Summary: Let $F$ be a finite field of prime order $d < |F|/2$ and $m \in \mathbb{N}$. These notes present a low-degree tester that, given oracle access to a function $f : \mathcal{F}^m \rightarrow \mathcal{F}$, queries the function at $d + 2$ points and satisfies the following conditions:

1. If $f$ is an $m$-variate polynomial of degree $d$, then the tester accepts with probability 1.
2. If $f$ is $\delta$-far from the class of $m$-variate polynomials of degree $d$, then the tester rejects with probability at least $\min(0.5\delta, \Omega(d^{-2}))$.

The sequence of queries, $q_0, q_1, \ldots, q_{d+1}$, is generated by selecting at random $x, h \in F^m$, and setting $q_i = x + i h$.

The notes are based on the work of Rubinfeld and Sudan [7] (see Section 4 and the appendix in [7]).

Note: For sake of simplicity, we focus on the case of finite fields of prime cardinality. In this case, the field $F$ consists of the set $\mathbb{Z}_|F| = \{0, 1, \ldots, |F|\}$ with addition and multiplication modulo $|F|$. In the general case, the sequence $(x + i h)_{i=0}^{d+1}$ is replaced by the sequence $(x + e_i h)_{i=0}^{d+1}$, where $e_i$'s are distinct field elements, and the $\alpha_i$'s used in interpolation formula (i.e., Eq. (2)) should be determined accordingly.

1 Preliminaries

Let $F$ be a finite field of prime cardinality, and $d, m$ be integers. We consider functions $f : \mathcal{F}^m \rightarrow \mathcal{F}$, and the class $\mathcal{P}_{m,d}$ of $m$-variate polynomials of total degree $d$. Such functions are called low degree polynomials, because their (total) degree is significantly smaller than $|F|$.

As shown next, $f$ is in $\mathcal{P}_{m,d}$ if and only if its restriction to each line in $\mathcal{F}^m$ can be represented as a univariate polynomial of degree $d$, where a line in $\mathcal{F}^m$ is a sequence of the form $L_{\overline{x}, \overline{h}} \overset{\text{def}}{=} \{ \overline{x} + i\overline{h} : i \in \mathcal{F} \}$ for $\overline{x}, \overline{h} \in \mathcal{F}^m$.

**Theorem 1** (local characterization of multivariate polynomials): Let $|\mathcal{F}| > 2d$. The function $f : \mathcal{F}^m \rightarrow \mathcal{F}$ is in $\mathcal{P}_{m,d}$ if and only if for every $\overline{x}, \overline{h} \in \mathcal{F}^m$ there exists a degree-$d$ univariate polynomial $p_{\overline{x}, \overline{h}}$ such that $p_{\overline{x}, \overline{h}}(i) = f(\overline{x} + i\overline{h})$ for every $i \in \mathcal{F}$.
Proof: Clearly, the restriction of \( f \in \mathcal{P}_{m,d} \) to any line in \( \mathcal{F}^m \) can be represented as a univariate polynomial of degree \( d \), since for every fixed \( \mathcal{F} = (x_1, ..., x_m) \in \mathcal{F}^m \) and \( \mathcal{H} = (h_1, ..., h_m) \in \mathcal{F}^m \) it holds that \( f(\mathcal{X} + z\mathcal{H}) = f(x_1 + zh_1, ..., x_m + zh_m) \) is a degree \( d \) polynomial in \( z \).

The opposite direction is proved by induction on \( m \), where the base case (of \( m = 1 \)) is trivial. In the induction step (from \( m = 1 \) to \( m \)), given \( f : \mathcal{F}^m \rightarrow \mathcal{F} \), for every fixed \( e \in \mathcal{F} \), we consider the \((m-1)\)-variate polynomial \( f_e \) defined by \( f_e(x_1, ..., x_{m-1}) = f(x_1, ..., x_{m-1}, e) \). By the induction hypothesis, \( f_e \) is an \((m-1)\)-variate polynomial of degree \( d \) (since the restriction of \( f_e \) to any line in \( \mathcal{F}^{m-1} \) is a degree \( d \) univariate polynomial). On the other hand, for every fixed \((e_1, ..., e_{m-1}) \in \mathcal{F}^{m-1}\), it holds that \( f(e_1, ..., e_{m-1}, x) \) is a degree \( d \) univariate polynomial in \( x \) (by considering the line \( L(e_1, ..., e_{m-1}, 0) \)). The following claim implies that \( f \) is a polynomial of total degree at most \( 2d \).

Claim 1.1 (the degree of \( f \) is at most \( 2d \)): For every \( e \in \{0, 1, ..., d\} \), let \( \delta_e \) be the unique degree \( d \) univariate polynomial that satisfies \( \delta_e(e) = 1 \) and \( \delta_e(e') = 0 \) for every \( e' \in \{0, 1, ..., d\} \setminus \{e\} \). Then, \( f(\mathcal{X}) = \sum_{e=0}^{d} \delta_e(x_m) f_e(x_1, ..., x_{m-1}) \).

Proof: Fixing any \( e_1, ..., e_{m-1} \in \mathcal{F} \), we need to show that \( f(e_1, ..., e_{m-1}, x) = \sum_{e=0}^{d} \delta_e(x) f_e(e_1, ..., e_{m-1}) \). This holds since each side of the equation is a degree \( d \) univariate polynomial, whereas these two polynomials agree on \( d+1 \) points (i.e., for every \( e' \in \{0, 1, ..., d\} \), it holds that \( \sum_{e=0}^{d} \delta_e(e') f_e(e_1, ..., e_{m-1}) \) equals \( f_e(e_1, ..., e_{m-1}, e') \)).

To show that \( f \) is actually of degree \( d \), we consider for each \( \mathcal{H} \in \mathcal{F}^m \) the univariate polynomial \( g_{\mathcal{H}}(z) = f(z\mathcal{H}) \). Then, with probability at least \( 1 - \frac{\deg(f)}{\deg(z\mathcal{H})} \) over the choice of \( \mathcal{H} \in \mathcal{F}^m \), it holds that \( \deg(g_{\mathcal{H}}) = \deg(f) \). (This holds since the coefficient of \( z^{\deg(f)} \) in \( f(z\mathcal{H}) \) is a polynomial in \( \mathcal{H} \) of total degree at most \( \deg(f) \).) Using \( \deg(f) \leq 2d < |\mathcal{F}| \), we infer that \( \deg(g_{\mathcal{H}}) = \deg(f) \) for some \( \mathcal{H} \in \mathcal{F}^m \). But, on the other hand, \( \deg(g_{\mathcal{H}}) \leq d \) for every \( \mathcal{H} \in \mathcal{F}^m \), since \( g_{\mathcal{H}} \) describes the values of \( f \) on the line \( L_{0,\mathcal{H}} \).

Notation. For \( i = 0, 1, ..., d+1 \), let \( \alpha_i = (-1)^{i+1} \cdot \binom{d+1}{i} \).

Theorem 2 (local characterization of univariate polynomials): A univariate function \( g : \mathcal{F} \rightarrow \mathcal{F} \) has degree \( d < |\mathcal{F}| \) if and only if for every \( e \in \mathcal{F} \) it holds that

\[
\sum_{i=0}^{d+1} \alpha_i \cdot g(e+i) = 0 \tag{1}
\]

Proof: We first show that \( g \) has degree exactly \( d > 0 \) if and only if \( g'(x) \overset{\text{def}}{=} g(x+1) - g(x) \) has degree exactly \( d-1 \). Writing \( g(x) = \sum_{j=0}^{d} c_j \cdot x^j \), we get

\[
g'(x) = \sum_{j=0}^{d} c_j \cdot (x+1)^j - \sum_{j=0}^{d} c_j \cdot x^j \\
= \sum_{j=1}^{d} \sum_{k=0}^{j-1} (x+1)^k x^{j-1-k} \\
= \sum_{j=0}^{d-1} \sum_{k=0}^{j} (x+1)^k x^{j-k}
\]
\begin{align*}
&= \sum_{j=0}^{d-1} c_{j+1} \sum_{k=0}^{j} \left( \begin{array}{c} k \\ \ell \end{array} \right) x^\ell x^{j-k}
\end{align*}
and observe that the coefficient of \(x^{d-1}\) equals \(c_{d} \sum_{k=0}^{d-1} \left( \begin{array}{c} k \\ \ell \end{array} \right) = d \cdot c_{d}\). Since \(d < |\mathcal{F}|\), the claim follows.

We now prove the main claim (i.e., the characterization of univariate polynomials via Eq. (1)) by induction on \(d\). For the base case (i.e., \(d = 0\)) we observe that \(g\) is a constant function if and only if \(-g(e) + g(e + 1) = 0\) holds for every \(e \in \mathcal{F}\). For the induction step (i.e., from \(d - 1\) to \(d\)), we use the fact that \(g\) has degree \(d > 0\) if and only if \(g'\) has degree \(d - 1\). Using the induction hypothesis, the latter condition coincides with \(\sum_{i=0}^{d} (-1)^{i+1} \cdot \frac{d}{i} \cdot g'(e + i) = 0\). Hence, \(g\) has degree \(d\) if and only if

\[\sum_{i=0}^{d} (-1)^{i+1} \cdot \frac{d}{i} \cdot (g(e + i + 1) - g(e + i)) = 0.\]

Finally, note that

\[
\sum_{i=0}^{d} (-1)^{i+1} \cdot \frac{d}{i} \cdot (g(e + i + 1) - g(e + i))
\]

\[
= \sum_{i=0}^{d} (-1)^{i+1} \cdot \left( \frac{d}{i} \right) \cdot g(e + i + 1) - \sum_{i=0}^{d} (-1)^{i+1} \cdot \left( \frac{d}{i} \right) \cdot g(e + i)
\]

\[
= \sum_{j=1}^{d+1} (-1)^{j} \cdot \left( \frac{d}{j-1} \right) \cdot g(e + j) + \sum_{i=0}^{d} (-1)^{i} \cdot \left( \frac{d}{i} \right) \cdot g(e + i)
\]

\[
= g(e) + (-1)^{d+1} \cdot g(e + d + 1) + \sum_{i=1}^{d} (-1)^{i} \cdot \left( \frac{d}{i} \right) + \left( \frac{d}{i-1} \right) \right) \cdot g(e + i)
\]

\[
= - \sum_{i=0}^{d+1} (-1)^{i+1} \cdot \frac{d+1}{i} \cdot g(e + i)
\]

and the inductive claim follows.

Combining Theorems 1 and 2, we get:

**Corollary 3** Let \(|\mathcal{F}| > 2d\) and \(\alpha_{i} = (-1)^{i+1} \cdot \frac{d+1}{i}\). The function \(f : \mathcal{F}^{m} \rightarrow \mathcal{F}\) is in \(\mathcal{P}_{m,d}\) if and only if for every \(\overline{\pi}, \overline{h} \in \mathcal{F}^{m}\) it holds that

\[
\sum_{i=0}^{d+1} \alpha_{i} \cdot f(\overline{\pi} + i\overline{h}) = 0 \quad (2)
\]

**Proof:** Clearly (by Theorem 2),\(^1\) any \(f \in \mathcal{P}_{m,d}\) satisfies Eq. (2), for every \(\overline{\pi}, \overline{h} \in \mathcal{F}^{m}\). When proving the opposite direction, for every line \(L = L_{\overline{\pi}, \overline{h}}\), we use Eq. (2) on the sequence \((\overline{\pi} + e\overline{h}) + i\overline{h})_{i=0}^{d+1}\), for each \(e \in \mathcal{F}\), and infer (by Theorem 2) that the restriction of \(f\) to \(L\) is a univariate polynomial of degree \(d\). The point is that, for every line \(L = L_{\overline{\pi}, \overline{h}}\), we consider the function \(g_{L}(z) = f(\overline{\pi} + z\overline{h})\) and infer \(\sum_{i=0}^{d+1} g_{L}(e + i) = 0\) (for each \(e \in \mathcal{F}\)) by using \(\sum_{i=0}^{d+1} f((\overline{\pi} + e\overline{h}) + i\overline{h}) = 0\). (We complete the proof by Using the non-obvious direction of Theorem 1.) \(\blacksquare\)

\(^{1}\)Indeed, we also use the easy direction of Theorem 1.
2 The tester

The characterization provided in Corollary 3 asserts that the global condition $f \in \mathcal{P}_{m,d}$ can be decomposed into $|\mathcal{F}^m|^2$ local conditions, where each local condition refers to the value of $f$ at $d + 2$ points in $\mathcal{F}^m$. Such a local decomposition is a highly non-obvious phenomenon, and it is even more non-obvious that the corresponding characterization (in terms of the conjunction of all local conditions) is robust. That is, whereas a characterization merely states a dichotomy, a robust characterization relates the fraction of satisfied local conditions to the distance of the object from the global condition.

**Algorithm 4** (testing whether $f$ is in $\mathcal{P}_{m,d}$): Select uniformly, $x, h \in \mathcal{F}^m$, query $f$ at $x, x + \overline{h}, \ldots, x + (d + 1)\overline{h}$ and accept if and only if these values satisfy Eq. (2). That is, the tester accepts if and only if

$$\sum_{i=0}^{d+1} \alpha_i \cdot f(x + i\overline{h}) = 0$$

where $\alpha_i = (-1)^{i+1} \cdot \binom{d+1}{i}$.

Recall that $f \in \mathcal{P}_{m,d}$ if and only if Eq. (3) holds for every $\overline{x}, \overline{h} \in \mathcal{F}^m$. At times, it will be useful to write Eq. (3) as

$$f(x) = \sum_{i=1}^{d+1} \alpha_i \cdot f(x + i\overline{h}),$$

which asserts that the value of $f \in \mathcal{P}_{m,d}$ at $x$ is determined (via interpolation) by the value of $f$ on $d + 1$ points on the line $L_{x,\overline{h}}$.

**Theorem 5** (analysis of Algorithm 4): Let $\delta_0 = 1/(d + 2)^2$. Then, Algorithm 4 is a (one-sided error) proximity oblivious tester with detection probability $\min(\delta, \delta_0)/2$, where $\delta$ denotes the distance of the given function from $\mathcal{P}_{m,d}$.

**Proof:** Clearly, each $f \in \mathcal{P}_{m,d}$ is accepted by the tester with probability 1. Hence, the theorem follows by proving that if $f$ is $\delta$-far from $\mathcal{P}_{m,d}$, then it is accepted by the tester with probability at most $1 - \min(\delta, \delta_0)/2$. Towards this goal, we assume that $f$ is accepted with probability $1 - \epsilon \geq 1 - (\delta_0/2)$, and show that $f$ is $2\epsilon$-close to $\mathcal{P}_{m,d}$. This is shown by presenting a function $g$ and proving that $g$ is $2\epsilon$-close to $f$ and that $g$ is in $\mathcal{P}_{m,d}$.

The function $g : \mathcal{F}^m \rightarrow \mathcal{F}$ is defined so that $g(\overline{x})$ is the most likely to equal $\sum_{i=1}^{d+1} \alpha_i \cdot f(x + i\overline{h})$, when $\overline{h}$ is uniformly distributed. In other words, letting $\text{MAJ}_{\overline{h} \in \mathcal{F}^m} \{v_e\}$ denote the most frequently occurring value of $v_e$ when $e \in S$ (with ties are broken arbitrarily), we define

$$g(\overline{x}) \overset{\text{def}}{=} \text{MAJ}_{\overline{h} \in \mathcal{F}^m} \left\{ \sum_{i=1}^{d+1} \alpha_i \cdot f(x + i\overline{h}) \right\}$$

The intuition is that $g$ is likely to agree with $f$, since

$$\Pr_{\overline{x}, \overline{h} \in \mathcal{F}^m} \left[ \sum_{i=0}^{d+1} \alpha_i \cdot f(x + i\overline{h}) = 0 \right] = 1 - \epsilon,$$

and so $g$ is likely to satisfy Eq. (3) on random $\overline{x}, \overline{h} \in \mathcal{F}^m$. However, we need much stronger assertions than the one just made. Still, note that if $f \in \mathcal{P}_{m,d}$, then $g = f$ and so $g$ satisfies Eq. (3) on every $\overline{x}, \overline{h} \in \mathcal{F}^m$.

**Claim 5.1** (closeness): The function $g$ is $2\epsilon$-close to $f$. 
Proof: This is merely an averaging argument, which counts as bad any point $\mathbf{r}$ such that Eq. (3) is satisfied by at most half of the possible $\mathbf{r}$’s, while noting that otherwise $g$ agrees with $f$ on $\mathbf{r}$. Details follow.

Let $B$ denote the set of $\mathbf{r}$’s such that Eq. (3) is satisfied by at most half of the possible $\mathbf{r}$’s; that is, $\mathbf{r} \in B$ if and only if

$$\Pr_{\mathbf{r} \in F_m} \left[ \sum_{i=0}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h}) = 0 \right] \leq 0.5.$$  

By Eq. (5), $\Pr_{\mathbf{r} \in F_m}[\mathbf{r} \in B] \leq 2\epsilon$, because otherwise $\Pr_{\mathbf{r},\mathbf{h} \in F_m} \left[ \sum_{i=0}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h}) \neq 0 \right]$ with probability greater than $2\epsilon \cdot 0.5$. On the other hand, for every $\mathbf{r} \in F_m \setminus B$, it holds that

$$\Pr_{\mathbf{r} \in F_m} \left[ f(\mathbf{r}) = \sum_{i=1}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h}) \right] > 0.5,$$

which implies that $f(\mathbf{r})$ is the majority value (obtained by the r.h.s of the foregoing random variable) and hence $f(\mathbf{r}) = g(\mathbf{r})$. 

Recall that $g(\mathbf{r})$ was defined to equal the most frequent value of $\sum_{i=1}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h})$, where frequencies were taken over all possible $\mathbf{h} \in F_m$. Hence, $g(\mathbf{r})$ occurs with frequency at least $1/|F|$ (yet, we saw, in the proof of Claim 5.1, that on at least $1 - 2\epsilon$ of the $\mathbf{r}$’s it holds that $g(\mathbf{r})$ is the majority value). We next show that $g(\mathbf{r})$ is much more frequent: it occurs in a strong majority.

Claim 5.2 (strong majority): For every $\mathbf{r} \in F_m$, it holds that

$$\Pr_{\mathbf{r} \in F_m} \left[ g(\mathbf{r}) = \sum_{i=1}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h}) \right] \geq 1 - 2(d + 1)\epsilon.$$  

Proof: Fixing any $\mathbf{r} \in F_m$, we consider the random variable $Z = Z_{\mathbf{r}}(\mathbf{h})$ defined to equal $\sum_{i=1}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h})$, where the probability space is uniform over the choice of $\mathbf{h} \in F_m$. By Eq. (5), we have $\Pr_{\mathbf{r} \in F_m}[f(\mathbf{r}) = Z_{\mathbf{r}}] = 1 - \epsilon$, which means that for typical $\mathbf{r}$ the value $Z_{\mathbf{r}}$ is almost always a fixed value (i.e., $f(\mathbf{r})$), which implies that $Z_{\mathbf{r}} = g(\mathbf{r})$ with high probability. However, we want to establish such a statement for any $\mathbf{r}$, not only for typical ones.

The idea is to lower bound the collision probability of $Z_{\mathbf{r}}$, which means sampling it twice, via $\mathbf{h}_1$ and $\mathbf{h}_2$ respectively, and computing

$$\Pr_{\mathbf{h}_1,\mathbf{h}_2 \in F_m} \left[ \sum_{i=1}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h}_1) = \sum_{i=1}^{d+1} \alpha_i \cdot f(\mathbf{r} + i\mathbf{h}_2) \right].$$  

The key observation is that each point on each of these two lines is uniformly distributed in $F_m$ and hence we can apply Eq. (5) to such a point using a random direction. Furthermore, we can use the direction $\mathbf{h}_2$ (resp., $\mathbf{h}_1$) for the points on $L_{\mathbf{r},\mathbf{h}_1}$ (resp., $L_{\mathbf{r},\mathbf{h}_2}$), which allows to express each of the two sums in Eq. (6) by the same double summation (see Figure 1, which illustrates that the $j^{th}$ point on the line $L_{\mathbf{r},\mathbf{h}_1,\mathbf{h}_2}$ can be reached as the $i^{th}$ point on the line $L_{\mathbf{r},\mathbf{h}_1,\mathbf{h}_2}$).\footnote{Indeed, $(\mathbf{r} + j\mathbf{h}_1) + j\mathbf{h}_2 = (\mathbf{r} + j\mathbf{h}_2) + j\mathbf{h}_1$.}

As shown below, it follows that the collision probability is lower bounded by $1 - 2(d + 1)\cdot \epsilon$ (and consequently $\Pr[g(\mathbf{r}) = Z_{\mathbf{r}}] \geq 1 - 2(d + 1)\epsilon$).
We now turn to the actual proof, where an arbitrary $x \in \mathcal{F}^m$ is fixed (for the entire proof). For every $i, j \in [d+1]$, if $h_1$ and $h_2$ are uniformly and independently distributed in $\mathcal{F}^m$, then so are $x + ih_1$ and $jh_2$ (resp., $x + jh_2$ and $ih_1$). By Eq. (5), for every $i \in [d+1]$, it follows that,

$$\Pr_{h_1,h_2 \in \mathcal{F}^m} \left[ f(x + ih_1) = \sum_{j=1}^{d+1} \alpha_j \cdot f((x + ih_1) + jh_2) \right] \geq 1 - \epsilon,$$

and likewise for every $j \in [d+1]$,

$$\Pr_{h_1,h_2 \in \mathcal{F}^m} \left[ f(x + jh_2) = \sum_{i=1}^{d+1} \alpha_i \cdot f((x + jh_2) + ih_1) \right] \geq 1 - \epsilon.$$

Hence,

$$\Pr_{h_1,h_2 \in \mathcal{F}^m} \left[ \sum_{i=1}^{d+1} \alpha_i f(x + ih_1) = \sum_{j=1}^{d+1} \sum_{i=1}^{d+1} \alpha_i \alpha_j \cdot f(x + ih_1 + jh_2) \right] \geq 1 - (d+1) \cdot \epsilon$$

and

$$\Pr_{h_1,h_2 \in \mathcal{F}^m} \left[ \sum_{j=1}^{d+1} \alpha_j f(x + jh_2) = \sum_{i=1}^{d+1} \sum_{j=1}^{d+1} \alpha_i \alpha_j \cdot f(x + jh_2 + ih_1) \right] \geq 1 - (d+1) \cdot \epsilon,$$

which implies that

$$\Pr_{h_1,h_2 \in \mathcal{F}^m} \left[ \sum_{i=1}^{d+1} \alpha_i f(x + ih_1) = \sum_{j=1}^{d+1} \alpha_j f(x + jh_2) \right] \geq 1 - 2(d+1)\epsilon.$$ 

Note that the two summations in Eq. (11) represent two independent (and identically distributed) random variables, which are functions of $h_1$ and $h_2$ respectively. Furthermore, each of these summations is distributed identically to the random variable $Z = Z(h) \overset{\text{def}}{=} \sum_{i=1}^{d+1} \alpha_i f(x + ih)$, which is a function of a uniformly distributed $h \in \mathcal{F}^m$. This means that the collision probability of $Z$ (i.e., $\sum_u \Pr[Z = u]Z$) is at least $1 - 2(d+1)\epsilon$, which implies that the most frequent value occurs in
Let \( \sum_u \Pr[Z = u]^2 \leq \sum_u \Pr[Z = v] \cdot \Pr[Z = u] = \Pr[Z = v] \). \( \blacksquare \)

Using Claim 5.2, we now show that \( g \in \mathcal{P}_{m,d} \). This follows by combining Claim 5.3 with the characterization of \( \mathcal{P}_{m,d} \).

**Claim 5.3** \( (g \in \mathcal{P}_{m,d}): \) For every \( \overline{x}, \overline{h} \in \mathcal{F}^m \), it holds that \( \sum_{i=0}^{d+1} \alpha_i \cdot g(\overline{x} + i\overline{h}) = 0 \).

**Proof:** Fixing any \( \overline{x}, \overline{h} \in \mathcal{F}^m \) and using Claim 5.2, we infer that, for each \( i \in \{0, 1, ..., d + 1\} \), it holds that
\[
\Pr_{\overline{h} \in \mathcal{F}^m} \left[ g(\overline{x} + i\overline{h}) = \sum_{j=1}^{d+1} \alpha_j \cdot f((\overline{x} + i\overline{h}) + j\overline{h}) \right] \geq 1 - 2(d+1)\varepsilon. \tag{12}
\]

Rather than using the same direction \( \overline{h} \) for each \( i \), we use pairwise independent directions such that the direction \( \overline{h}_1 + i\overline{h}_2 \) is used for approximating \( g(\overline{x} + i\overline{h}) \), which means that we interpolate (at the point \( \overline{x} + i\overline{h} \)) according to the line \( L_i = L_{\overline{x} + i\overline{h}, \overline{h}_1 + i\overline{h}_2} \). Hence, the \( j^{\text{th}} \) point on the line \( L_i \) is \( (\overline{x} + i\overline{h}) + j \cdot (\overline{h}_1 + i\overline{h}_2) \), which can be written as \( (\overline{x} + j\overline{h}_1) + i \cdot (\overline{h} + j\overline{h}_2) \). Now, by the Eq. (5), for every \( j \in [d+1] \) it holds that
\[
\Pr_{\overline{h}_1, \overline{h}_2 \in \mathcal{F}^m} \left[ \sum_{i=0}^{d+1} \alpha_i \cdot f((\overline{x} + j\overline{h}_1) + i \cdot (\overline{h} + j\overline{h}_2)) = 0 \right] \geq 1 - \varepsilon. \tag{13}
\]

As shown below, when all equalities captured in Eq. (12)\&(13) hold (which happens with probability at least \( 1 - (d+2) \cdot 2(d+1)\varepsilon - (d+1) \cdot \varepsilon \)), it follows that
\[
\sum_{i=0}^{d+1} \alpha_i \cdot g(\overline{x} + i\overline{h}) = \sum_{i=0}^{d+1} \alpha_i \cdot \sum_{j=1}^{d+1} \alpha_j \cdot f((\overline{x} + i\overline{h}) + j \cdot (\overline{h}_1 + i\overline{h}_2)) = \sum_{j=1}^{d+1} \alpha_j \cdot \sum_{i=0}^{d+1} \alpha_i \cdot f((\overline{x} + j\overline{h}_1) + i \cdot (\overline{h} + j\overline{h}_2)) = \sum_{j=1}^{d+1} \alpha_j \cdot 0.
\]

The claim follows by noting that the event in question (i.e., \( \sum_{i=0}^{d+1} \alpha_i \cdot g(\overline{x} + i\overline{h}) = 0 \)) is fixed, and so if it occurs with positive probability (according to an analysis carried through in some auxiliary probability space) then it simply holds.

We now turn to the actual proof, where arbitrary \( \overline{x}, \overline{h} \in \mathcal{F}^m \) are fixed (for the entire proof). Let \( \overline{h}_1 \) and \( \overline{h}_2 \) be uniformly and independently distributed in \( \mathcal{F}^m \). For every \( i \in \{0, 1, ..., d+1\} \), using Claim 5.2, while noting that \( \overline{h}_1 + i\overline{h}_2 \) is uniformly distributed in \( \mathcal{F}^m \), we get
\[
\Pr_{\overline{h}_1, \overline{h}_2 \in \mathcal{F}^m} \left[ g(\overline{x} + i\overline{h}) = \sum_{j=1}^{d+1} \alpha_j \cdot f((\overline{x} + i\overline{h}) + j(\overline{h}_1 + i\overline{h}_2)) \right] \geq 1 - 2(d+1)\varepsilon. \tag{14}
\]

On the other hand, for every \( j \in [d+1] \), noting that \( \overline{x} + j\overline{h}_1 \) and \( \overline{h} + j\overline{h}_2 \) are uniformly and independently distributed in \( \mathcal{F}^m \), and using Eq. (5), we get
\[
\Pr_{\vec{h}_1, \vec{h}_2 \in \mathcal{F}^m} \left[ \sum_{i=0}^{d+1} \alpha_i \cdot f((\overline{x} + j\overline{h}_1) + i(\overline{h} + j\overline{h}_2)) = 0 \right] \geq 1 - \epsilon. \tag{15}
\]

Note that the argument to \( f \) (i.e., \((\overline{x} + j\overline{h}_1) + i(\overline{h} + j\overline{h}_2)\)) can be written as \((\overline{x} + i\overline{h}) + j(\overline{h}_1 + i\overline{h}_2)\). Hence, we get

\[
\Pr_{\vec{h}_1, \vec{h}_2 \in \mathcal{F}^m} \left[ \sum_{i=0}^{d+1} \sum_{j=1}^{d+1} \alpha_i \sum_{j=1}^{d+1} \alpha_j \cdot f((\overline{x} + i\overline{h}) + j(\overline{h}_1 + i\overline{h}_2)) = 0 \right] \geq 1 - (d+1) \cdot \epsilon. \tag{16}
\]

Combining Eq. (14) & (16), we get

\[
\Pr_{\vec{h}_1, \vec{h}_2 \in \mathcal{F}^m} \left[ \sum_{i=0}^{d+1} \alpha_i g(\overline{x} + i\overline{h}) = \sum_{i=0}^{d+1} \alpha_i \sum_{j=1}^{d+1} \alpha_j \cdot f((\overline{x} + i\overline{h}) + j(\overline{h}_1 + i\overline{h}_2)) = 0 \right] \geq 1 - (d+2) \cdot (d+1) \epsilon - (d+1) \epsilon. \tag{17}
\]

Using \((2d + 5)(d + 1) \epsilon < 1\) (which follows from \( \epsilon \leq 1/2(d + 2)^2 \)), we get

\[
\Pr_{\vec{h}_1, \vec{h}_2 \in \mathcal{F}^m} \left[ \sum_{i=0}^{d+1} \alpha_i g(\overline{x} + i\overline{h}) = 0 \right] > 0 \tag{18}
\]

and the claim follows (since \( \sum_{i=0}^{d+1} \alpha_i g(\overline{x} + i\overline{h}) = 0 \) is independent of the choice of \( \vec{h}_1, \vec{h}_2 \in \mathcal{F}^m \).)

Combining Claims 5.1 and 5.3 with the characterization of \( \mathcal{P}_{m,d} \), it follows that \( f \) is \( 2 \epsilon \)-close to \( \mathcal{P}_{m,d} \).

### 3 Final comments

The analysis of the Algorithm 4 follows the strategy used in the analysis (as presented in [4]) of the linearity tester of Blum, Luby, and Rubinfeld [2]. Indeed, the implementation of this strategy is more complex in the current setting (of low degree testing).

An improved analysis of a related tester appeared in [3]. This tester select uniformly, \( \overline{x}, \overline{h} \in \mathcal{F}^m \) and \( i \in \mathcal{F} \), query \( f \) at \( \overline{x}, \overline{x} + h, \ldots, \overline{x} + dh \) and \( \overline{x} + ih \), and accept if and only if there exists a degree \( d \) polynomial that agrees with these \( d + 2 \) values (i.e., a polynomial \( p \) such that \( p(j) = f(\overline{x} + j\overline{h}) \) for every \( j \in \{0, 1, \ldots, d\} \)). Friedl and Sudan [3] showed that the foregoing tester is a (one-sided error) proximity oblivious tester with detection probability \( \min(0.124, \delta/2) \), where \( \delta \) denotes the distance of the given function from \( \mathcal{P}_{m,d} \) (and 0.124 can be replaced by any constant \( c_0 \) smaller than \( 1/8 \)).

Our presentation has focused on the “high error regime”; that is, we have only guaranteed detection probability smaller than \( 1/2 \), and equivalently asserted that if \( f \) is accepted with high probability (i.e., \( 1 - \epsilon > 7/8 \)), then it is close (i.e., \( 2 \epsilon \)-close) to \( \mathcal{P}_{m,d} \). Subsequent research regarding low degree testing refers to the “low error regime” where one asks what can be said about a function that is accepted with probability at least \( 0.01 \) (or so). It turns out that in this case the function

---

3 Recall that \( \overline{x}, \overline{h} \in \mathcal{F}^m \) are fixed. Hence, the probability in Eq. (18) is either 0 and 1, whereas the bound rules out 0.

4 In addition, it is required that \( |\mathcal{F}| > c \cdot d \) (rather than \( |\mathcal{F}| > 2d \)), where \( c \) is a constant that depends on \( c_0 \).
is 0.99-close to $P_{m,d}$; that is, if $f$ is accepted with probability at least $\epsilon$, then it agree with some degree $d$ polynomial on at least $\epsilon$ fraction of the domain (cf. [1, 6]).

Actually, subsequent studies of low-degree tests are conducted in terms of the “robustness” of Theorem 1. Specifically, the robustness of the “line tester” is defined as the minimum, over all $f \not\in P_{m,d}$, of the ratio of the expected distance of the restriction of $f$ to a random line from $P_{1,d}$ (i.e., univariate degree $d$ polynomials) versus the distance of $f$ from $P_{m,d}$. The robustness of the “plane test” (which considers the restriction of the function to a random plane) can be defined similarly. In these terms, the aforementioned works establish the following results:

1. If $|F| \geq O(d)$, then the line tester has $\Omega(1)$ robustness (see Friedl and Sudan [3]).

2. For every $c > 1$ there exists a constant $c'$ such that if $|F| \geq c'd$, then the plane tester has robustness $c$ (see Raz and Safra [6]).

3. For every $c > 1$ there exists a polynomial $p$ such that if $|F| \geq p(d)$, then the line tester has robustness $c$ (see Arora and Sudan [1]).

In addition, a recent result of Guo, Haramaty, and Sudan [5] shows that the plane tester has $\Omega(1)$ robustness for every $|F| > (1 + \Omega(1)) \cdot d$.

References


