is 0 on $(L_{\lambda^{(1)}} \backslash M_{\lambda^{(1)}}) \cup B_1$ and $L_{\lambda^{(2)}} \backslash (M_{\lambda^{(2)}} \cup B_2)$. It is easy to see that $\text{dist}(f_0, C) \geq \text{dist}(f, C) = \text{IF}(C)$ and, therefore, $\text{dist}(f_0, C) = \text{IF}(C)$. In addition, f_0 satisfies the property that for $M'_\lambda = L_\lambda \cap f_0^{-1}(1)$, we have $m' := ||M'_{\lambda^{(1)}}| - |M'_{\lambda^{(2)}}| \leq 1$. Therefore, we may assume that w.l.o.g, for any λ, $|M_\lambda| - |M_{0^d}| \in \{0, 1\}$. If $\text{IF}(C) > 1/2 + 4/q^{n-d}$, then[21]

$$\frac{1}{2} + \frac{4}{q^{n-d}} < \text{dist}(f, C) \leq \text{dist}(f, 1) = \sum_\lambda \mathbf{Pr}[L_\lambda \backslash M_\lambda] = \sum_\lambda \left(\frac{1}{q^d} - \mathbf{Pr}[M_\lambda]\right) \leq 1 - q^d \mathbf{Pr}[M_{0^d}].$$

Therefore, $\mathbf{Pr}[M_{0^d}] < 1/(2q^d) - 4/q^n$, and for every λ,

$$\mathbf{Pr}[M_\lambda] \leq \mathbf{Pr}[M_{0^d}] + \frac{1}{q^n} < \frac{1}{2q^d} - \frac{3}{q^n}.$$

[21] Here $\mathbf{Pr}[A] = \mathbf{Pr}_x[x \in A]$ where x is random uniform in $\mathcal{F}^n$.

Now

$$\begin{aligned}\frac{1}{2}+\frac{4}{q^{n-d}} &< \operatorname{dist}(f,C)\le \operatorname{dist}(f,g_{0^d}) = \frac{1}{q^d}-\mathbf{Pr}[M_{0^n}]+\sum_{\lambda\neq 0^d}\mathbf{Pr}[M_\lambda]\\ &= \frac{1}{q^d}+\mathbf{Pr}[M_{1^d}]-\mathbf{Pr}[M_{0^d}]+\sum_{\lambda\neq 0^d,1^d}\mathbf{Pr}[M_\lambda]\\ &\le \frac{1}{q^d}+\frac{1}{q^n}+\sum_{\lambda\neq 0^d,1^d}\mathbf{Pr}[M_\lambda] < \frac{1}{q^d}+\frac{1}{q^n}+\frac{q^d-2}{2q^d}-\frac{3(q^d-2)}{q^n}<\frac{1}{2}.\end{aligned}$$

A contradiction. Therefore $\mathrm{IF}(C)\le 1/2+o_n(1)$.

We now prove 5-6. For $C=d$-**LS**, d-**APLS**, d-**AS**, and d-**APAS**, By Lemma 15, $\operatorname{dist}(C,0\text{-}\mathbf{LS})=1-q^{-d}$. Therefore, $\mathrm{IF}(C)\ge 1-q^{-d}$.

For $C=d$-**LS** and d-**APLS**, let $f\in B(\mathcal{F})$. We have two cases: If $\mathbf{Pr}[f=1]\le 1-2q^{-d}$, then for any $g\in C$, $\mathbf{Pr}[f\neq g]\le \mathbf{Pr}[f=1]+\mathbf{Pr}[g=1]\le 1-q^{-d}$. The second case is when $\mathbf{Pr}[f=1]>1-2q^{-d}$. Consider the following functions $g_i\in d$-**APLS** that satisfies $g_i^{-1}(1)=\{a\in\mathcal{F}^n|a_{(i-1)d+1}=\cdots=a_{id}=0\}$, for $i\in[m]$ and $m=q^{d/2}$. By the inclusion–exclusion principle,

$$\mathbf{Pr}\left[\cup_{i=1}^m g_i^{-1}(1)\right]=\sum_{i=1}^m(-1)^{i+1}\frac{\binom{m}{i}}{q^{id}}=\frac{m}{q^d}-\Theta\left(\frac{m^2}{q^{2d}}\right).$$

Then

$$\mathbf{Pr}\left[f^{-1}(1)\cap\cup_{i=1}^m g_i^{-1}(1)\right]\ge \mathbf{Pr}[f^{-1}(1)]+\mathbf{Pr}[\cup_{i=1}^m g_i^{-1}(1)]-1=\frac{m-2}{q^d}-\Theta\left(\frac{m^2}{q^{2d}}\right).$$

Now since

$$\mathbf{Pr}\left[f^{-1}(1)\cap\cup_{i=1}^m g_i^{-1}(1)\right]=\mathbf{Pr}\left[\cup_{i=1}^m(f^{-1}(1)\cap g_i^{-1}(1))\right]\le\sum_{i=1}^m\mathbf{Pr}\left[(f^{-1}(1)\cap g_i^{-1}(1))\right],$$

there is $i_0\in[m]$ such that

$$\mathbf{Pr}\left[(f^{-1}(1)\cap g_{i_0}^{-1}(1))\right]\ge\frac{m-2}{mq^d}-\Theta\left(\frac{m}{q^{2d}}\right)=\frac{1}{q^d}-\Theta\left(\frac{1}{mq^d}+\frac{m}{q^{2d}}\right)=\frac{1}{q^d}-\Theta\left(\frac{1}{q^{3d/2}}\right).$$

Then

$$\mathbf{Pr}[f\neq g_{i_0}]\le 1-\mathbf{Pr}\left[(f^{-1}(1)\cap g_{i_0}^{-1}(1))\right]\le 1-\frac{1}{q^d}+\Theta\left(\frac{1}{q^{3d/2}}\right).$$

Therefore $\mathrm{IF}(d\text{-}\mathbf{APLS})\le 1-q^{-d}+\Theta(q^{-3d/2})$.

For $C=d$-**AS** and d-**APAS**, let $f\in B(\mathcal{F})$. For $\lambda\in\mathcal{F}^d$ let $g_\lambda^{-1}(1)=\{a\in\mathcal{F}^n|a_1=\lambda_1,\ldots,a_d=\lambda_d\}$. Since $\{g_\lambda^{-1}(1)\}_\lambda$ is a partition of $\mathcal{F}^n$, we have $\mathbf{Pr}[f=1]=\sum_{\lambda\in\mathcal{F}^d}\sum[f=g_\lambda]$. Therefore, there is λ_0 such that $\mathbf{Pr}[f=g_{\lambda_0}]=\mathbf{Pr}[f=1]/q^d$. Then $\mathbf{Pr}[f\neq g_{\lambda_0}]=1-\mathbf{Pr}[f=1]/q^d$. Now, if $\mathbf{Pr}[f=1]\le 1-2q^{-d}+q^{-2d}$, then $\mathbf{Pr}[f\neq g_{\lambda_0}]\le\mathbf{Pr}[f=1]+\mathbf{Pr}[g_{\lambda_0}=1]\le 1-q^{-d}+q^{-2d}$. Otherwise,

$$\mathbf{Pr}[f\neq g_{\lambda_0}]=1-\frac{\mathbf{Pr}[f=1]}{q^d}<1-\frac{1-2q^{-d}+q^{-2d}}{q^d}=1-\frac{1}{q^d}+\Theta(q^{-2d}).$$

Therefore, $\mathrm{IF}(d\text{-}\mathbf{APAS})\le 1-q^{-d}+\Theta(q^{-2d})$. □

Now we show

Theorem 27. *We have*

1. *There are one-sided testers for* **APLS**, **LS**, **APAS**, $(\le d)$-**AS** $(\le d)$-**APLS**, $(\le d)$-**LS**, $(\le d)$-**APAS** *and* $(\le d)$-**AS** *with proximity parameter* $\epsilon > 1/2$ *that make no queries.*
2. *There are one-sided testers for* d-**APLS** *and* d-**LS** *with proximity parameter* $\epsilon > 1 - q^{-d} + \Theta(q^{-3d/2})$ *that make no queries.*
3. *There are one-sided testers for* d-**APAS** *and* d-**AS** *with proximity parameter* $\epsilon > 1 - q^{-d} + \Theta(q^{-2d})$ *that make no queries.*

In particular,

Corollary 28. *We have*

1. *There are one-sided testers for* **Monomial**, **Term**, $(\le d)$-**Monomial**, *and* $(\le d)$-**Term** *with proximity parameter* $\epsilon > 1/2$ *that make no queries.*
2. *There are one-sided testers for* d-**Monomial** *with proximity parameter* $\epsilon > 1-2^{-d}+\Theta(2^{-3d/2})$ *that make no queries.*
3. *There are one-sided testers for* d-**Term** *and* d-**AS** *with proximity parameter* $\epsilon > 1 - 2^{-d} + \Theta(2^{-2d})$ *that make no queries.*

Proof. The result follows from Lemma 19 and Theorem 26. □

References

[1] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing low-degree polynomials over GF(2). In *Approximation, Randomization, and Combinatorial Optimization: Algorithms and Techniques, 6th International Workshop on Approximation Algorithms for Combinatorial Optimization Problems, APPROX 2003 and 7th International Workshop on Randomization and Approximation Techniques in Computer Science, RANDOM 2003, Princeton, NJ, USA, August 24-26, 2003, Proceedings*, pages 188–199, 2003. doi:10.1007/978-3-540-45198-3_17.

[2] Noga Alon, Tali Kaufman, Michael Krivelevich, Simon Litsyn, and Dana Ron. Testing reed-muller codes. *IEEE Trans. Information Theory*, 51(11):4032–4039, 2005. doi:10.1109/TIT.2005.856958.

[3] Manuel Blum, Michael Luby, and Ronitt Rubinfeld. Self-testing/correcting with applications to numerical problems. *J. Comput. Syst. Sci.*, 47(3):549–595, 1993. doi:10.1016/0022-0000(93)90044-W.

[4] Nader H. Bshouty. Almost optimal testers for concise representations. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, APPROX/RANDOM 2020, August 17-19, 2020, Virtual Conference*, pages 5:1–5:20, 2020. doi:10.4230/LIPIcs.APPROX/RANDOM.2020.5.

[5] Nader H. Bshouty and Oded Goldreich. On properties that are non-trivial to test. *Electronic Colloquium on Computational Complexity (ECCC)*, 13, 2022. URL: https://eccc.weizmann.ac.il/report/2022/013/.

[6] Sourav Chakraborty, David García-Soriano, and Arie Matsliah. Efficient sample extractors for juntas with applications. In *Automata, Languages and Programming - 38th International Colloquium, ICALP 2011, Zurich, Switzerland, July 4-8, 2011, Proceedings, Part I*, pages 545–556, 2011. doi:10.1007/978-3-642-22006-7_46.

[7] Xi Chen and Jinyu Xie. Tight bounds for the distribution-free testing of monotone conjunctions. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms, SODA 2016, Arlington, VA, USA, January 10-12, 2016*, pages 54–71. SIAM, 2016. doi:10.1137/1.9781611974331.ch5.

[8] Elya Dolev and Dana Ron. Distribution-free testing for monomials with a sublinear number of queries. *Theory of Computing*, 7(1):155–176, 2011. doi:10.4086/toc.2011.v007a011.

[9] Luisa Gargano, János Körner, and Ugo Vaccaro. Sperner capacities. *Graphs Comb.*, 9(1):31–46, 1993. doi:10.1007/BF01195325.

[10] Dana Glasner and Rocco A. Servedio. Distribution-free testing lower bound for basic boolean functions. *Theory of Computing*, 5(1):191–216, 2009. doi:10.4086/toc.2009.v005a010.

[11] Jay Goldman and Gian-Carlo Rota. On the foundations of combinatorial theory IV: finite vector spaces and Eulerian generating functions. *Studies in Applied Mathematics*, 49:239–258, 1970. URL: http://cr.yp.to/bib/entries.html#1970/goldman.

[12] Oded Goldreich, editor. *Property Testing - Current Research and Surveys*, volume 6390 of *Lecture Notes in Computer Science*. Springer, 2010. doi:10.1007/978-3-642-16367-8.

[13] Oded Goldreich. Reducing testing affine spaces to testing linearity. *Electron. Colloquium Comput. Complex.*, page 80, 2016. URL: https://eccc.weizmann.ac.il/report/2016/080.

[14] Oded Goldreich. *Introduction to Property Testing*. Cambridge University Press, 2017. URL: http://www.cambridge.org/us/catalogue/catalogue.asp?isbn=9781107194052, doi:10.1017/9781108135252.

[15] Oded Goldreich, Shafi Goldwasser, and Dana Ron. Property testing and its connection to learning and approximation. *J. ACM*, 45(4):653–750, 1998. doi:10.1145/285055.285060.

[16] Oded Goldreich and Dana Ron. One-sided error testing of monomials and affine subspaces. *Electron. Colloquium Comput. Complex.*, page 68, 2020. URL: https://eccc.weizmann.ac.il/report/2020/068.

[17] Daniel J. Kleitman and Joel H. Spencer. Families of k-independent sets. *Discret. Math.*, 6(3):255–262, 1973. doi:10.1016/0012-365X(73)90098-8.

[18] Moni Naor, Leonard J. Schulman, and Aravind Srinivasan. Splitters and near-optimal derandomization. In *36th Annual Symposium on Foundations of Computer Science, Milwaukee, Wisconsin, USA, 23-25 October 1995*, pages 182–191. IEEE Computer Society, 1995. doi:10.1109/SFCS.1995.492475.

[19] Michal Parnas, Dana Ron, and Alex Samorodnitsky. Testing basic boolean formulae. *SIAM J. Discrete Math.*, 16(1):20–46, 2002. URL: http://epubs.siam.org/sam-bin/dbq/article/40744.

[20] Dana Ron. Property testing: A learning theory perspective. *Foundations and Trends in Machine Learning*, 1(3):307–402, 2008. doi:10.1561/2200000004.

[21] Dana Ron. Algorithmic and analysis techniques in property testing. *Foundations and Trends in Theoretical Computer Science*, 5(2):73–205, 2009. doi:10.1561/0400000029.

[22] 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.

[23] Gadiel Seroussi and Nader H. Bshouty. Vector sets for exhaustive testing of logic circuits. *IEEE Trans. Inf. Theory*, 34(3):513–522, 1988. doi:10.1109/18.6031.

[24] Jun Wu, Yongxi Cheng, and Ding-Zhu Du. An improved zig zag approach for competitive group testing. *Discret. Optim.*, 43:100687, 2022. doi:10.1016/j.disopt.2022.100687.

Appendix: Testing Monomial and Term with Self-Corrector

Test-$(\le d)$**-Monomial**(f,ϵ)
Input: Oracle that accesses a Boolean function $f:\mathcal{F}_2^n\to\mathcal{F}_2$.
Output: Either "Accept" or "Reject".

1. If **AKKLR-Test**$(f,\min(\epsilon,2^{-d-3}))$ rejects then Reject.
2. Choose $m=O(2^{2d}\log d)$ uniformly at random $Z=\{z^{(1)},\ldots,z^{(m)}\}$.
3. Choose $t=2^{d+1}\log(100d)$, $P:=\{y^{(1)},\ldots,y^{(t)}\}\subset Z$ such that $P\subseteq f^{-1}(1)$.
4. If no such P exists, then Accept.
5. Let $y=Y(y^{(1)},\ldots,y^{(t)})$.
6. Choose $m=2^{d+1}\log(100)$ uniformly at random $x^{(1)},\ldots,x^{(m)}\in\mathcal{F}_2^n$
7. Use self-corrector to compute $z_i=g(y)(x^{(i)})$, $i\in[m]$.
   Here g is the degree-d polynomial that is close to f.
8. If $z_i=1$ for all $i\in[m]$, then Accept else Reject.

Figure 8: A Tester for $(\le d)$-**Monomial**.

In this appendix, we prove.

Theorem 29. *There is a one-sided ϵ-tester for $(\le d)$-**Monomial** that makes $O(1/\epsilon+d2^{2d})$ queries.*

The following is the self-corrector.

Lemma 20. *(Self-corrector [2]) Let $f:\mathcal{F}_2^n\to\mathcal{F}_2$ be a Boolean function that is ϵ-close to a polynomial g of degree d. Let $A=\mathcal{F}_2^{d+1}\backslash\{0^{d+1},10^d\}$. Then*

$$\mathbf{Pr}_{y^{(0)},y^{(1)},\ldots,y^{(d)}\in\mathcal{F}_2^n}\left[g(0)=\sum_{\lambda\in A\cup\{10^d\}} f\left(\sum_{i=0}^{d}\lambda_{i+1}y^{(i)}\right)\right]\ge 1-\epsilon(2^{d+1}-1),$$

and for every $x\in\mathcal{F}_2^n$,

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(d)}\in\mathcal{F}_2^n}\left[g(x)+g(0)=\sum_{\lambda\in A} f\left(\lambda_1 x+\sum_{i=1}^{d}\lambda_{i+1}y^{(i)}\right)\right]\ge 1-\epsilon(2^{d+1}-2).$$

For $y^{(1)},\ldots,y^{(t)}\in\mathcal{F}_2^n$, we define the random variable $Y(y^{(1)},\ldots,y^{(t)})\in\mathcal{F}_2^n$ to be $y=(y_1,\ldots,y_n)$ where $y_i=1$ if $(\forall j\in[t])y_i^{(j)}=1$ and[22] $y_i=x_i$, otherwise. Notice that, for a function $g:\mathcal{F}_2^n\to\mathcal{F}_2$, we have $g(y)=g(Y(y^{(1)},\ldots,y^{(t)})):\mathcal{F}_2^n\to\mathcal{F}_2$.

We now prove

Lemma 21. *Let $g:\mathcal{F}_2^n\to\mathcal{F}_2$ be a polynomial of degree d. Let $t=2^{d+1}\log(d/\delta)$. If g is a monomial, then*

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(t)},Y}[g(Y(y^{(1)},\ldots,y^{(t)}))\equiv 1\mid g(y^{(1)})=\cdots=g(y^{(t)})=1]=1.$$

[22] The variable x_i.

If g is not a monomial, then

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(t)},Y}[g(Y(y^{(1)},\ldots,y^{(t)}))\equiv 1 \mid g(y^{(1)})=\cdots=g(y^{(t)})=1]\le\delta.$$

Proof. Let $y = Y(y^{(1)},\ldots,y^{(t)})$. Suppose $g = x_{i_1}\cdots x_{i_k}$ is a monomial. Since for all $j\in[t]$, $g(y^{(j)})=1$ we have that for all $j\in[t]$ and all $\ell\in[k]$, $y^{(j)}_{i_\ell}=1$. Therefore, for all $\ell\in[k]$, $y_{i_\ell}=1$. Thus $g(y)=1$.

If g is not a monomial, then $g = Mh$, where M is a monomial and $h\not\equiv 1$ is a polynomial of degree $deg(g)-deg(M)$ that is independent of the variables in M and satisfies $h_{|x_i\leftarrow 0}\not\equiv 0$ for every $i\in[n]$. Suppose, wlog, $M = x_1x_2\cdots x_k$. Then h is of degree $d-k$ and is independent of $x_1,\ldots,x_k$. Let wlog, $M' = x_{k+1}\cdots x_d$ be one of the monomials of h. Then for any $i\in[k+1,d]$, we have[23]

$$\begin{aligned}\mathbf{Pr}[x_i=0\mid g(x)=1] &= \frac{\mathbf{Pr}[x_i=0,h(x)=1,M(x)=1]}{\mathbf{Pr}[h(x)=1,M(x)=1]}\\ &= \frac{\mathbf{Pr}[x_i=0,h(x)=1]\cdot\mathbf{Pr}[M(x)=1]}{\mathbf{Pr}[h(x)=1,M(x)=1]}\\ &\ge \mathbf{Pr}[x_i=0,h(x)=1]\\ &= \frac{1}{2}\mathbf{Pr}[h_{|x_i\leftarrow 0}(x)=1]\ge\frac{1}{2^{d+1}}.\end{aligned}$$

Now for any $i\in[k+1,d]$

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(t)}}[(\forall j\in[t])y^{(j)}_i=1\mid g(y^{(1)})=\cdots=g(y^{(t)})=1]\le\left(1-\frac{1}{2^{d+1}}\right)^t.$$

and

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(t)}}[(\exists i\in[k+1,d])(\forall j\in[t])y^{(j)}_i=1\mid g(y^{(1)})=\cdots=g(y^{(t)})=1]\le d\left(1-\frac{1}{2^{d+1}}\right)^t\le\delta.$$

So now, with probability at least $1-\delta$, $(\forall i\in[k+1,d])(\exists j\in[t])y^{(j)}_i=0$. Then, for $y = Y(y^{(1)},\ldots,y^{(t)})$, $y_i=1$ for all $i\in[k]$ and $y_i=x_i$ for all $i=[k+1,d]$. Therefore, $g(y)=h(y)\not\equiv 1$. □

We are now ready to prove Theorem 29. Consider the tester **Test-($\le d$)-Monomial** in Figure 8. In the first step, the tester runs the one-sided tester of Alon et al. [1], **AKKLR-Test**, that tests if the function f is $\min(\epsilon,2^{-d-3})$-close to a polynomial (over $\mathcal{F}_2$) of degree at most d. If f is ($\le d$)-**Monomial**, then **AKKLR-Test** accepts. If f is $\min(\epsilon,2^{-d-3})$-far from any polynomial of degree at most d, then, with probability at least 2/3, it rejects. So, after step 1, we may assume that f is $\min(\epsilon,2^{-d-3})$-close to g where g is a polynomial (over $\mathcal{F}_2$) of degree at most d. In particular,

$$\mathbf{Pr}[f=1]\ge\mathbf{Pr}[g=1]-\mathbf{Pr}[g\ne f]\ge 2^{-d}-\min(\epsilon,2^{-d-3})\ge 2^{-d-1}.$$

The query complexity of **AKKLR-Test** is $O(1/\epsilon+d2^{2d})$.

In steps 2-4, if f is ϵ-far from ($\le d$)-**Monomial**, then since $\mathbf{Pr}[f=1]\ge 2^{-d-1}$, with high probability, the tester succeeds in finding such $P\subseteq f^{-1}(1)$. The query complexity in steps 2-4 is $O(2^{2d}\log d)$.

[23]It is well known that for any non-zero polynomial g of degree d over $\mathcal{F}_2$, we have $\mathbf{Pr}[g=1]\ge 2^{-d}$.

Let $y = Y(y^{(1)}, \ldots, y^{(t)})$. Notice that $g(y)$ is a function $g(y) : \mathcal{F}_2^n \to \mathcal{F}_2$ and a polynomial of degree at most d. By Lemma 21, if f is a monomial, then $g = f$ and

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(t)},Y}[g(y) \equiv 1] = 1.$$

If f is ϵ-far from monomial (and $\min(\epsilon, 2^{-d-3})$-close to a polynomial (over $\mathcal{F}_2$) of degree at most d), then g is not a monomial and therefore

$$\mathbf{Pr}_{y^{(1)},\ldots,y^{(t)},Y}[g(y) \equiv 1] \le \delta.$$

Now steps 6-8 test if g is the constant one function. Since we only have access to a black box to f, the tester uses self-corrector to query g. This is possible by Lemma 20. If $g \equiv 1$, the self-corrector always returns $z_i = 1$, and the tester accepts. If $g \not\equiv 1$, then, since g is a polynomial of degree at most d, $\mathbf{Pr}_x[g(x) = 0] \ge 1/2^d$, and therefore, with high probability, one of the $x^{(i)}$ satisfies $g(y)(x^{(i)}) = 0$. Steps 6-8 make $O(2^{2d})$ queries. This completes the proof of the Theorem.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il