Limits of Approximation Algorithms	18 Mar, 2010 (TIFR)

Lec. 7: Low degree testing (Part I)

Lecturer: Prahladh Harsha *Scribe: Nutan Limaye*

In this lecture[1], we will give a local algorithm to test whether a given function is close to a low degree polynomial, i.e. check whether the function $f : \mathbb{F}^m \to \mathbb{F}$ (given as a truth-table) is close to the evaluation of some multi-variate polynomial of low degree without reading all of f. This problem is refered to as the "low-degree testing". The main references for this lecture include Lecture 14 from Sudan's course on inapproximability at MIT [Sud99] and the papers by Raz and Safra [RS97] and Moshkovitz and Raz [MR08] on the plane-point low-degree test.

Recap from last lecture: In the last lecture, we showed that the Walsh-Hadamard code has excellent locally checkable properties using the Fourier analysis of linearity test. Recall that the Walsh-Hadamard code is a $[k, 2^k, 2^{k-1}]_2$ code. The disadvantage of this code is that the rate of the code is inverse-exponential, it blows up the message exponentially! In fact, using the local checkability of the WH-code, we constructed the following PCP for NP: $\mathsf{NP} \subseteq \mathsf{PCP}_{1,1/2}(O(n^2), 14)$. Recall that we intend to eventually prove the following PCP theorem: $\mathsf{NP} \subseteq \mathsf{PCP}_{1,1/2}(O(\log n), O(1))$. A possible starting point would be to show that some code with not-too-bad-a-rate (inverse polynomial is fine) is locally checkable. The low-degree testing algorithm we will discuss today will show that the Reed-Muller code is in fact one such code: it has inverse-polynomial rate and is locally checkable. In later lectures, we will then prove the PCP theorem using the local checkability of Reed-Muller codes.

Low Degree Test: Let $\mathbb{F}$ is a finite field and $|\mathbb{F}| = q$ and $d < q$. A function $f : \mathbb{F}^m \to \mathbb{F}$ is said to be a degree d polynomial if it can be expressed as follows[2].

$$f(x_1, \ldots, x_m) = \sum_{i_1+\ldots+i_k \le d} a_{i_1\ldots i_m} x_1^{i_1} \ldots x_m^{i_m}, \qquad \forall (x_1, \ldots, x_m) \in \mathbb{F}^m.$$

Let us denote the set of all m-variate degree-d polynomial by $\mathcal{P}_d^m$. The main problem in "low-degree testing" is as follows:

> Given a function $f : \mathbb{F}^m \to \mathbb{F}$ (as a table of values), check whether f is a low-degree polynomial or far from being low-degree (i.e., if $f \in \mathcal{P}_d^m$ or $\delta(f, P)$ is large for all $P \in \mathcal{P}_d^m$) by querying f at as few points as possible.

Here, "farness" or its complement "closeness" is measured in terms of the Hamming distance, i.e. two functions $f, g : X \to Y$ are said to be δ-close to each other if $\Pr_{x\in X}[f(x) \neq g(x)] \le$

[1]Prahladh: These notes are far more detailed than the lecture it corresponds to. Thanks to the scribe Nutan for filling in all the missing details in the lecture.

[2]Here we do not distinguish between the formal representation of the function as a polynomial and the evaluation of the function.

δ. And a function f is said to be δ-close to a family of functions S, if there exists a function $g \in S$ such that f is δ-close to g.

We would like to design a low-degree test which has the following properties.

Completeness: If f is a low degree polynomial, then test accepts with probability 1.

Soundness: There exists $\delta_0 \in (0, 1)$ such that if $\Pr[\text{Test Rejects}] \leq \delta \leq \delta_0$ then f is $O(\delta)$-close to a low degree polynomial.

We would like to ask how large can δ_0 be?

The crucial property that has led to the local checkability of Reed-Muller codes is the following.

> The restriction of a degree d polynomial to lower dimensional spaces is also a degree d polynomial. In other words, if $f \in \mathcal{P}_d^m$ and s is a k-dimensional affine subspace of $\mathbb{F}^m$, then $f_{|_s} \in \mathcal{P}_d^k$.

7.1 History of the Low-degree Test

In this section, we will briefly go over the history of the low-degree testing problem. There is a long history of low degree testing. In fact, the history of the low-degree test not surprisingly mirrors the history of PCPs: each time a better low degree test was proved, it resulted in an improved probabilistic proof system.

7.1.1 Axis parallel test

1. Pick a random axis parallel line l. (i.e. pick an index $i \in_R [m]$ and then pick $x_1, x_2, \ldots x_{i-1}, x_{i+1}, \ldots, x_m$ randomly from $\mathbb{F}$.)
2. Query f on l. (i.e. query f on $(x_1, \ldots, x_{i-1}, x_i, x_{i+1}, x_m)$ for all $x_i \in \mathbb{F}$.)
3. Accept if $f_{|_l}$ is a univariate degree d polynomial.

This axis parallel test was proposed by Babai, Fortnow and Lund [BFL91]. They used this test to prove $\mathsf{MIP} = \mathsf{NEXP}$. In terms of the parameters mentioned earlier, they obtained $\delta_0 = O(1/md)$. Later Arora and Safra [AS98] improved the parameter by removing the dependence on the degree and got $\delta_0 = O(1/m)$. The dependence on m is unavoidable: consider a function which is low-degree along all but one axis. The test will fail only if the function is queried along that axes which happens with probability $1/m$. Polishchuk and Spielman [PS94] then further improved the parameters for the axis parallel test and gave a very clean analysis using resultants.

7.1.2 Random line test

This test was proposed by Gemmel, Lipton, Rubinfeld, Sudan, and Wigderson [GLR+91] to get around the $1/m$ barrier.

1. Choose a random line l
   (i.e., choose two random points $a, b \in \mathbb{F}^m$ and set $l = \{a + tb | t \in \mathbb{F}\}$.)

2. Query f along l.

3. Accept if $f_{|_l}$ is a univariate, degree d polynomial (i.,e $f_{|_l} \in \mathcal{P}_d^1$).

This got around the $1/m$ barrier as the line chosen was a random line not necessarily an axis-parallel line. This test was analyzed by Rubinfeld and Sudan [RS96] and Arora, Lund, Motwani, Sudan, and Szegedy [ALM+98] which eventually led to the PCP Theorem. Their analyses gave the following soundness

> There exists $\delta_0 = O(1)$ such that if $\Pr[\text{Test Rejects}] \leq \delta \leq \delta_0$ then f is $O(\delta)$-close to degree d polynomial.

The above theorem shows that if the line-test accepts the function with probability close to 1, then it must be the case that the function is very close to some (in fact unique) low-degree polynomial. Arora and Sudan [AS03] considerably improved this analysis and showed that even if the line-test passes with non-trivial probability, then it must be the case that the function has non-trivial agreement with some low-degree polynomial (not necessarily a unique one in this case).

> There exists $\varepsilon_0 = \text{poly}\left(m, d, \frac{1}{|\mathbb{F}|}\right)$ such that if $\Pr\left[f \in \mathcal{P}_d^1\right] \geq \delta$, then there exists a degree d polynomial P such that $\text{agr}(f, P) \geq \delta - \varepsilon_0$.

where agreement $\text{agr}(f, g)$ between two functions $f, g : X \to Y$ is defined as the fraction of points f and g agree on, i.e., $\Pr_{x \in X}[f(x) = g(x)]$. In fact, they proved the following even stronger statement

Theorem 7.1.1 (Line-Test [AS03])**.** *There exists $\varepsilon_0 = \text{poly}\left(m, d, \frac{1}{|\mathbb{F}|}\right)$ such that for all $f : \mathbb{F}^m \to \mathbb{F}$,*

$$\mathop{\mathbb{E}}_{l}\left[\text{agr}(f_{|_l}, \mathcal{P}_d^1)\right] \geq \delta \implies \text{agr}(f, \mathcal{P}_d^m) \geq \delta - \varepsilon_0.$$

where agreement $\text{agr}(f, G)$ between a function f and a set of functions G is defined as the maximum agreement between f and elements of G (i.e, $\max_{g \in G} \text{agr}(f, g)$).

7.1.3 The plane-test

Raz and Safra [RS97] suggested another low-degree test which is the plane analogue of the above line-test.

Plane-Test

1. Pick a random plane s.

2. Query f along s.

3. Accept if $f_{|_s}$ is a bivariate degree d polynomial (i.e, $f \in \mathcal{P}_d^2$).

It is easy to see that the completeness for this test is 1. As in the case of the Arora-Sudan analysis, Raz and Safra (independently and almost simultaneoulsy with Arora and Sudan) showed that

> There exists $\varepsilon_0 = \text{poly}\left(m, d, \frac{1}{|\mathbb{F}|}\right)$ such that if $\Pr\left[f \in \mathcal{P}_d^2\right] \geq \delta$, then there exists a degree d polynomial Q such that $\text{agr}(f, Q) \geq \delta - \varepsilon_0$.

The Raz-Safra analysis is simpler than the Arora-Sudan analysis and we will use their version of the low-degree test. Our main goal is to prove the following theorem, which is a slightly stronger statement than the above mentioned soundness statement.

Theorem 7.1.2 (Soundness of the Plane-Test [RS97]). *There exists* $\varepsilon_0 = \text{poly}\left(m, d, \frac{1}{|\mathbb{F}|}\right)$ *such that for all* $f : \mathbb{F}^m \to \mathbb{F}$,

$$\mathop{\mathbb{E}}_{s\text{ - }plane}\left[\text{agr}(f_{|s}, \mathcal{P}_d^2)\right] \geq \delta \implies \text{agr}(f, \mathcal{P}_d^m) \geq \delta - \varepsilon_0.$$

In other words, if $\mathbb{E}_{s-\text{ plane}}\left[\text{agr}(f_{|s}, \mathcal{P}_d^2)\right] \geq \delta$ (i.,e if locally the function f agrees with a degree d polynomial) then there is a global agreement in the sense that there exists $Q \in \mathcal{P}_d^m$ such that $\text{agr}(f, Q) \geq \delta - \varepsilon_0$.

7.2 The Plane-Point Test

In order to analyse the soundness of the plane-test, it will be convenient for us to work with a slightly different test, which we will call the "plane-point Test". Before describing this new test, we introduce some notation. Let $\mathcal{S}_k^m$ be the set of all affine subspaces of dimension k in $\mathbb{F}^m$. Recall that $\mathcal{P}_d^m$ is the set of all m-variate degree d polynomials. This new test has two inputs: the point oracle $f : \mathbb{F}^m \to \mathbb{F}$ as before and an additional plane oracle $\mathcal{A} : \mathcal{S}_2^m \to P_d^2$. The plane oracle is supposed to give for every plane s in $\mathbb{F}^m$, the degree d bivariate polynomial which corresponds to the restriction of f to the plane s [3].

Plane-Point Test

Inputs: $f : \mathbb{F}^m \to \mathbb{F}, \mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$.

1. Pick a plane at random, $s \in \mathcal{S}_2^m$.
2. Query the plane oracle at this plane.
3. Pick a point x at random from s.

[3] It is to be noted that all works on low-degree tests actually deal with tests of this form (i.e, one point oracle and an additional oracle). We took a slightly different presentation as that seemed more natural in the context of this course..

4. Accept if $f(x) = \mathcal{A}(s)(x)$

The following lemma lets us move from the plane-test to the plane-point test and vice-versa.

Lemma 7.2.1. $\mathbb{E}_{s\in\mathcal{S}_2^m}\left[\mathrm{agr}(f_{|_s}, \mathcal{P}_d^2)\right] \geq \delta$ *if and only if there exists an oracle* $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$ *such that* $\Pr_{s\in\mathcal{S}_2^m, x\in s}\left[\mathcal{A}(s)(x) = f(x)\right] \geq \delta$

Proof. The "if" part follows by definition. For the other ("if only") direction, let us first show the weaker statement: If $\Pr_{s\in\mathcal{S}_2^m}\left[f_{|_s} \in \mathcal{P}_d^2\right] \geq \delta$ then there exists an oracle $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$ such that $\Pr_{s\in\mathcal{S}_2^m, x\in s}\left[\mathcal{A}(s)(x) = f(x)\right] \geq \delta$

Let a plane s be called *good* if $f_{|_s} \in \mathcal{P}_d^2$ and *bad* otherwise. For each good plane s, let $\mathcal{A}(s)$ be $f_{|_s}$. For all the bad planes, let $\mathcal{A}(s)$ be assigned arbitrarily. With this $\mathcal{A}$, for all the good planes and for all x, $\mathcal{A}(s)(x) = f(x)$. Hence the statement. Now for the stronger claim, by the definition of agr we have

$$\mathop{\mathbb{E}}_s\left[\mathrm{agr}(f_{|s}, \mathcal{P}_d^2)\right] = \mathop{\mathbb{E}}_s\left[\max_{g\in\mathcal{P}_d^2}\left\{\mathrm{agr}(f_{|s}, g)\right\}\right]$$

For a fixed plane s let $\mathcal{A}(s)$ be the polynomial in $\mathcal{P}_d^2$ that achieves the maximum.

$$\begin{aligned}\mathop{\mathbb{E}}_s\left[\mathrm{agr}(f_{|s}, \mathcal{P}_d^2)\right] &= \mathop{\mathbb{E}}_s\left[\Pr_x\left[f(x) = \mathcal{A}(s)(x)\right]\right] \\ &= \Pr_{s,x}\left[f(x) = \mathcal{A}(s)(x)\right]\end{aligned}$$

Thus, proved. □

Given the above lemma, the soundness theorem for the plane-test translates as follows.

Theorem 7.2.2 (Soundness of Plane-point test (equivalent to Theorem 7.1.2))**.** *There exists* $\varepsilon_0 = \mathrm{poly}\left(\frac{md}{|\mathbb{F}|}\right)$ *such that for all functions* $f : \mathbb{F}^m \to \mathbb{F}$*, if there exists a plane oracle* $\mathcal{A}$ *for which*

$$\Pr_{s\in\mathcal{S}_2^m, x\in s}\left[\mathcal{A}(s)(x) = f(x)\right] \geq \delta$$

then there exists a degree d *polynomial* Q *such that* $\Pr_{x\in\mathbb{F}^m}\left[Q(x) = f(x)\right] \geq \delta - \varepsilon_0$

7.3 List decoding version of low degree test

The conclusion of the low degree test (which we wish to prove) claims that the function f has $\delta - \varepsilon_0$ agreement with some low-degree polynomial. Can there be more than polynomial with which the function has this agreement? In fact, for such low-agreement, there could be several polynomials with which the function has this agreement. The following lemma shows that however this list of polynomials with which a function has non-trivial agreement cannot be too long.

Lemma 7.3.1. *Suppose* $\delta \geq 2\sqrt{\frac{d}{q}}$*. Let* $f : \mathbb{F}^m \to \mathbb{F}$ *and let* $P_1, \ldots, P_t : \mathbb{F}^m \to \mathbb{F}$ *be all the degree* d *polynomials that have agreement at least* δ *then* $t \leq 2/\delta$*.*

In other words, f cannot have δ-agreement with too many polynomials as long as δ is not small.[4]

In fact, it can be shown that Theorem 7.2.2 has the following equivalent version in terms of the list of polynomials that agree with f.

Theorem 7.3.2. *There exists* $\varepsilon_0 = \text{poly}\left(\frac{md}{|\mathbb{F}|}\right)$. *Let* $f : \mathbb{F}^m \to \mathbb{F}$ *be a function and* $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$ *a planes oracle. For every* $\delta > \varepsilon_0$ *there exist* $t \le O(1/\delta)$ *polynomials* $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ *such that*

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) = f(x) \text{ and } \nexists i \in [t], {Q^i}_{|s} \equiv \mathcal{A}(s)\right] \le \delta.$$

In other words, there exist a short list of polynomials which explains all but δ-probability of the success of the low-degree test. The equivalence between Theorem 7.2.2 and Theorem 7.3.2 follows from the following two propositions, the first of which we prove in class and the second is defered to the appendix.

Proposition 7.3.3 (list-decoding to decoding)**.** *Let* $f : \mathbb{F}^m \to \mathbb{F}$ *be a function and* $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^2$ *(possibly randomized) such that*

$$\Pr_{s,x}\left[\mathcal{A}(s)(x) = f(x)\right] \ge \gamma$$

where the probability is also taken over the randomness of the plane oracle $\mathcal{A}$. *Furthermore suppose that for some* $\delta \ge \text{poly}(d/q)$ *that there exist* $t \le O(1/\delta)$ *polynomials* $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ *that explains almost all the success of the low-degree test, i.e.,*

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) = f(x) \text{ and } \nexists i \in [t], {Q^i}_{|s} \equiv \mathcal{A}(s)\right] \le \delta.$$

Then, there exists $i \in [t]$, *such that* $\Pr_x\left[f(x) = Q^i(x)\right] \ge \gamma - \delta - \text{poly}\left(\frac{d}{q}\right)$.

Proposition 7.3.4 (decoding to list-decoding)**.** *Let* $d \le d'$. *Let* $f : \mathbb{F}^m \to \mathbb{F}$ *be a function. Suppose* f *satisfies the low-degree test theorem, i.e., there exists some* $\alpha : [0,1] \to [0,1]$ *such that for every planes oracle* $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^m$, *we have*

$$\Pr[\mathcal{A}(s)(x) = f(x)] \ge \gamma \implies \exists Q \in \mathcal{P}_{d'}^m, \Pr[f(x) = Q(x)] \ge \alpha(\gamma).$$

Then, f *also satisfies the list-decoding version. In other words, there exists* $\varepsilon_0 = poly(d/q)$ *such that for all* $\delta > \varepsilon_0$ *and* $\delta' = \alpha(\delta - \varepsilon_0) - \varepsilon_0$ *such that for every planes oracle* $\mathcal{A} : \mathcal{S}_2^m \to \mathcal{P}_d^m$ *there exists a list of* $t \le 2/\delta'$ *polynomials* $Q^1, \ldots, Q^t : \mathbb{F}^m \to \mathbb{F}$ *of degree* d' *such that*

$$\Pr_{s \in \mathcal{S}_2^m, x \in s}\left[\mathcal{A}(s)(x) = f(x) \text{ and } \nexists i \in [t], {Q^i}_{|s} \equiv \mathcal{A}(s)\right] \le \delta.$$

[4] This lemma is Problem 4 in the 2nd problem set. For completeness, we present a proof in the appendix.

7.4 What we will prove in lecture

In the rest of today's and next lecture, we will prove the above theorem (ie., Theorem 7.2.2 and its equivalent list-decoding version Theorem 7.3.2) for the case when $m = 3$. In other words, we will prove the soundness of the plane-point test for planes in a cube. Observe that planes are 2=(3-1)-dimensional affine subspaces in $\mathbb{F}^3$. One can then check that the argument for planes-point test soundness actually generalizes to any ($(m-1)$-dimensional affine subspance point test in $\mathbb{F}^m$ giving us the following theorem.

Theorem 7.4.1. *There exists $\varepsilon_0 = \mathrm{poly}\left(\frac{md}{|\mathbb{F}|}\right)$ such that for all functions $f : \mathbb{F}^m \to \mathbb{F}$, if there exists a $(m-1)$-dimensional affine space oracle oracle $\mathcal{A} : \mathcal{S}^m_{m-1} \to \mathcal{P}^{m-1}_d$ for which*

$$\Pr_{s \in \mathcal{S}^m_{m-1}, x \in s} [\mathcal{A}(s)(x) = f(x)] \geq \delta$$

then there exists a degree d polynomial Q such that $\Pr_{x \in \mathbb{F}^m} [Q(x) = f(x)] \geq \delta - \varepsilon_0$. Or equivalently

$$\mathop{\mathbb{E}}_{s \in \mathcal{S}^m_{m-1}} \left[\mathrm{agr}(f_{|s}, \mathcal{P}^{m-1}_d)\right] \geq \delta \implies \mathrm{agr}(f, \mathcal{P}^m_d) \geq \delta - \varepsilon_0.$$

Theorem 7.2.2 follows from Theorem 7.4.1 by the following bootstrapping argument.

$$\begin{aligned}
\mathrm{agr}(f, \mathcal{P}^m_d) &\geq \mathop{\mathbb{E}}_{s_1 \in \mathcal{S}^m_{m-1}} \left[\mathrm{agr}(f_{|s_1}, \mathcal{P}^{m-1}_d)\right] - \varepsilon_0 \\
&\geq \mathop{\mathbb{E}}_{s_1 \in \mathcal{S}^m_{m-1}} \left[\mathop{\mathbb{E}}_{s_2 \in \mathcal{S}^m_{m-2}} \left[\mathrm{agr}\left(\left(f_{|s_1}\right)_{|s_2}, \mathcal{P}^{m-2}_d\right)\right] - \varepsilon_0\right] - \varepsilon_0 \\
&= \mathop{\mathbb{E}}_{s_1 \in \mathcal{S}^m_{m-1}} \left[\mathop{\mathbb{E}}_{s_2 \in \mathcal{S}^m_{m-2}} \left[\mathrm{agr}(f_{|s_2}, \mathcal{P}^{m-2}_d)\right] - \varepsilon_0\right] - \varepsilon_0 \\
&\vdots \\
&\geq \mathop{\mathbb{E}}_{s_1 \in \mathcal{S}^m_{m-1}} \left[\mathop{\mathbb{E}}_{s_2 \in \mathcal{S}^m_{m-2}} \left[\cdots \mathop{\mathbb{E}}_{s_{m-2} \in \mathcal{S}^m_2} \left[\mathrm{agr}(f_{|s_{m-2}}, \mathcal{P}^2_d)\right]\right]\right] - (m-2)\varepsilon_0 \\
&= \mathop{\mathbb{E}}_{s \in \mathcal{S}^m_2} \left[\mathrm{agr}(f_{|s}, \mathcal{P}^2_d)\right] - (m-2)\varepsilon_0
\end{aligned}$$

Thus, it suffices to prove the soundness of the $(m-1)$-dimensional space point test to prove the soundness of the plane-point test. We will assume that $m = 3$ for the rest of the lecture. It can be checked that the same proof generalizes to larger m. Even for $m = 3$, we will only be able to prove a weaker version of Theorem 7.4.1 in these two lectures. The polynomial Q that we will come up with will have the agreement $\delta^2 - \varepsilon_0$ instead of $\delta - \varepsilon_0$[5]. More precisely, we will prove the following theorem next week.

[5] For details on how to get around this (i.,e $\delta^2 \to \delta$), see Appendix of the next lecture.

Theorem 7.4.2. *There exists* $\varepsilon_0 = \text{poly}\left(\frac{d}{|\mathbb{F}|}\right)$ *such that for all functions* $f : \mathbb{F}^3 \to \mathbb{F}$*, if there exists a planes oracle oracle* $\mathcal{A} : \mathcal{S}_2^3 \to \mathcal{P}_d^2$ *for which*

$$\Pr_{s \in \mathcal{S}_2^3, x \in s} [\mathcal{A}(s)(x) = f(x)] \geq \delta$$

then there exists a degree d *polynomial* Q *such that* $\Pr_{x \in \mathbb{F}^m} [Q(x) = f(x)] \geq \delta^2 - \varepsilon_0$.

References

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. *Proof verification and the hardness of approximation problems.* J. ACM, 45(3):501–555, May 1998. (Preliminary Version in *33rd FOCS*, 1992). eccc:TR98-008, doi:10.1145/278298.278306.

[AS98] Sanjeev Arora and Shmuel Safra. *Probabilistic checking of proofs: A new characterization of NP.* J. ACM, 45(1):70–122, January 1998. (Preliminary Version in *33rd FOCS*, 1992). doi:10.1145/273865.273901.

[AS03] Sanjeev Arora and Madhu Sudan. *Improved low-degree testing and its applications.* Combinatorica, 23(3):365–426, 2003. (Preliminary Version in *29th STOC*, 1997). eccc:TR97-003, doi:10.1007/s00493-003-0025-0.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. *Non-deterministic exponential time has two-prover interactive protocols.* Comput. Complexity, 1(1):3–40, 1991. (Preliminary Version in *31st FOCS*, 1990). doi:10.1007/BF01200056.

[GLR+91] Peter Gemmell, Richard J. Lipton, Ronitt Rubinfeld, Madhu Sudan, and Avi Wigderson. *Self-testing/correcting for polynomials and for approximate functions.* In *Proc.* 23rd *ACM Symp. on Theory of Computing (STOC)*, pages 32–42. 1991. doi:10.1145/103418.103429.

[MR08] Dana Moshkovitz and Ran Raz. *Sub-constant error low degree test of almost-linear size.* SIAM J. Computing, 38(1):140–180, 2008. (Preliminary Version in *38th STOC*, 2006). eccc:TR05-086, doi:10.1137/060656838.

[PS94] Alexander Polishchuk and Daniel A. Spielman. *Nearly-linear size holographic proofs.* In *Proc.* 26*th ACM Symp. on Theory of Computing (STOC)*, pages 194–203. 1994. doi:10.1145/195058.195132.

[RS96] Ronitt Rubinfeld and Madhu Sudan. *Robust characterizations of polynomials with applications to program testing.* SIAM J. Computing, 25(2):252–271, April 1996. (Preliminary Version in *23rd STOC*, 1991 and *3rd SODA*, 1992). doi:10.1137/S0097539793255151.

[RS97] Ran Raz and Shmuel Safra. *A sub-constant error-probability low-degree test, and a sub-constant error-probability PCP characterization of NP.* In *Proc.* 29*th ACM Symp. on Theory of Computing (STOC)*, pages 475–484. 1997. doi:10.1145/258533.258641.

[Sud99] Madhu Sudan. *6.893: Approximability of optimization problems*, 1999. (A course on Approximability of Optimization Problems at MIT, Fall 1999).

A Proof of Lemma 7.3.1

Lemma 7.3.1 (Restated) *Suppose $\delta \geq 2\sqrt{\frac{d}{q}}$. Let $f : \mathbb{F}^m \to \mathbb{F}$ and let $P_1, \ldots, P_t : \mathbb{F}^m \to \mathbb{F}$ be all the degree d polynomials that have agreement at least δ then $t \leq 2/\delta$.*

Proof of Lemma 7.3.1. Let A_i be $\{x \mid f(x) = P_i(x)\}$. We have that for each $i \in [t]$ $|A_i| \geq \delta q^m$. Any two distinct degree d polynomials can agree on at most $\frac{d}{q}$ fraction of points by Schwartz-Zippel, i.e. $|A_i \cap A_j| \leq \frac{d}{q} q^m$ for all $i \neq j$ and $i, j \in [t]$.

$$\cup_i A_i \subseteq \mathbb{F}^m$$

by inclusion-exclusion:

$$\sum_i A_i - \sum_{i \neq j} |A_i \cap A_j| \leq q^m$$

$$t\delta q^m - \binom{t}{2} \frac{d}{q} q^m \leq q^m$$

Assume for the sake of contradiction that $t = \frac{2}{\delta} + \varepsilon$. Therefore, $t\delta q^m$ is at least $2q^m$. Also, $\binom{t}{2} \frac{d}{q} q^m$ is at most q^m as long as $\delta \geq 2\sqrt{\frac{d}{q}}$, which is a contradiction. □