A PCP of proximity for Real Algebraic Polynomials

Klaus Meer

BTU Cottbus-Senftenberg, Computer Science Institute,
Platz der Deutschen Einheit 1, D-03046 Cottbus
Email: meer@b-tu.de

Abstract. Let $f : F_q^k \mapsto \mathbb{R}$ be a function given via its table of values, where $F_q := \{0, 1, \ldots, q-1\} \subset \mathbb{R}, k, q \in \mathbb{N}$. We design a randomised verification procedure in the BSS model of computation that verifies if f is close to an algebraic polynomial of maximal degree $d \in \mathbb{N}$ in each of its variables. If f is such an algebraic polynomial there exists a proof certificate that the verifier will accept surely. If f has at least distance $\epsilon > 0$ to the set of max-degree algebraic polynomials on F_q^k, the verifier will reject any proof with probability at least $\frac{1}{2}$ for large enough q. The verification procedure establishes a real number PCP of proximity, i.e., it has access to both the values of f and the additional proof certificate via oracle calls. It uses $O(k \log q)$ random bits and reads $O(1)$ many components of both f and the additional proof string, which is of length $O((kq)^{O(k)})$. The paper is a contribution to the not yet much developed area of designing PCPs of proximity in real number complexity theory.

1 Introduction

Property testing in the last decades has evolved as an important area in theoretical computer science. One of its several versions studies fast randomized verification algorithms that yield an approximate decision making for a decision problem L in the following sense: given an input x and an error bound $\epsilon > 0$, the verification should confirm with probability 1 if $x \in L$ and reject every x that is not ϵ-close[1] to S with large enough constant probability. Most importantly, the verifier may access components of x only by oracle calls and one major goal is to reduce the number of such calls. In addition to this one-sided-error definition other variants have been studied as well. Property testing among other applications has become crucial in relation with designing probabilistically checkable proofs PCPs and proving the famous PCP theorem [1, 2]. In the context of PCPs the question is varied; here, the verifier has full access to the input x and oracle access to an additional certificate meant to provide a proof that $x \in L$. In yet another scenario, so called PCPs of proximity (a notion coined in [6]), both x and an additional certificate are accessible via oracle calls and again one major goal is to give an approximate decision using as few as possible oracle calls to

[1] where closeness usually is measured by using the Hamming distance of strings.

both objects. A thorough presentation of the field can be found, for example, in [12].

Similar questions also played a crucial role in using algebraic methods to derive a real number analogue of the PCP theorem in the computational model by Blum, Shub, and Smale, BSS model henceforth, over the real numbers [5]. Whereas in the first proof of the classical PCP theorem in [1, 2] algebraic polynomials defined over finite fields are used crucially, the proof of the real number $\mathrm{PCP}_{\mathbb{R}}$ theorem heavily relies on using trigonometric polynomials on suitable subsets of $\mathbb{R}$ instead. They were in one major step of the proof used as coding objects for real solutions of a quadratic system of polynomial equations; then, a PCP of proximity was designed to show that trigonometric polynomials are useful in this context.

It remained open whether algebraic polynomials can be used as coding objects as well, i.e., whether they can be tested by a real number PCP of proximity using the same (low) amount of resources. The purpose of this paper is to answer this question in the positive. Our construction heavily relies on the use of trigonometric polynomials in [5] for designing segmented verifiers for real number problems and on the structure of algebraic polynomials on arbitrary finite subsets of $\mathbb{R}^k$ as analysed in [11]. The main result complements the one of [11]; therein, a property test for algebraic polynomials on such general domains is designed which uses a non-constant number of oracle queries. The PCP of proximity given in this paper reduces the number of proof components read by the verifier to be constant, having access to an additional proof certificate beside the table of function values. Also from this additional certificate the verifier inspects a constant number of components.

The present paper extends the still small list of objects for which real number PCPs of proximity exist by algebraic polynomials - a central class for many problems studied in BSS computability over $\mathbb{R}$.

1.1 Previous work and outline

In the first proof of the PCP theorem in the Turing model [2, 1] multivariate algebraic polynomials defined on finite fields were used as coding objects for satisfying assignments of instances of the 3SAT problem. Testing a function given by a table of its values for being close to such a polynomial was one key ingredient in the entire proof. Most importantly, the test had to have a segmented structure, see below, in order to be used in a further proof step called verifier composition.

When trying to do the same in the real number BSS model [7], major difficulties arise from the fact that a function value table can only specify a function on a finite domain which, as subset of the reals, is not any longer a field. Loosing the field structure causes severe problems when using algebraic polynomials in the PCP framework over $\mathbb{R}$.

In [15], a low degree test designed by Friedl et al. in [11] for functions $f : F^k \mapsto \mathbb{R}$ on finite domains $F \subset \mathbb{R}$ was used to prove the existence of short almost transparent proofs for the real number complexity class $\mathrm{NP}_{\mathbb{R}}$. Though the test is able to verify closeness to an algebraic polynomial of maximal degree d in each of its variables, it lacks the main feature of segmentation. This means the following: A verifier is called segmented if it reads $O(1)$ positions in the input table for f as well as $O(1)$ segments of an additional proof certificate π provided by a prover; here, a certificate is a sequence of reals and a segment is a consecutive subsequence of it. The segments are allowed to have non-constant length, but they have to be queried in this structured form. This is a basic requirement in the PCP framework for using such a verifier in the so-called composition step - another important keystone to reduce the query complexity.

In [5] the authors succeeded in proving this theorem using algebraic methods and replacing the role of algebraic polynomials by trigonometric ones. [2] A significant amount of work was devoted to developing a test, more precisely a PCP of proximity, for trigonometric polynomials that is in segmented form. It relies on the fact that at least some features of finite fields can be regained when considering trigonometric polynomials on finite subdomains of $\mathbb{R}$. However, the authors have not been able to design a similar test for algebraic polynomials that can be used as ingredient of a proof of the real PCP theorem.

In the present paper we show that such a test can be designed once we have the machinery from [5] at hand. There are two main previous results needed in our approach. The actual test for closeness to an algebraic polynomial uses (a variant of) a result from [11]. It gives an estimate for the distance of a function $f : F^k \mapsto \mathbb{R}$ to algebraic polynomials by distances of f to the set of functions that are polynomials in at least one variable. The main task is to put this test procedure into segmented form. To do so, we again use trigonometric polynomials for coding certain restrictions of algebraic ones. This gives a segmented test algorithm using $O(k \log |F|)$ random bits and making $O(1)$ inspections of the table of function values for f as well as $O(1)$ inspections into proof segments of length $O(|F|^2)$. In a final standard step, the technique of verifier composition as used in [5] for the real number framework can be applied to reduce the total number of proof components read to be constant. Our test procedure complements the one from [11], which actually is a property testing algorithm.

The paper is organised as follows: Section 2 collects some basic definitions and states the main result of this paper. Its proof is described in Section 3. In its first subsection, we describe and analyse the closeness test verifying whether a function is close to an algebraic polynomial. Section 3.2 is the main part of the paper. Here, we explain how the closeness test can be put into segmented form necessary for verifier composition. Since the construction heavily relies on the low-degree test for trigonometric polynomials from [5], we first recall those results in the form we need them. Then we show how trigonometric polynomials can be used to code the information needed in the closeness test for algebraic polynomials in such a way that the letter can be performed in segmented form and how this leads to our main result. Section 3.3 briefly explains how the

[2] Note that the real number PCP theorem had been established in the BSS model earlier in [4] by a more combinatorial proof along the lines of [10].

technique of real verifier composition leads to our main result. We close with some concluding remarks.

2 Basic definitions, main result

We assume the reader to be familiar with the very basics of the BSS model of computation and its complexity theoretic features over the real numbers, see [7], and [16] for some surveys on more recent developments. Our main objects of interest are real valued functions that are algebraic polynomials on a finite subset of some $\mathbb{R}^k$. More precisely, the following definition is fundamental.

Definition 1. *Let $q, k, d \in \mathbb{N}$ and let $F_q := \{0, 1, \ldots, q-1\} \subset \mathbb{R}$.*

a) The set $P(k, d)$ denotes all functions $f : F_q^k \mapsto \mathbb{R}$ that have an extension to $\mathbb{R}^k$ being a polynomial with maximal degree d in each of its variables.

b) For all $1 \le i \le k$ we denote by $P_i(k, d)$ the set of all functions $f : F_q^k \mapsto \mathbb{R}$ that have an extension $\tilde{f} : \mathbb{R}^k \mapsto \mathbb{R}$ being a polynomial of degree at most d in its i-th variable. This means that whenever a point $x \in \mathbb{R}^k$ is fixed, the map $t \mapsto \tilde{f}(x + te_i)$ with $e_i \in \mathbb{R}^k$ being the i-th unit vector is a univariate polynomial in t of degree at most d. It is not hard to see that $P(k, d) = \bigcap\limits_{i=1}^{k} P_i(k, d)$. [3]

c) The distance of two functions $f, g : F_q^k \mapsto \mathbb{R}$ is defined as $d(f, g) := \frac{1}{q^k}|\{x \in F_q^k | f(x) \neq g(x)\}|$. Similarly, for the distance between an f and a set A of functions from $F_q^k \mapsto \mathbb{R}$ we define $d(f, A) := min\{d(f, g) | g \in A\}$.

Below, we shall choose q to be (without loss of generality) a prime and large enough in relation to k, d, and $1/\epsilon$, where $\epsilon > 0$ is a constant error bound, for our results to hold. Our aim is to design a verification procedure that figures out whether a given function value table represents with high probability an algebraic polynomial of certain max-degree. The concept of such a verification procedure in the BSS model and the resources it uses is defined next. We directly focus on the task of designing a PCP of proximity for real algebraic polynomials. The corresponding algorithms use randomisation and are allowed to inspect an additional proof certificate in order to come to a decision.

Definition 2. *a) Let $r, u : \mathbb{N} \to \mathbb{N}$ be two resource functions. A real probabilistic $(r(n), u(n))$-restricted verifier V for testing algebraic polynomials is a randomised real BSS machine; on input $f : F_q^k \mapsto \mathbb{R}$, given via a table of its $n := q^k$ real function values, V first generates uniformly and independently a string ρ of $O(r(n))$ random bits. Using ρ it makes $O(u(n))$ non-adaptive queries into the table for f and into an additional proof certificate $\pi \in \mathbb{R}^\infty := \bigsqcup_{i \ge 1} \mathbb{R}^i$. A query is made by writing an address on a query tape and then in one step the real number stored at that address in the table or in*

[3] This can be shown by easy induction on k, see for example [3], pages 225ff.

π, respectively, is returned. The verifier uses the results of the queries and computes in time polynomial in n its decision 'accept' or 'reject'.

b) We call a verifier V segmented *if the queries are structured such that V asks $O(1)$ many segments of length at most $O(u(n))$ from the table for f and the certificate π. Note that these objects are given as elements in $\mathbb{R}^\infty$, thus a segment is sequence of contiguous components of real numbers in such an element.*

*c) Let $\epsilon > 0$. A verifier for testing algebraic polynomials is ϵ-*reliable *if the following conditions are satisfied. If $f \in P(k,d)$, there is a proof certificate π such that V accepts (f,π) with probability 1. And if $d(f,P(k,d)) > \epsilon$, then for all certificates π the verifier V rejects (f,π) with probability $> \frac{1}{2}$.*

Note that the segmentation requirement only is meaningful when the number of queries is not yet constant. Segmentation is crucial for obtaining our main result:

Theorem 1. *Let $\epsilon > 0$ be fixed; let q be a prime and let $q,k,d \in \mathbb{N}$ be such that $q \in \Omega(\frac{k^2d^3}{\epsilon^2})$ and $F_q := \{0,1,\ldots,q-1\} \subset \mathbb{R}$. There is a $(O(k\log q), O(1))$-restricted verifier that is ϵ-reliable for testing whether a given $f : F_q^k \mapsto \mathbb{R}$ is an algebraic polynomial of maximal degree d in each of its variables. The verifier gets as input a table of the function values of f together with a proof certificate of length $O((kq)^{O(k)})$. Its running time is polynomial in kq.*

Using the techniques behind the proof of the real number $\mathrm{PCP}_\mathbb{R}$ theorem in [5], in particular verifier composition, the theorem actually follows easily from the following one, in which the verifier's query complexity is not yet constant and thus segmentation is an important requirement. Proving Theorem 2 therefore is the major task that will be solved in this paper.

Theorem 2. *Let $\epsilon > 0$ be fixed, q be a prime and $F_q := \{0,1,\ldots,q-1\} \subset \mathbb{R}$. Let $q,k,d \in \mathbb{N}$ be s.t. $q \in \Omega(\frac{k^2d^3}{\epsilon^2})$. There is a* segmented *and $(O(\frac{1}{\epsilon}k\log q), O(q^2))$-restricted verifier that is ϵ-reliable for testing whether a given $f : F_q^k \mapsto \mathbb{R}$ is an algebraic polynomial of maximal degree d in each of its variables. The verifier gets as input a table of the function values of f together with a proof certificate of length $O((kq)^{O(k)})$, i.e., it is a PCP of proximity. Its running time is polynomial in kq.*

An outline for proving Theorems 1 and 2 is as follows. Two steps are needed. The first consists of a test actually verifying closeness of a given f to a max-degree d polynomial. The design and analysis of this test, given in Theorem 3, is based on a variant of a result from [11] relating $d(f,P(k,d))$ to the sum of distances $\sum\limits_{i=1}^{k} d(f,P_i(k,d))$. Its resources are not yet those required. In order to reduce it we want to apply the classical technique of verifier composition. However, to do so the closeness test has to be put into segmented form which it does not have. Whereas a general procedure for putting a verifier into segmented form for the Turing model has been developed in relation with the first proof of the classical PCP theorem, a similar technique in the real number framework needs significant changes. A major part of [5] is devoted to design the relevant steps in relation with a proof of the PCP theorem in the real number BSS model. More precisely, a closeness test in form of a PCP of proximity is given for trigonometric polynomials, i.e., [5] solves for trigonometric problems the question we are now looking for to solve for algebraic polynomials. Our way to succeed with the latter is based on the former. We therefore in the second proof step show that the ideas from [5] as well can be used to put the above closeness test for algebraic polynomials into segmented form. This will prove Theorem 2. Our main Theorem 1 then follows by applying the verifier composition technique for real number verifiers as designed in [5].

3 Segmentation as main task

We now explain how the main result is proved. We start with describing and analyzing the test for verifying proximity of a function to an algebraic polynomial of given max-degree. The significantly more intricate part of segmenting this test is done in Section 3.2. Therein, we recall the necessary results from [5] for testing trigonometric polynomials and show, how this can be used to put our proximity test into a segmented form. Note that this step is by far not straightforward given the results from [5]. The final step then will apply verifier composition for achieving the claim of Theorem 1.

3.1 Distance to paraxial univariate restrictions

In this subsection we study the distance of an algebraic polynomial to paraxial univariate restrictions. We describe a test for verifying closeness of a function to an algebraic polynomial and give the test analysis.

Proposition 1 below occurs as an intermediate result in a slightly different form within the proof of Theorem 2.2 in [11], page 61. For sake of completeness and since that paper might not be easily available we include a proof here. We also correct some minor typos.

Proposition 1. *Let $q, k, d \in \mathbb{N}$ be such that $q \geq 18kd^3$ and define $F_q := \{0, 1, \ldots, q-1\}$. Let $f : F_q^k \to \mathbb{R}$ and $f_i \in P_i(k, d)$ for $1 \leq i \leq k$ be given. Then the following holds, where $\mu := \frac{\sqrt{d}}{\sqrt{18q}}$:*

$$\frac{1}{6} \cdot d(f, P(k,d)) \;\leq\; 2k\mu + d(f, f_1) + \sum_{j=1}^{k-1} d(f_j, f_{j+1}).$$

Proof. Before we give the proof note that the major change in our assertion with respect to the statement as it occurs on page 61, right column of [11] is the following: Our statement is about an arbitrary set of polynomials $f_i \in P_i(k, d), 1 \leq$

$i \leq k$, whereas in [11] the authors consider $f_i \in P_i(k,d)$ that minimize the distance from f to $P_i(k,d)$. However, in the proof of the intermediate result this optimality of the f_i's is not used.[4]

Now towards the proof of the statement as we need it. The proof in [11] uses a result from [2] and an easy corollary of it, stated as Lemmas 4.4 and 4.5 in [11]. These two results lead in [11], page 61 to the following alternatives, that we take as starting point for proving the proposition.

Lemma 1. *Let F_q, q, k, d be as in the statement of the proposition, define $\mu := \frac{\sqrt{d}}{\sqrt{18q}}$ and let $g : F_q^k \mapsto \mathbb{R}$ be an element of $P_1(k,d)$. Then either*

$$\left|\{c \in F_q \mid d(g|_{x_1=c}, P(k-1,d)) \leq \frac{1}{6}\}\right| \;\leq\; 2d-1 \tag{1}$$

or

$$\left|\{c \in F_q \mid \;\; d(g|_{x_1=c}, P(k-1,d)) \leq d(g, P(k,d)) - \mu\}\right| \;\leq\; 6\mu q \tag{2}$$

Now let functions $f, f_1, \ldots, f_k$ with $f_i \in P_i(k,d)$ be given. We use the lemma to show by induction on i the following

Claim: For all $1 \leq i \leq k$ and any point $(c_1, \ldots, c_i) \in F_q^i$ except for at most a fraction of $6i\mu$, i.e., except for at most $6iq^i\mu$ many points, it is

$$\frac{1}{6}d(f, P(k,d)) \leq i\mu + d(f, f_1) + \sum_{j=1}^{i-1} d(f_j|_{x_1=c_1,\ldots,x_j=c_j}, f_{j+1}|_{x_1=c_1,\ldots,x_j=c_j}) + \\ + d(f_i|_{x_1=c_1,\ldots,x_i=c_i}, P(k-i,d)).$$

Proof (of the Claim). For $f_1 \in P_1(k,d)$ one of the alternatives (1) or (2) holds according to Lemma 1. If (1) is satisfied we have $d(f_1|_{x_1=c_1}, P(k-1,d)) > \frac{1}{6}$ for at least $q-2d+1$ choices of $c_1 \in F_q$. Clearly, $d(f, P(k,d)) \leq 1$, so $\frac{1}{6}d(f, P(k,d)) \leq \frac{1}{6} < d(f_1|_{x_1=c_1}, P(k-1,d))$ for a fraction of at least $1 - \frac{2d-1}{q} \geq 1 - 6\mu$ choices for c_1. The last inequality results from $q > 2d$ and the definition of μ.

If alternative (2) holds, then for all but an exception of at most $6\mu q$ choices for c_1 one has $d(f_1, P(k,d)) < d(f_1|_{x_1=c_1}, P(k-1,d)) + \mu$ and thus $d(f, P(k,d)) \leq d(f, f_1) + d(f_1, P(k,d)) \leq d(f, f_1) + d(f_1|_{x_1=c_1}, P(k-1,d)) + \mu$. In both cases it follows

$$\frac{1}{6}d(f, P(k,d)) \leq 1 \cdot \mu + d(f, f_1) + d(f_1|_{x_1=c_1}, P(k-1,d))$$

as required.[5]

[4] In [11] the optimality is needed because the final statement relates $d(f, P(k,d))$ with the sum of the distances $d(f, P_i(k,d))$. Note that we use the letters k, d for arity and degree instead of n, k in [11].

[5] Note that this argument does nowhere rely on whether f_1 is the best approximation from $P_1(k,d)$ to f or not. Similarly below in the induction step.

The argument is the same in the induction step: If (1) is true for an $1 \le i < k$ and the function $f_{i+1}|_{x_1=c_1,\ldots,x_i=c_i}$, which is in $P_1(k-i,d)$ with respect to x_{i+1}, then $\frac{1}{6}d(f,P(k,d)) \le \frac{1}{6} < d(f_{i+1}|_{x_1=c_1,\ldots,x_{i+1}=c_{i+1}}, P(k-i-1,d))$ except for a fraction of at most $\frac{2d-1}{q} < 6\mu$ choices for $c_{i+1} \in F_q$. In this situation the claim is trivially satisfied.

And if (2) holds, then for all but an exception of at most $6\mu q$ choices for c_{i+1} one has

$$d(f_{i+1}|_{x_1=c_1,\ldots,x_i=c_i}, P(k-i,d)) < d(f_{i+1}|_{x_1=c_1,\ldots,x_{i+1}=c_{i+1}}, P(k-i-1,d)) + \mu$$

and thus by the triangle inequality

$$\begin{aligned} d(f_i|_{x_1=c_1,\ldots,x_i=c_i}, P(k-i,d)) &\le d(f_i|_{x_1=c_1,\ldots,x_i=c_i}, f_{i+1}|_{x_1=c_1,\ldots,x_i=c_i}) + \\ &\qquad d(f_{i+1}|_{x_1=c_1,\ldots,x_i=c_i}), P(k-i,d)) \\ &< d(f_i|_{x_1=c_1,\ldots,x_i=c_i}, f_{i+1}|_{x_1=c_1,\ldots,x_i=c_i}) + \\ &\qquad d(f_{i+1}|_{x_1=c_1,\ldots,x_{i+1}=c_{i+1}}, P(k-i-1,d)) + \mu \end{aligned}$$

except for a fraction of at most 6μ choices of $c_{i+1} \in F_q$ (and that for each fixed $(c_1,\ldots,c_i)$ for which the induction hypothesis holds). Together with the induction hypothesis for i this implies

$$\begin{aligned} \tfrac{1}{6}d(f,P(k,d)) \le (i+1)\mu + d(f,f_1) + \sum_{j=1}^{i} d(f_j|_{x_1=c_1,\ldots,x_j=c_j}, f_{j+1}|_{x_1=c_1,\ldots,x_j=c_j}) \\ + d(f_{i+1}|_{x_1=c_1,\ldots,x_{i+1}=c_{i+1}}, P(k-i-1,d)). \end{aligned}$$

It remains to upper bound the number of points in F_q^{i+1} for which this is false. The induction hypothesis is false for at most $6iq^i\mu$ points in F_q^i, which contributes at most $6iq^{i+1}\mu$ violations in F_q^{i+1}. Moreover, each of the at least $q^i(1-6\mu)$ points in F_q^i that satisfy the hypothesis contributes at most $6\mu q$ bad choices of $c_{i+1} \in F_q$. Altogether, this yields at most $6iq^{i+1}\mu + 6\mu q q^i(1-6i\mu) \le 6(i+1)\mu q^{i+1}$ exceptions. The claim is proved.

To finish the proof of the proposition for $i = k$ we take the average over $\underline{c} \in F_q^k$ of all the inequalities in the claim as follows: for satisfying choices $\underline{c} \in F_q^k$ we take the average of the inequality as it is stated in the claim, for the other at most $6k\mu q^k$ choices we take the inequality with $\frac{1}{6}$ added on the right hand side, which results trivially in a correct inequality. The latter for the average contributes an additional term of $k\mu$ and we finally get

$$\frac{1}{6} \cdot d(f,P(k,d)) \ \le \ 2k\mu + d(f,f_1) + \sum_{j=1}^{k-1} d(f_j,f_{j+1}).$$

□

The proposition gives a nearby idea to test closeness of a given $f_0 := f$ to $P(k,d)$. The verifier estimates for suitable f_i the distances $d(f_i,f_{i+1})$ for

$0 \le i \le k-1$ by comparing the values in a randomly chosen point $x^{(i+1)} \in F^k$. In one test round a function f_i has to be evaluated in two random points, one for estimating its distance to f_{i-1} and one for the distance to f_{i+1}. These two points have to be independent. Now if f has a large distance to $P(k,d)$ the proposition will result in a sufficient error probability for the test. Before we describe precisely the test and its analysis note the following two aspects: Later on, we shall explain how information about functions f_i is presented to the verifier as part of a proof certificate π. Basically, this will be done through univariate polynomials resulting canonically from the random points in which an f_i is evaluated by the test. However, since this information should be accessed in segmented form, the implementation needs the machinery of testing trigonometric polynomials. We elaborate on this in the next subsection. Secondly, whereas the above outline naively would require to generate k random points in F_q^k we can reduce the amount of randomness by the well known method of two point sampling, see Lemma 2. We only have to guarantee that the two points in which one function f_i is evaluated are independent, so pairwise independence of the k random points suffices.

Lemma 2. *(Two-point sampling, see [9]) Given random elements $x^{(1)}, x^{(2)} \in F_q^k$ there is a deterministic BSS algorithm running in polynomial time in k that computes a sequence of points $tps(x^{(1)}, x^{(2)}) := (x^{(1)}, \dots, x^{(k)}) \in (F_q^k)^k$ that are pairwise independent random variables being uniformly distributed.*

We are now ready to describe the first test. In the description we assume that the verification algorithm has access to a black box (later: a part of the certificate) for evaluating f_i in the demanded points.

Test: Closeness to $P(k,d)$:

Input: Function value table for an $f : F_q^k \mapsto \mathbb{R}$; black box for evaluating functions $f_i \in P_i(k,d), 1 \le i \le k$ in requested points from F_q^k.

1) Generate two uniformly distributed random points $x^{(1)}, x^{(2)} \in F_q^k$
2) Compute by two-point sampling the sequence
   $tps(x^{(1)}, x^{(2)}) := (x^{(1)}, \dots, x^{(k)}) \in (F_q^k)^k$
3) Evaluate and check the following equalities: $f(x^{(1)}) = f_1(x^{(1)}), f_1(x^{(2)}) = f_2(x^{(2)}), f_2(x^{(3)}) = f_3(x^{(3)}), \dots, f_{k-1}(x^{(k)}) = f_k(x^{(k)})$
4) If one of the equalities is violated reject; otherwise accept. Similarly for several rounds of the test: Reject if at least one equality is violated.

Theorem 3. *Let $f, f_i, 1 \le i \le k$ be as above, and let $\epsilon > 0$ be a constant such that $\mu := \frac{\sqrt{d}}{\sqrt{18q}} \le \frac{\epsilon}{24k}$. This holds, for example, if $q \ge 32k^2 d \frac{1}{\epsilon^2}$. Then the Closeness Test satisfies the following: If $f \in P(k,d)$ and the f_i all equal f, then the test accepts with probability 1. If $d(f, P(k,d)) \ge \epsilon$, then for all choices of $f_1, \dots, f_k$ performing $m \ge \frac{12}{\epsilon} + 1$ rounds of the test is sufficient to reject with probability $> \frac{1}{2}$.*

One round of the test needs $2k \log q$ random bits and inspects one value of f and f_k, and two values of each $f_i, 1 \leq i \leq k-1$. Similarly, in m rounds considering ϵ as a constant the test needs $O(k \log q)$ random bits and inspects $O(1)$ values of each of the functions.

Proof. All statements except the one for the error probability are obvious, so let us assume that $d(f, P(k,d)) \geq \epsilon$. Define $\epsilon_1 := d(f, f_1)$ and $\epsilon_i := d(f_{i-1}, f_i)$ for $2 \leq i \leq k$. Using Proposition 1 and the assumption on μ we have $\frac{\epsilon}{12} \leq \frac{1}{6}\epsilon - 2k\mu \leq \sum\limits_{i=1}^{k} \epsilon_i$. The test in one round does not realize an error with probability at most $\prod\limits_{i=1}^{k}(1-\epsilon_i)$. This holds because the sequence of $x^{(i)}$'s consists of pairwise independent uniformly distributed random points and for one such the probability that $f_{i-1}(x^{(i)}) = f_i(x^{(i)})$ is at most $1 - \epsilon_i$. Using the above and a well known inequality for the Weierstraß product, see [8] for a proof, we get $\prod\limits_{i=1}^{k}(1-\epsilon_i) \leq \frac{1}{1+\sum\limits_{i=1}^{k} \epsilon_i} \leq \frac{1}{1+\epsilon/12}$. Thus, in m rounds of the test an error is not detected with probability at most $\left(\frac{1}{1+\epsilon/12}\right)^m \leq \left(\frac{1}{e}\right)^{\frac{m\epsilon}{12+\epsilon}}$. The latter is $< \frac{1}{2}$ for $m \geq \frac{12}{\epsilon} + 1$, which proves the theorem. □

Remark 1. In the next subsection below, for a point $x \in F_q^k$ a proof certificate is expected to represent the univariate restrictions of f_i into the paraxial directions e_i, i.e., a representation of the univariate polynomial $t \mapsto f_i(x + te_i)$. In this context, the verifier expects an ideal proof certificate to represent the correct restriction of f to that paraxial line through x.

3.2 Segmentation of closeness test

The goal of this subsection is to transform the above verifier performing the closeness test into a segmented form. As in the proof of the original PCP theorem [1], segmented verifiers were crucial in [5] to prove the real number $\mathrm{PCP}_{\mathbb{R}}$ theorem when using an algebraic approach. However, the real number setting causes severe difficulties when working with algebraic polynomials. To circumvent these difficulties, in [5] trigonometric polynomials mapping a vector space F_q^k over a finite field F_q to $\mathbb{R}$ are considered. A main result in [5] is a segmented test for verifying, whether a given function f is close to a trigonometric polynomial of certain max-degree. This test is used below to achieve segmentation of the closeness test as follows: We suppose that all information about the algebraic polynomials $f_i, 1 \leq i \leq k$ which is potentially queried in the closeness test, is coded by particular values of a trigonometric polynomial s of sufficient max-degree. This potential information consists of the univariate paraxial restrictions of an f_i in a point $x \in F_q^k$ having been generated by two-point sampling. The corresponding trigonometric polynomial s is given as additional information to the verifier in form of a table of its values, thereby replacing the black box assumption in the closeness test. To guarantee that this table with high probability represents a trigonometric polynomial the test from [5] is applied first. Segmentation then is obtained as follows: For each pair $(x^{(1)}, x^{(2)}) \in F_q^{2k}$, the necessary information about $tps(x^{(1)}, x^{(2)})$ and the corresponding restrictions can be found when restricting s to a two-dimensional plane. In the ideal case, this restriction is a bivariate trigonometric polynomial b of low max-degree. The certificate expected by the verifier in addition contains the coefficients of these bivariate polynomials as entire segments. The verifier in each round of the closeness test reads this segment, reconstructs b and performs the test. There are several additional technical details such as guaranteeing that b with high probability is the correct restriction of s. This foregoing will result in Theorem 2; it proves that the closeness test can be put into a format ready to apply composition of real number verifiers as developed in [5]. This will suffice to obtain Theorem 1. Note finally that the classical segmentation technique seems not to work directly (at least to the best of our knowledge) in the real number setting because restrictions of trigonometric functions to lines or planes in general do not behave well with respect to the resulting max-degrees of the restrictions. On the other hand, real algebraic polynomials seem not appropriate as coding objects for proving the real number $\mathrm{PCP}_{\mathbb{R}}$ theorem along the lines of [1], see [5] for more detailed explanations of the involved problems. This in the end is the reason why we have to take the detour along trigonometric polynomials for proving a result on algebraic ones. Now towards the details.

Trigonometric polynomials, previous results. We define a special version of real-valued trigonometric polynomials with a finite field as domain and recall the results on testing them. Let $F_q = \{0, \ldots, q-1\}$ be a finite field with q being prime. We consider the elements of F_q as subset of $\mathbb{R}$ when appropriate.

Definition 3. *Let F_q be a finite field as above. For $d \in \mathbb{N}$ a trigonometric polynomial $f : F_q^k \mapsto \mathbb{R}$ of max-degree d is given as $f(x_1, \ldots, x_k) = \sum\limits_t c_t \cdot \exp(\frac{2\pi i}{q} \sum\limits_{j=1}^{k} x_j t_j)$, where the sum is taken over all $t := (t_1, \ldots, t_k) \in \mathbb{Z}^k$ with $|t_1| \leq d, \ldots, |t_k| \leq d$ and $c_t \in \mathbb{C}$ satisfy $c_t = \overline{c_{-t}}$ for all such t.*

Remark 2. Note the following technical detail: if below a verifier is used as BSS algorithm for inputs of varying size, then for different cardinalities q of the finite field F it needs to work with different constants $\cos \frac{2\pi}{q}, \sin \frac{2\pi}{q}$. It is not hard to see that given q one could add two real numbers to the verification proof which in the ideal case represent real and imaginary part of a complex primitive q-th root of unity. The verifier in question deterministically checks in polynomial time whether this is the case and then continues to use these constants for evaluating trigonometric polynomials.

The following theorem is used crucially later on. It deals with the problem to verify whether a function s, given by a table of values, is close to a trigonometric polynomial. The parameters k_s, q_s, d_s used in the statement later on will depend on the parameters k, q, d given with the input f.

Theorem 4 (Testing and correcting trigonometric polynomials; see Theorems 2.4 and 5.2 in [5]). *Let $d_s \in \mathbb{N}$, $h := 10^{15}$, $k_s \geq \frac{3}{2}(2h+1), \tilde{d_s} := 2hk_sd_s$, and let F_{q_s} be a finite field with q_s being a prime number larger than $10^4(2hk_sd_s+1)^3$. Let $s : F_{q_s}^{k_s} \to \mathbb{R}$ be a function given by a table of its values.*

a) There exists a probabilistic verification algorithm in the BSS-model of computation over the reals with the following properties:

- *i) The verifier as input gets the table for s together with a proof string consisting of at most $q_s^{2k_s}$ segments. Each segment has at most $2hk_sd_s+k_s+1$ many real components. The verifier uniformly generates $O(k_s \log q_s)$ random bits and has a running time that is polynomially bounded in the quantity $k_s \log q_s$, i.e., polylogarithmic in the input size $O(q_s^{k_s})$.*
- *ii) For every table representing a trigonometric max-degree d_s polynomial on $F_{q_s}^{k_s}$ there exists a proof such that the verifier accepts with probability 1.*
- *iii) For any $0 < \epsilon < 10^{-19}$ and for every function value table whose distance to a closest max-degree $\tilde{d_s} := 2hk_sd_s$ trigonometric polynomial is at least 2ϵ, the probability that the verifier rejects is at least ϵ, no matter which proof is given.*

b) Suppose the verifier under a) has accepted s and the closest trigonometric polynomial of max-degree $\leq \tilde{d_s}$ is $\tilde{s}$ with a distance at most δ for arbitrary fixed and small enough $\delta > 0$. There exists another segmented verifier working as follows:

- *i) It gets as input the table for s, a point $x \in F_{q_s}^{k_s}$ and an additional proof certificate with at most $O(\sqrt{q_s}^{k_s-1})$ segments of length $2\sqrt{q_s}k_sd_s+1$ each. The verifier uniformly generates $O(k_s \log q_s)$ random bits and has a running time that is polynomially bounded in the quantity $k_s\sqrt{q_s}d_s$.*
- *ii) If $s \equiv \tilde{s}$ is a trigonometric max-degree d_s polynomial, there is a certificate such that the verifier accepts with probability 1.*
- *iii) If $s(x) \neq \tilde{s}(x)$, the verifier rejects every certificate with probability $\geq \frac{3}{4}$.*

Note that even though the theorem does not give a sharp test in the sense that acceptance of s only implies with high probability closeness to a trigonometric polynomial of larger max-degree than d_s, in the subsequent steps below that rely on this test a verifier still expects from a correct prover to receive data as if s is a max-degree d_s polynomial. This refers, for example, to certain bivariate restrictions of s used further on.

Coding univariate algebraic polynomials. We shall now work out how to code the information a verifier needs in view of Theorem 3 when dealing with a given function $f : F_q^k \to \mathbb{R}$. This will be done using, among other things, a trigonometric polynomial s with suitable values for k_s, q_s, and d_s to which, as part of the verification procedure, Theorem 4 has to be applied.

For each pair $(x^{(1)}, x^{(2)}) \in F_q^{2k}$ which the verifier might randomly generate in the closeness test it needs to access information about the algebraic polynomials f_i when restricted to the paraxial direction e_i. Those restrictions have to be evaluated in some of the points constituting $tps(x^{(1)}, x^{(2)})$. We next describe how to encode this information using a trigonometric polynomial s in such a way that each round of the closeness test needs to inspect a single segment of the function value table for s only. The basic idea is to encode the $d+1$ coefficients of a restriction of the form $t \to f_i(x + te_i)$ as certain values of s in such a way, that the information needed for one round of the test is encoded in one segment representing the bivariate restriction of s to a two-dimensional plane. Consider a fixed pair $(x^{(1)}, x^{(2)}) \in F_q^{2k}$ and let $tps(x^{(1)}, x^{(2)}) =: (x^{(1)}, x^{(2)}, \ldots, x^{(k)}) \in F_q^{(k^2)}$. Suppose the closeness test needs to access the k functions $f_j, 1 \leq j \leq k$ with $f_j \in P_j(k, d)$. More precisely, the following univariate restrictions then are of interest; the index in the table below will later on denote the first (of two) values used to parameterize the plane.

index	univariate restriction	index	univariate restriction
1	$t \to f_1(x^{(1)} + te_1)$	$2i-1$	$t \to f_i(x^{(i)} + te_i)$
2	$t \to f_1(x^{(2)} + te_1)$	$2i$	$t \to f_i(x^{(i+1)} + te_i)$
3	$t \to f_2(x^{(2)} + te_2)$	$\vdots$	$\vdots$
4	$t \to f_2(x^{(3)} + te_2)$	$2k-1$	$t \to f_k(x^{(k)} + te_k)$
5	$t \to f_3(x^{(3)} + te_3)$		
$\vdots$	$\vdots$		

Every restriction is a univariate algebraic polynomial of degree d. We encode the coefficients of these polynomials as values of a trigonometric function $s : F_{q_s}^{k_s} \to \mathbb{R}$; here $k_s := 2 + 2k$ and q_s is chosen to be at least as large as q and satisfying the additional requirements of Theorem 4 once d_s has been chosen below. Furthermore, $s(2i-1, m, x^{(1)}, x^{(2)})$ gives the coefficient of monomial t^m of the polynomial $t \to f_i(x^{(i)} + te_i)$, similarly for $s(2i, m, x^{(1)}, x^{(2)})$. Note that s is considered on $F_{q_s}^{k_s}$ instead of $F_q^{k_s}$ in view of the requirements of the test behind Theorem 4, part a) used later on. It follows that for each pair $(x^{(1)}, x^{(2)}) \in F_q^{2k}$ the information used by the closeness test is coded by the values of s on the plane $E(x^{(1)}, x^{(2)}) := \{(j, m, x^{(1)}, x^{(2)}) \mid j, m \in F_{q_s}\} \subset F_{q_s}^{k_s}$ parameterized by the first two coordinates. On $E(x^{(1)}, x^{(2)})$ we have to specify $(2k-1)(d+1)$ many values. The following easy technical result is necessary to bound the size of that part of a certificate which specifies s as well as the size of another part that codes the bivariate trigonometric polynomials obtained as restrictions of s to the planes $E(x^{(1)}, x^{(2)})$.

Lemma 3. *Let $q, k, d \in \mathbb{N}$ be given, $k_s := 2k+2, q_s \geq q$ and let $f_i \in P_i(k, d), 1 \leq i \leq k$.*

a) There exists a trigonometric polynomial $s : F_{q_s}^{k_s} \to \mathbb{R}$ of max-degree $d_s := O(q)$ which codes the coefficients of the f_i for all pairs $(x^{(1)}, x^{(2)})$ as described above.

b) For all pairs $(x^{(1)}, x^{(2)}) \in F_q^{2k}$*, the bivariate trigonometric polynomial defined on* $E(x^{(1)}, x^{(2)})$ *by* $b_{(x^{(1)},x^{(2)})}(j,m) := s(j,m,x^{(1)},x^{(2)})$ *has max-degree* $O(q)$*.*

c) Let $q', k', d' \in \mathbb{N}$ *and let* $s' : F_{q'}^{k'} \to \mathbb{R}$ *be a trigonometric polynomial of max-degree* $d' \in \mathbb{N}$ *not identically* 0*. Then the number of zeros of* s' *is at most* $2d'(k'+1)(q')^{k'-1}$*.*

Proof. We just briefly sketch the elementary proofs. The given bounds might not be sharp, but they suffice for later purposes.

a) This can be shown using trigonometric interpolation. Note that the intended coding only prescribes values in points $(j, m, x^{(1)}, x^{(2)})$, where $1 \le j \le 2k-1, 0 \le m \le d$ and $x^{(1)}, x^{(2)} \in F_q^k$. Thus, all components range between 0 and $\max\{2k-1, d, q-1\}$. The previous conditions on q (see Proposition 1 and Theorem 3) guarantee that $q-1$ is the maximal value. In the univariate case q prescribed values can be interpolated by a trigonometric polynomial of degree $\lceil \frac{q-1}{2} \rceil$. Now, a standard tensor-product construction gives a suitable trigonometric Lagrange polynomial in the multivariate case of max-degree $\lceil \frac{q-1}{2} \rceil$ as well, see for example [14].

b) follows immediately from the fact that the plane is parameterised by the two first unit vectors $(1,0,\ldots)^T$ and $(0,1,0,\ldots)^T \in F_{q_s}^{k_s}$. The definition of the degree of a trigonometric polynomial shows that the max-degree resulting from a restriction to a plane depends on the values of the components of the respective directional vectors. Since here those values only are 0 or 1, the max-degree of the bivariate restrictions is no larger than that of s.

c) This is an easy induction on k', noticing that in the univariate case $2d'+1$ zeros imply that a degree d' polynomial is identically 0. The induction step can be performed as done, for example, in [3], pp. 222f in the case of algebraic polynomials. □

Revised Closeness test. We now describe and analyze an extended form of the closeness test from Section 3.1. This will lead to the proof of Theorem 2. Before we do so let us summarize the conditions on the involved parameters resulting from our considerations so far: $q, k, d \in \mathbb{N}$ are given with the function f to be tested, $\epsilon > 0$ is the fixed reliability parameter. Here, $q \ge \max\{18kd^3, 32k^2d/\epsilon\}$. Then, $k_s := 2k+2, d_s = O(q)$ and $q_s = \Omega(k_s^3 d_s^3)$, and thus $q_s = \Omega(k^3q^3); h$ is a (huge) constant.

<u>**Closeness Test Revised:**</u> Let $q, q_s, k, k_s, d, d_s, h$ be as above, $\epsilon > 0$

Input: Function value table for an $f : F_q^k \to \mathbb{R}$; a proof certificate π of length $O((kq)^{O(k)})$. It consists of four parts $\pi_1, \ldots, \pi_4$. Here, π_1 is a function value table for an $s : F_{q_s}^{k_s} \to \mathbb{R}, \pi_2$ is a certificate necessary to perform the tests on s behind Theorem 4, part a), π_3 represents for every pair $(x^{(1)}, x^{(2)}) \in F_q^{2k}$ a bivariate trigonometric polynomial $b_{(x^{(1)},x^{(2)})} : F_{q_s}^2 \to \mathbb{R}$ of max-degree q, given by its coefficients, and π_4 is the certificate used for the correctness test on s underlying Theorem 4, part b).

Goal: The test should be ϵ-reliable with respect to the question whether $f \in P(k,d)$.

1. Perform the test behind Theorem 4, part a) on s and verify, whether s is sufficiently close to a trigonometric polynomial $\tilde{s} : F_{q_s}^{k_s} \to \mathbb{R}$ of max-degree $\tilde{d}_s := 2hk_sq$ using part π_2 of the certificate. If the test fails reject.

Perform $O(1/\epsilon)$ many rounds of the following steps 2-8:

2. Randomly generate two points $x^{(1)}, x^{(2)} \in F_q^k$.

3. Compute deterministically $(x^{(1)}, x^{(2)}, \ldots, x^{(k)}) := tps(x^{(1)}, x^{(2)}) \in (F_q^k)^k$.

4. Read the coefficients of $b_{(x^{(1)},x^{(2)})}$ from part π_3 of the certificate.

5. Generate random $j, m \in F_{q_s}$, verify $s(j,m,x^{(1)},x^{(2)}) = \tilde{s}(j,m,x^{(1)},x^{(2)})$ using the correctness test for s from Theorem 4, part b).

6. Check whether $s(j,m,x^{(1)},x^{(2)}) = b_{(x^{(1)},x^{(2)})}(j,m)$; reject if not.

7. Check consistency: if a single f_i in one or several rounds has to be evaluated in two points lying on the same paraxial line check that the resulting restrictions are the same.

8. Check the equalities from the closeness test. Here, $f(x^{(1)})$ is read from the given table for f, whereas the values of an f_i in $x^{(i)}$ or $x^{(i+1)}$, respectively, are computed deterministically: Compute all coefficients from $b_{(x^{(1)},x^{(2)})}$, evaluate it for the relevant values of j, m and then compute the value of the coded univariate algebraic polynomial. Reject, if at least one of the equations does not hold.

If at least one round leads to a reject, the verifier rejects, otherwise it accepts.

A verifier performing this revised closeness test fulfills the statement of Theorem 2. More precisely, we get

Theorem 2 (reformulated). *Let $f : F_q^k \to \mathbb{R}$. For $\epsilon > 0$ let a verifier V perform $O(1/\epsilon)$ rounds of the above revised closeness test. Then V is ϵ-reliable concerning the question whether f is an algebraic polynomial of max-degree d. The running time of V is polynomial in kq, it generates $O(k \log q)$ many random bits, uses a certificate of size $O((kq)^{O(k)})$, and reads $O(1)$ segments of maximal length $O((qk)^{O(1)})$.*

Proof. Let us first inspect the resources needed by V. The lengths of certificate π and of segments can be estimated as follows: The table of values for f has size q^k. The test behind Theorem 4, part a) requires the table of values for s, which has size $O(q_s^{k_s})$. Lemma 3 shows that it suffices to require that the trigonometric polynomial represented by the table has max-degree at most q; together with the conditions $q_s \geq 10^4(2hk_sq+1)^3$ and $k_s = 2+2k$ (and $k_s \geq \frac{3}{2}(2h+1)$) it follows that the size of the table for s is in $O((kq)^{3k})$. Performing the test for closeness of s to a trigonometric polynomial $\tilde{s}$ uses a certificate π_2 consisting of $q_s^{2k_s} = O((kq)^{3k})$ many segments; each segment has length $O(k_sq + k_s) = O(kq)$. Next, for all q^{2k} many pairs $(x^{(1)}, x^{(2)}) \in F_q^{2k}$ part π_3 of the certificate contains the coefficients of the bivariate trigonometric polynomials $b_{(x^{(1)},x^{(2)})}$. By Lemma 3 their max-degrees are bounded by $O(q)$, so $O(q^2)$ coefficients are sufficient. Thus, π_3 has total length $O(q^{2k+2})$, split into q^{2k} segments of size $O(q^2)$. Finally, in each round the test in Step 5 performs a correction relying on Theorem 4, part b). It requires a certificate π_4 of length $O(\sqrt{q_s}^{k_s} k_s q) = O((kq)^{2k})$, split into segments of length $2\sqrt{q_s}k_s q + 1 = O((kq)^{2.5})$. Altogether, the certificate π has size $O((kq)^{O(k)})$ and the segments have maximal size $O((kq)^{2.5})$. Given the way the restrictions of the f_i's are coded together with Theorem 4 the verifier reads $O(1)$ many segments.

Next, we determine the number of random bits: Step 1 of the test needs $O(k_s \log q_s) = O(k \log q)$ random bits; Step 2 requires as well $O(k \log q)$ random bits in each round. Step 5 generates in each round two elements from F_{q_s} using $O(\log q_s) = O(\log(kq))$ random bits. The subsequent correctness test uses $O(k_s \log q_s) = O(k \log(kq))$ random bits. In Section 3.1 we assumed $q \geq 18kd^3$, so the number of random bits can be bounded by $O(k \log q)$.

The running time for Step 1 is $poly(k_s q_s) = poly(k \log q)$, again using that $q_s = \Theta(k^3 q^3)$ and $q \geq 18kd^3$, so $\log q_s = O(\log q)$. The computation of the sequence $tps(x^{(1)}, x^{(2)})$ runs in polynomial time in k. Each $b_{(x^{(1)},x^{(2)})}$ has $O(q^2)$ many coefficients, so this is also the time to read all of them. The correctness test for s according to Theorem 4, part b) can be performed in $poly(k_s\sqrt{q_s}d) = poly(kq)$ steps. For Step 6, $b_{(x^{(1)},x^{(2)})}$ has to be evaluated in a (j, m) which needs time $O(q^2)$. Checking validity of the k equations constituting the closeness test then can be done in time $poly(kd)$. The same holds for recording the points in which the restriction of an f_i is evaluated and for determining, whether different such points lie on the same paraxial line. Altogether, verifier V runs in time $poly(kq)$.

Finally, we analyze the failure probability. Clearly, if f is a max-degree d algebraic polynomial and if the information provided by certificate π is correct, then V accepts with probability 1. Suppose then that f is not ϵ-close to an algebraic max-degree d polynomial. As usual in this area, the arguments below suffice to conclude that an independent repetition of some of the tests performed constantly many times yields the required probability bounds. The error sources in the test are the following: either s is not sufficiently close to a trigonometric polynomial of suitable max-degree; or s is close but for the values in which s has to be evaluated the result is not that of the closest trigonometric polynomial $\tilde{s}$; or the restriction of this polynomial to one of the planes E occurring in the revised closeness test does not equal the bivariate polynomial b; or the univariate algebraic polynomials coded by b do not cause f to pass the original closeness test. We now argue that the verifier detects if one of these cases holds with arbitrarily high (constant) probability. Step 1 of the test rejects at least with a positive constant probability $\delta > 0$, if s is not 2δ-close to a trigonometric polynomial $\tilde{s}$ of a corresponding max-degree; thus, $O(1/\delta)$ repetitions suffice to raise this probability to an arbitrary constant close to 1. Next, the correctness test behind Step 5 detects a difference in the values of s and $\tilde{s}$ in the chosen point with probability at least $\frac{3}{4}$. Step 6 verifies whether the restriction s' of $\tilde{s}$ to the plane $E_{(x^{(1)},x^{(2)})}$ equals $b_{(x^{(1)},x^{(2)})}$. Here, b has max-degree $O(q)$ and s' has arity $k' := 2$ and max-degree $d' := 2hk_s q$. Note that even though the low-degree test for s gives closeness to a polynomial of higher max-degree $\tilde{s}$, the verifier expects the degree to be the one of a correct s. Therefore, b is taken to have max-degree $O(q)$ only. The potentially larger degree of $\tilde{s}$ enters the error analysis only with respect to the domain $F_{q_s}^2$ from which the test randomly chooses the point (j,m) in which b and s' are evaluated. Using Lemma 3 applied to $s'-b$ (with k',d' as above and $q' := q_s$) a difference between s' and b is realized by the verifier with probability at least $1-\frac{12hk_sqq_s}{q_s^2}$. Since $q_s \geq 10^4(2hk_sq+1)^3$ this probability is $\geq 1-10^{-3}$. If all tests so far have passed without rejection, then with arbitrarily high constant probability the data encoded by the different b's corresponds to suitable algebraic univariate polynomials of degree d. Now, according to Theorem 3, Step 8 rejects with probability $>\frac{1}{2}$ if f is not ϵ-close to an algebraic polynomial. □

3.3 Finishing the proof

The final step necessary for improving the statement of Theorem 2 to that of Theorem 1 relies on the well known technique of (segmented) verifier composition and the way it has been used in the real number framework in [5].

Proof. (of Theorem 1). We apply the well known technique of verifier composition developed in [2] and used also in the BSS framework in [5]. Therefore, we only briefly outline how to apply the technique in the present situation. Consider the verifier V of Theorem 2. Whenever it reads a segment of length $O((kq)^{O(1)})$ it subsequently computes deterministically from the data read in polynomial time in the size of the segment the corresponding answer to one of the questions occuring in the revised closeness test. This question can be expressed as $\mathrm{P}_{\mathbb{R}}$-question by formalizing the verifier's computation on the information read in the currently queried segment. For example, this can be done by describing the computation via an instance of the $\mathrm{NP}_{\mathbb{R}}$-complete problem of deciding solvability of a system of quadratic polynomial equations over the real numbers; then, the segment read provides a solution assignment to (part of) the variables of that system; see [7] for this basic construction behind the corresponding $\mathrm{NP}_{\mathbb{R}}$-completeness proof. Reformulating things that way this part of the verification can be replaced by what is called an inner verifier: Instead of reading the entire segment (this would not reduce the number of proof components required to be seen) the inner verifier performs a verification for the resulting instance of the above mentioned $\mathrm{NP}_{\mathbb{R}}$-problem. The advantage is that the input size is reduced, and so is the number of positions of a new corresponding certificate read by the inner verifier. Composition of verifiers means that a new composed verifier uses the old (outer) verifier to determine the segments that should be asked, but replaces the deterministic polynomial time procedure that uses the entire segment to compute the answer to the corresponding query by another inner verification procedure. In order to make this ongoing working the composed verifier in addition has to perform certain consistency checks. These checks guarantee that a prover gives consistent answers to the inner verifier if the outer verifier asks in several queries segments that contain overlapping data. This is only a sketchy outlook. In the above situation, the outer verifier behind Theorem 2 has to be composed several times with inner verifiers. More precisely, one can compose it twice with the verifier designed in [5] that codes satisfying assignments of polynomial systems using low max-degree trigonometric polynomials and after that compose the resulting intermediate verifier with the long transparent verifier for $\mathrm{NP}_{\mathbb{R}}$, see also [5]. Since the way how those verifiers work is described in full detail in the cited papers, this should suffice as short outline. That way, finally a verifier is obtained that has $O(k \log q)$ randomness, query complexity $O(1)$ and is ϵ-reliable, i.e., it has the properties stated in Theorem 1. □

4 Conclusions

In [11] an ϵ-reliable property test for algebraic k-variate polynomials of given max-degree defined on a finite subdomain of suitable size q of the reals was designed. The test uses $O(k \log q)$ random bits and queries $O(k)$ positions in a table for f (considering ϵ as a constant). In this paper we constructed a real number PCP of proximity for this problem using as well $O(k \log q)$ random bits, but only $O(1)$ oracle calls to both the table of f and an additional proof certificate. Here are some subsequent questions, some of which are inspired by the helpful comments of the reviewers: The parameters used in our algorithm likely are far from being optimal. This holds both for the necessary domain size on which f is defined, for the size of the additional certificate, for the number of queries, and for the running time. Can we significantly reduce the constants hidden behind the respective O-statements? Next, it still seems puzzling that the algorithm for algebraic polynomials relies on the use of trigonometric polynomials as coding objects. This clearly makes the approach complicated and technically involved. Are there easier verification algorithms not needing the detour along trigonometric polynomials? In the classical PCP literature, the important initial role played by segmented verifiers has been subsumed by that of so-called robust verifiers, see [6] and also [13]. Since the main technical problem to overcome is segmentation, it is of course interesting to ask whether robust verifiers in the real-number framework would lead to easier proofs as well, including a possibility to avoid trigonometric polynomials. Another impact of classical robust verifiers is to obtain property testers instead of PCPs of proximity. Would this be possible both for algebraic and trigonometric polynomials? We do not have an educated guess at the moment.[6] Next, what about studying algebraic polynomials with a more 'continuous' closeness measure like the L_1-norm, and then allowing small differences between given values and those of a best-approximating polynomial? Finally, there are of course numerous problems in the real number framework where one could ask for the existence of either PCPs of proximity or property testers, for example for algebraic polynomials (as said above), but also for many other real-number problems. Together with the previous question this is also related to the not yet studied question of software testing in the BSS model: Here one could ask for checking in a randomized way whether a given program approximately computes a predetermined function or a function from a given class with not too many errors.

[6] Thanks to an anonymous referee for very helpful comments in this respect.

Acknowledgement. Thanks are due to M. Baartse for helpful discussions in the initial phase leading to this work, and to the anonymous referees for their extremely careful reading and the many informative hints to further literature and interesting future questions.

References

1. S. Arora, C. Lund, R. Motwani, M. Sudan, M. Szegedy: Proof verification and hardness of approximation problems. Journal of the ACM 45 (3), 501–555, 1998.
2. S. Arora, S. Safra: Probabilistic checking proofs: A new characterization of NP. Journal of the ACM 45 (1), 70–122, 1998.
3. G. Ausiello, P. Crescenzi, G. Gambosi, V. Kann, A. Marchetti-Spaccamela, M. Protasi: Complexity and Approximation: Combinatorial Optimization Problems and Their Approximability Properties. Springer, 1999.
4. M. Baartse, K. Meer: The PCP theorem for NP over the reals. Foundations of Computational Mathematics, Vol. 15(3), Springer, 651–680, 2015.
5. M. Baartse, K. Meer: An algebraic proof of the real number PCP theorem. Journal of Complexity, Vol. 40, 34–77, 2017.
6. E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, and S. P. Vadhan: Robust PCPs of Proximity, Shorter PCPs, and Applications to Coding. SIAM J. Comput., vol. 36, no. 4, pp. 889–974, 2006.
7. L. Blum, F. Cucker, M. Shub, S. Smale: Complexity and Real Computation. Springer, 1998.
8. T.J.I.A. Bromwich: An introduction to the theory of infinite series. Macmillan, London, 1955.
9. B. Chor, O. Goldreich: On the power of two-point based sampling. Journal of Complexity, Vol. 5, 96–106,1989.
10. I. Dinur: The PCP theorem by gap amplification. J. of the ACM Vol. 54 (3), 2007.
11. K. Friedl, Z. Hátsági, A. Shen: Low-degree tests. Proc. SODA, 57–64, 1994.
12. O. Goldreich: Introduction into Property Testing. Cambridge Univ. Press, 2017.
13. P. Harsha: Robust PCPs of Proximity and Shorter PCPs. Massachusetts Institute of Technology, Cambridge, MA, USA, 2004. http://www.tcs.tifr.res.in/~prahladh/papers/thesis/
14. G. Mastroianni, G. Milovanic: Interpolation processes. Springer Monographs in Mathematics, 2008.
15. K. Meer: Almost transparent short proofs for $NP_{\mathbb{R}}$. Extended abstract in: Proc. 18th Symposium FCT 2011, Oslo, LNCS 6914, 41–52, 2011.
16. J.L. Montaña and L.M. Pardo (editors): Recent Advances in Real Complexity and Computation. AMS Contemporary Mathematics Vol. 604, 2013.