Approximate Testing with Relative Error

Marcos Kiwi* Frédéric Magniez† Miklos Santha ‡

Abstract

We formalize the notion and initiate the investigation of approximate testing for arbitrary forms of the error term. Until now only the case of absolute error had been addressed ignoring the fact that often only the most significant figures of a numerical calculation are valid. This work considers approximation errors whose magnitude grows with the size of the input to the program. We demonstrate the viability of this new concept by addressing the basic and benchmark problem of self–testing for the class of linear and polynomial functions. We obtain stronger versions of results of Ergün, Ravi Kumar, and Rubinfeld [EKR96] by exploiting elegant techniques from Hyers–Ulam stability theory.

1 Introduction

The following is a quote from Knuth [Knu98, Ch. 4, § 2.2]: *Floating point computation is by nature inexact, and programmers can easily misuse it so that the computed answers consist almost entirely of "noise." One of the principal problems of numerical analysis is to determine how accurate the results of certain numerical methods will be. There's a credibility gap: we don't know how much of the computer's answers to believe.... Many serious mathematicians have attempted to analyze a sequence of floating point operations rigorously, but have found the task so formidable that they have tried to be content with plausibility arguments instead.* Then, Knuth goes on to say: *A rough (but reasonably useful) way to express the behavior of floating point arithmetic can be based on the concept of "significant figures" or relative error.*

If the exact real number x is represented inside the computer, an approximation $\widehat{x} = x(1+\theta)$ is often used. The quantity $\theta = (\widehat{x} - x)/x$ is called the relative error of approximation.

Consider now the task of writing a program P purported to compute a real valued function f. One of the difficulties of such an endeavor is that once P is implemented it is difficult to verify its correctness, i.e., that $P(x) = f(x)$ for all valid inputs x. Moreover, due to the inexact nature of digital computations, it might be impossible to compute f exactly. A more realistic requirement is that P compute f in such a way that $|P(x) - f(x)| \leq \beta(x)$ on every valid input x, where $\beta(x)$ is some appropriate error function.

The inaccuracies of many computational processes are made worst by a crucial and pervasive issue that arises in the programming practice; it is not easy to get a program right. To address the software correctness problem the notion of program checking [Blu88, BK89], self–testing programs [BLR90], and self–correcting programs [BLR90, Lip91] was pioneered by Blum et al. during the late 80's and early 90's. A *program checker* verifies whether the program gives the correct answer on a particular input, a *self–testing program* for f verifies whether the program P is correct on most inputs, and a *self–correcting program* for f takes a program P that is correct on most inputs and uses it to compute f correctly on every input with high probability. Checkers and self–testers/correctors, testers for short, may call the program as a black box but are required to do something different and simpler than to actually compute the function f in a sense that is formalized in [BK89].

Initially, it was assumed in the testing literature, that programs performed exact computations and that the space of valid inputs was closed under the stan-

*Dept. de Ing. Matemática, U. de Chile, Santiago 170–3, Chile, (mkiwi@dim.uchile.cl). Gratefully acknowledges the support of Conicyt, via Fondecyt No. 1981182 and a CNRS–Conicyt'98 Project.

†Université Paris–Sud, 91405 Orsay, France. (magniez@lri.fr). Partially supported by a CNRS–Conicyt'98 Project, Fondap'98 in Applied Mathematics, and ESPRIT Working Group RAND2, No. 21726.

‡CNRS, URA 410, Université Paris–Sud, 91405 Orsay, France. (santha@lri.fr). Partially supported by a CNRS–Conicyt'98 Project and ESPRIT Working Group RAND2, No. 21726.

dard arithmetic operations, i.e., was an algebraically closed domain. Early on, it was recognized that these assumptions were too simplistic to capture the real nature of many computations. In particular the computation of real valued functions and of functions defined over rational domains (finite subsets of fixed point arithmetic of the form $\{i/s : |i| \leq n, i \in \mathbb{Z}\}$ for some $n, s > 0$). This led to the development of approximate testers [GLR$^+$91, ABC$^+$93], testers over finite rational domains [Lip91], and testers which consider both aspects simultaneously [EKR96].

A key issue that arises throughout the testing literature is to verify whether a program belongs to a particular function class, i.e., the *property testing* problem. Once this problem has been resolved, testers for the members of the function class are often easier to derive. This justifies why we henceforth focus on this problem. But, we concentrate on an aspect of the problem that has been ignored in the literature; the magnitude of the inaccuracies in many numerical computations depends on the size of the values involved in the calculations. This leads us to the following:

Problem: For a program P purportedly computing a function in the class of real valued functions $\mathcal{F}$, and given error functions β and β', find a simple and efficient self–tester for P which, with high probability,

- Outputs PASS if $\Pr_{x \in D}[|P(x) - f(x)| > \beta(x)]$ is at most δ for some function $f \in \mathcal{F}$.
- Outputs FAIL if $\Pr_{x \in D'}[|P(x) - f(x)| > \beta'(x)]$ is at least δ' for all functions $f \in \mathcal{F}$.

Exact self–testing is an instance of the above problem where β and β' are identically 0. Approximate self–testing corresponds to the *absolute error* case of the above problem, i.e., the case where the error functions are constants. Testers have been built, in both of the latter scenarios, for different function classes and domains. But, they suffer from the following problem: when the error term is a small constant they fail good programs, e.g., those in which the error in the computation of $P(x)$ grows with the size of x. If on the contrary, the error term is a large constant, they might pass programs that make incorrectly large errors in the computation of $P(x)$ for small values of x. This work addresses the more realistic case where the acceptable error terms are not necessarily constant functions. We refer to this case as that of *relative error* since errors are measured relative to some pre-specified function of the input to the program being tested. To derive our results we will require the error terms to satisfy certain conditions. But, before we describe our specific contributions let us discuss the context where they arise.

Previous Work: Here we will only discuss the literature concerned with testing over rational domains and/or approximate testing. For a thorough exposition of the motivations, applications, and work on exact testing, see the survey of Blum and Wasserman [BW94] and the thesis of Rubinfeld [Rub90].

Self–testers/correctors for programs whose input values are from finite rational domains were first considered by Lipton [Lip91] and further developed by Rubinfeld and Sudan [RS92]. In [Lip91] a self–corrector for multivariate polynomials over a finite rational domain is given. In the same scenario [RS92] describes more efficient versions of this result as well as a self-tester for univariate polynomials.

The study of testing in the context of inexact computations was started by Gemmell et al. [GLR$^+$91] who provided approximate self–testers/correctors for linear functions, logarithmic functions, and floating point exponentiation. Nevertheless, their work was limited to the context of algebraically closed domains. Program checking in the approximate setting was first considered by Ar et al. [ABC$^+$93] who provided, among others, approximate checkers for some trigonometric functions and matrix operations.

The works discussed above left many open questions, several of which were settled by Ergün, Ravi Kumar, and Rubinfeld [EKR96] who addressed the testing problem in the approximate context and over finite rational domains. Among other things, they showed how to perform approximate testing for linear functions, polynomials, and for functions satisfying addition theorems. One of their significant contributions was to recognize the importance of stability theory in the context of testing. It is beyond the possibilities of this brief discussion to give a fair account of the achievements of this theory (the interested reader is referred to the surveys of Forti [For95] and Hyers and Rassias [HR92]). But, a description of its goals is due. In order to do so, and also for concreteness sake, it will be convenient to recall a simple albeit fundamental testing problem that has played a key role in the development of the theory of testers; the Blum–Luby–Rubinfeld linearity test [BLR90]. Given a program P purportedly computing a homomorphism from one finite group G into another one, this test picks $u, v \in G$ at random and verifies whether $P(u) + P(v) = P(u+v)$. The analysis of this test described in [BLR90] is due to Coppersmith [Cop89] and goes as follows; define a function g whose value at u is the Majority of the multi-set $\{P(u+v) - P(v) : v \in G\}$ (here, the Majority of a multi-set is the most commonly occurring element in the multi-set, where ties are broken arbitrarily). Then, show that if the probability of the test failing is sufficiently small, three things happen. First, an overwhelming majority of the values $\{P(u+v) - P(v) : v \in G\}$ agree with $g(u)$, second, g is linear, and last, g is close to P. The analyzes of approximate tests with ab-

solute error over algebraically non-closed domains follow a similar approach than the one described above. But, there are two significant differences. First, instead of taking Majority the Median is used [EKR96]. Second, both the closeness of g to P and the linearity of g can be ascertained only approximately. Therefore, to conclude that P is close to a linear function a result showing that g is close to a linear function is needed. In general, this is referred to as *proving stability*. The setting of the stage where a stability type result can be applied is referred to as *proving robustness*. The latter term was coined and formally defined in [RS96] and studied in [Rub94].

Our Contributions: In Sect. 2 we address several instances of the so called *local stability problem*. Specifically, we consider functional equations, e.g., $f(x+y) = f(x)+f(y)$, and provide conditions under which a function that approximately satisfies the functional equation (over an algebraically non-closed domain) is well approximated by a function that satisfies it exactly (on some subset of the domain). We restrict our discussion to real valued functions whose domain is $D_n \stackrel{\text{def}}{=} \{i \in \mathbb{Z} : |i| \leq n\}$. But, our results can be directly extended to finite rational domains as those considered in [Lip91, RS92, EKR96].

In the literature, the local stability problem has been addressed only in the absolute error case, i.e., when the approximation error is constant. On the contrary, we consider more general forms of the approximation error. In particular, we allow error terms that grow with the size of the input on which a function is evaluated. As discussed earlier, we believe that this is a more realistic and interesting scenario. Moreover, our results generalize those previously obtained for the absolute error case. Nevertheless, our arguments are simpler than those previously used in the related literature. We illustrate them in Sect. 2.1. For the sake of precision, below we give an example of the kind of results we can derive. First, we need to introduce the notion of *valid error terms of degree* $p \in \mathbb{R}$, i.e., functions like $\beta(\cdot,\cdot)$ which are nonnegative, nondecreasing and even in each of its coordinates, and such that $\beta(2s,2t) \leq 2^p\beta(s,t)$ for all integers s,t. Examples of this type of function are $\beta(s,t) = |s|^p + |t|^p$, and $\beta(s,t) = \max\{a, |s|^p, |t|^p\}$ for some nonnegative real number a.

Theorem 1 *Let $\beta(\cdot,\cdot)$ be a valid error term of degree $p \in [0,1)$. Let $g\colon D_{2n} \to \mathbb{R}$ be such that for all $x, y \in D_n$,*

$$|g(x+y) - g(x) - g(y)| \quad \leq \quad \beta(x,y)\,. \tag{1}$$

Let $q_0 = r_0 = 0$ and for $x \in \mathbb{Z} \setminus \{0\}$ let $q_x \in \mathbb{Z}$ and $r_x \in D_n$ be the unique numbers such that $x = q_x n + r_x$ and $|q_x n| < |x|$. Then, for $C_p = (1+2^p)/(2-2^p)$ and $h\colon \mathbb{Z} \to \mathbb{R}$ where $h(x) = g(r_x) + q_x g(n)$, the function $T\colon \mathbb{Z} \to \mathbb{R}$ defined by $T(x) = \lim_{m\to\infty} h(2^m x)/2^m$ is a well defined linear mapping such that

$$\forall x \in \mathbb{Z}\,, \qquad |h(x) - T(x)| \quad \leq \quad C_p\beta(x,x)\,.$$

Furthermore, if $x \in D_n$, the previous inequality also holds when h is replaced by g.

Analogous results for multi-linear functions are derived in Sect. 2.2, and for univariate polynomials in Sect. 2.3.

In Sect. 3 we undertake the task of proving robustness in the scenario where non-constant error terms are allowed. These proofs of robustness follow those of [EKR96] albeit with one major technical difference; the Median is taken over sets of non-fixed size. In Sect. 3.1 we give the first of our robustness results. It concerns linear functions, and from it we prove the following:

Theorem 2 *Let $\delta \in [0,1]$ and $\beta(\cdot,\cdot)$ be a valid error term of degree $p \in [0,1)$. If $P\colon D_{8n} \to \mathbb{R}$ is such that*

$$\Pr_{x,y\in D_{4n}}[|P(x+y) - P(x) - P(y)| > \beta(x,y)] \quad \leq \quad \delta/384,$$

then there exists a linear function $T\colon \mathbb{Z} \to \mathbb{R}$ such that for $C_p = (1+2^p)/(2-2^p)$,

$$\Pr_{x\in D_n}[|P(x) - T(x)| > 17C_p\beta(x,x)] \quad \leq \quad 7\sqrt{\delta}/6\,.$$

(If $p = 0$, then $\beta(\cdot,\cdot)$ is a constant function and the latter inequality holds with $\delta/6$ in its RHS.)

In Sect. 3.2 we derive a similar result for univariate polynomials. (An example showing that without additional conditions on $\beta(\cdot,\cdot)$ the $\sqrt{\delta}$ in the conclusion of Theorem 2 is tight, up to constant factors, is given in Appendix A.)

In Sect. 4, we extend the approximate self–testers definition of [EKR96, GLR$^+$91] in order to capture the idea of approximate self–testing with relative error. We then show how the results of Sect. 2 and Sect. 3 yield approximate self–testers for more general forms of the error term than previously known. This is achieved through standard arguments when self–testing is done in the exact or in the absolute error case. In the relative error case, it is not as simple. Indeed, the issue is somewhat complicated by the fact that the error function might be too costly to compute. (It is interesting to note that the testing literature has so far implicitly assumed that the error term is efficiently computable.) In Sect. 4 we discuss this issue, and show that a good approximation of the error function suffices for self–testing. We conclude, in Sect. 5, by stating an open problem.

Due to space limitations several proofs are omitted. Moreover, we restrict our discussion to approximate self–testing with relative error and will not address issues concerning approximate program checkers and self–correctors in a similar setting.

Relationship to other work: Although initially intended to address the problem of program correctness, the theory of self–testers/correctors had unanticipated consequences. Indeed, all known constructions of probabilistically checkable proofs [ALM+92] use in some way or another ideas and results concerning testers. Moreover, it has been shown that it has implications in learning theory and approximation theory [GGR96], local stability theory [EKR96], and coding theory [RS96].

2 Stability with Relative Error

2.1 Approximate Linearity

In this section we prove Theorem 1 and illustrate an elegant technique for proving stability results in the context of approximate testing over finite rational domains. We bring together and strengthen two ideas developed in stability theory. Our argument first relates a function g satisfying (1) to a function h satisfying the same type of inequality but for all $x, y \in \mathbb{Z}$. Moreover, we will carefully choose h so that $h(x) = g(x)$ for all $x \in D_n$. In other words, h will be an *extension* of g restricted to D_n. Thus, in order to establish that the function g can be well approximated by a linear function it will suffice to show that h can be well approximated by a linear function T over all of $\mathbb{Z}$. This task is greatly simplified by the fact that the domain of h is a group. In fact, an elegant sequence of papers, starting with the 1941 paper of Hyers [Hye41], addresses such a problem for functions whose domain have a semi–group structure (a semi–group structure is a group where elements do not necessarily have inverses). Hyers work was motivated by a question posed by Ulam who asked whether a function f that satisfies the functional equation $f(x+y) = f(x) + f(y)$ only approximately could always be approximated by a linear function. Hyers showed that if the equality was satisfied within a constant error term then f could be approximated, also within a constant error term, by a linear function. Many other positive answers to Ulam's question and variations of it are now known (see [HR92, For95] for a discussion of such results), e.g.,

Lemma 1 [Rassias [Ras78]] *Let E_1 be a normed semi–group, let E_2 be a Banach space, and let $h\colon E_1 \to E_2$ be a mapping for which there exists $\theta > 0$ and $p \in [0, 1)$ such that for all $x, y \in E_1$,*

$$\|h(x+y) - h(x) - h(y)\| \quad \leq \quad \theta(\|x\|^p + \|y\|^p)\,.$$

Then, the function $T\colon E_1 \to E_2$ defined by $T(x) = \lim_{m\to\infty} h(2^m x)/2^m$ is a well defined linear mapping satisfying

$$\forall x \in E_1\,, \qquad \|h(x) - T(x)\| \quad \leq \quad (2/2{-}2^p)\theta\|x\|^p\,.$$

The main reason why we can not directly apply Rassias's Lemma to a function g such that $|g(x+y) - g(x) - g(y)| \leq \theta(|x|^p + |y|^p)$ for all $x, y \in D_n$, is that D_n is not a semi–group. It is in order to address this issue and to be able to exploit results like the one of Rassias that we extend g into a function defined over all of $\mathbb{Z}$ (a group!) in such a way that the extension will satisfy the hypothesis of Lemma 1. The following result, based on an argument due to Skof [Sko83], illustrates this approach:

Lemma 2 [Extension Lemma] *Let $p \in [0, 1]$ and let $g\colon D_{2n} \to \mathbb{R}$ be such that for all $x, y \in D_n$,*

$$|g(x+y) - g(x) - g(y)| \quad \leq \quad \theta\,(|x|^p + |y|^p)\,.$$

Let $q_0 = r_0 = 0$ and for $x \in \mathbb{Z} \setminus \{0\}$ let $q_x \in \mathbb{Z}$ and $r_x \in D_n$ be the unique numbers such that $x = q_x n + r_x$ and $|q_x n| < |x|$. Then, the function $h\colon \mathbb{Z} \to \mathbb{R}$ such that $h(x) = g(r_x) + q_x g(n)$ satisfies that for all $x, y \in \mathbb{Z}$,

$$|h(x+y) - h(x) - h(y)| \quad \leq \quad (1{+}2^p)\theta\,(|x|^p + |y|^p)\,.$$

Thus, we immediately obtain the following:

Theorem 3 *Let $p \in [0, 1)$ and $C_p = (1{+}2^p)/(2{-}2^p)$. If $g\colon D_{2n} \to \mathbb{R}$ is such that for all $x, y \in D_n$,*

$$|g(x+y) - g(x) - g(y)| \quad \leq \quad \theta\,(|x|^p + |y|^p)\,,$$

then there exists a linear function $T\colon D_n \to \mathbb{R}$ such that

$$\forall x \in D_n\,, \qquad |g(x) - T(x)| \quad \leq \quad 2C_p\theta|x|^p\,.$$

Proof: Define h as in the Extension Lemma and T as in Lemma 1. Observe then that $h|_{D_n} = g$ and restrict T to D_n. ∎

In [HS92] it is shown that the condition that p be strictly less than 1 is necessary for Lemma 1 to hold. To see this, let f be the function which at x takes the value $x \log_2 |x{+}1|$ if $x \geq 0$, and $x \log_2 |x{-}1|$ if $x < 0$. Observe that f is nonlinear and that $|f(x+y) - f(x) - f(y)| \leq |x| + |y|$ for all $x, y \in \mathbb{Z}$. The same function is a counterexample for Theorem 3 when $p = 1$.

The particular case of Theorem 3 where $p = 0$ is implicit in [Sko83] and reduces to the result of [EKR96] concerning stability of the functional equation $f(x+y) - f(x) - f(y) = 0$. But, even in this special case, the analysis in [EKR96] is rather technical and requires first approximating the function at hand by two additive functions (one defined over the negative elements and another for the positive elements of the domain) and then combining them to get the desired additive function. We bypass all of these technical problems.

In summary, in order to tackle the local stability problem one could follow a two step approach. First, extend the function in an appropriate way to a domain which is algebraically closed and then use a Rassias

type result to obtain the desired conclusion. Although this is a rather natural approach, it requires more work than necessary. To explain this, observe that if g and h are such that $h(x) = h(r_x) + q_x g(n)$, then the limit of $T(x) = h(2^m x)/2^m$ when m goes to ∞ is $xg(n)/n$. Hence, we get for free that T is well defined and determines a linear mapping. Thus, Lemma 1 is only needed in the proof of Theorem 3 in order to prove that T is a good approximation of g. The next lemma shows that to prove this a hypothesis weaker than the one of Lemma 1 suffices.

Lemma 3 *Let E_1 be a normed semi–group and E_2 be a normed vector space over $\mathbb{R}$. Let $p \in [0,1)$, let $\beta(\cdot)$ be a nonnegative, nondecreasing, and even function, such that $\beta(2s) \leq 2^p \beta(s)$ for all $s \in E_1$,[1] and let $h\colon E_1 \to E_2$ be such that*

$$\forall x \in E_1\,, \qquad \|h(2x) - 2h(x)\| \;\leq\; 2\beta(x)\,.$$

If $T\colon E_1 \to E_2$ is such that $T(x) = \lim_{m\to\infty} h(2^m x)/2^m$ is a well defined mapping, then

$$\forall x \in E_1\,, \qquad \|h(x) - T(x)\| \;\leq\; 2/(2{-}2^p)\beta(x)\,.$$

Proof: We follow the same argument used by Rassias [Ras78] to prove Lemma 1. We claim that for any positive integer m,

$$\|h(2^m x)/2^m - h(x)\| \;\leq\; \beta(x) \sum_{t=0}^{m-1} 2^{t(p-1)}\,.$$

The verification of this claim follows by induction on m. The case $m = 1$ is clear because of the hypothesis. Assume the claim holds for m. To prove it for $(m{+}1)$, note that

$$\begin{aligned}
&\left\| \tfrac{h(2^{m+1}x)}{2^{m+1}} - h(x) \right\| \\
&\leq \left\| \tfrac{h(2x)}{2} - h(x) \right\| + \tfrac{1}{2} \left\| \tfrac{h(2^m \cdot 2x)}{2^m} - h(2x) \right\| \\
&\leq \beta(x) + \tfrac{1}{2}\beta(2x) \sum_{t=0}^{m-1} 2^{t(p-1)}\,.
\end{aligned}$$

To conclude the induction observe that $\beta(2x) \leq 2^p \beta(x)$. Thus, $\|h(2^m x)/2^m - h(x)\| \leq 2/(2{-}2^p)\beta(x)$ for all $x \in E_1$ and all m. Since T is well defined the desired conclusion follows letting $m \to \infty$. ∎

When the same error term is considered, the hypothesis of Lemma 3 is weaker than that of Rassias' Lemma. Hence, in order to apply Lemma 3, a weaker conclusion than that of the Extension Lemma will suffice. Below we state such a weaker form of the Extension Lemma but for a more general error term.

[1] E.g., $\beta(s) = \|s\|^p$, or $\beta(s) = \max\{a, \|s\|^p\}$ for some nonnegative real number a.

Lemma 4 *Let $\beta(\cdot,\cdot)$ be a valid error term of degree $p \in [0,1)$. Let $g\colon D_{2n} \to \mathbb{R}$ be such that*

$$\forall x, y \in D_n, \qquad |g(x{+}y) - g(x) - g(y)| \;\leq\; \beta(x,y)\,.$$

Let $q_0 = r_0 = 0$ and for $x \in \mathbb{Z} \setminus \{0\}$ let $q_x \in \mathbb{Z}$ and $r_x \in D_n$ be the unique numbers such that $x = q_x n + r_x$ and $|q_x n| < |x|$. Then, the function $h\colon \mathbb{Z} \to \mathbb{R}$ such that $h(x) = g(r_x) + q_x g(n)$ satisfies that

$$\forall x \in \mathbb{Z}, \qquad |h(2x) - 2h(x)| \;\leq\; (1{+}2^p)\beta(x,x)\,.$$

Proof: See Appendix B. ∎

An immediate consequence of the two previous results is Theorem 1.

2.2 Approximate Multi-linearity

In this section we consider functions of k-variables that satisfy in each of its k coordinates an approximately linear functional equation on a bounded hypercube of $\mathbb{Z}^k$. We again extend such a function, but now to a function defined over all of $\mathbb{Z}^k$. We then show that such an extension can be well approximated by a function which is linear in each of its coordinates. Thus, our approximate stability result for multi-linear functions is obtained using an extension technique similar to the one illustrated in Sect. 2.1.

We now state our problem precisely. For clarity of exposition we limit our discussion to functions of two variables. Consider a function $g\colon D_{2n} \times D_{2n} \to \mathbb{R}$ such that for all $x, x', y, y' \in D_n$,

$$\begin{aligned}
|g(x{+}x', y) - g(x,y) - g(x',y)| &\leq \beta_{1,y}(x,x')\,, \\
|g(x, y{+}y') - g(x,y) - g(x,y')| &\leq \beta_{2,x}(y,y')\,,
\end{aligned}$$

where $\beta_{i,z}(\cdot,\cdot)$ is a valid error term of degree $p \in [0,1)$ which when viewed as a function of z is even and is such that $\beta_{i,\lambda z}(\cdot,\cdot) \leq \lambda \beta_{i,z}(\cdot,\cdot)$ for all real numbers z and $\lambda \geq 1$. Examples of this type of function are $\beta_{i,z}(s,t) = \max\{|z|^p, |s|^p, |t|^p\}$, and $\beta_{i,z}(s,t) = |z|^p + |s|^p + |t|^p$.

For r_z and q_z defined as in Sect. 2.1 let $h\colon \mathbb{Z}\times\mathbb{Z} \to \mathbb{R}$ be such that

$$\begin{aligned}
h(x,y) \;=\; & g(r_x, r_y) + q_x g(n, r_y) \\
& + q_y g(r_x, n) + q_y q_x g(n,n)\,.
\end{aligned}$$

Theorem 1 implies that the function $T_1\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{R}$ defined by

$$T_1(x,y) \;=\; \lim_{m\to\infty} \frac{1}{2^m} h(2^m x, y) \;=\; \frac{x}{n} h(n,y)\,,$$

is such that $|h(x,y) - T_1(x,y)| \leq C_p \beta_{1,y}(x,x)$ for all $x \in \mathbb{Z}$ and $y \in D_n$. Note that $T_1(\cdot, y)$ is linear for all $y \in \mathbb{Z}$. Furthermore, for all $x, y \in \mathbb{Z}$, we have that

$$\begin{aligned}
|T_1(x,2y) - 2T_1(x,y)| &= \frac{|x|}{n} |h(n,2y) - 2h(n,y)| \\
&\leq \frac{|x|}{n} (1{+}2^p) \beta_{2,n}(y,y)\,,
\end{aligned}$$

where the equality follows by definition of T_1 and the inequality follows from Lemma 4. Hence, the function $T_2\colon \mathbb{Z}\times\mathbb{Z}\to\mathbb{R}$ defined by

$$T_2(x,y) \;=\; \lim_{m\to\infty}\frac{1}{2^m}T_1(x,2^m y) \;=\; \frac{xy}{n^2}g(n,n)\,,$$

is linear in each of its coordinates. Moreover, Lemma 3 implies that for all $x,y\in\mathbb{Z}$, $|T_1(x,y)-T_2(x,y)|\le C_p\frac{|x|}{n}\beta_{2,n}(y,y)$. Observe that $h(x,y)=g(x,y)$ and $\frac{|x|}{n}\beta_{2,n}(y,y)\le\beta_{2,x}(y,y)$ if $x,y\in D_n$. We conclude that T_2 is linear in each of its coordinates and for all $x,y\in D_n$,

$$|g(x,y)-T_2(x,y)| \;\le\; C_p(\beta_{1,y}(x,x)+\beta_{2,x}(y,y))\,.$$

Clearly, the above argument can be generalized to functions of more than two variables. We leave the details to the interested reader. Nevertheless, we do state one form of the general result that we will use.

Theorem 4 *Let $p\in[0,1)$, $C_p=(1{+}2^p)/(2{-}2^p)$, $\theta>0$, and $a\ge 0$. Also, let $\vec{e}_i\in\mathbb{Z}^k$ be such that $(\vec{e}_i)_j=1$ if $i=j$ and 0 otherwise. Let $g\colon (D_{2n})^k\to\mathbb{R}$ be such that for all $i\in\{1,\ldots,k\}$, $\vec{z}\in(D_n)^k$ where $z_i=0$, and $x,x'\in D_n$,*

$$\begin{aligned}&|g(\vec{z}{+}(x{+}x')\vec{e}_i)-g(\vec{z}{+}x\vec{e}_i)-g(\vec{z}{+}x'\vec{e}_i)|\\ &\qquad\le\;\theta\max\{a,|z_1|^p,\ldots,|z_k|^p,|x|^p,|x'|^p\}\,.\end{aligned}$$

Then, there is a function $T\colon(D_n)^k\to\mathbb{R}$ linear in each of its coordinates such that for all $\vec{x}\in(D_n)^k$,

$$|g(\vec{x})-T(\vec{x})| \;\le\; \theta C_p k\max\{a,|x_1|^p,\ldots,|x_k|^p\}\,.$$

When $p=0$, Theorem 4 reduces to the result stated in [EKR96, Theorem 9].

2.3 Polynomials

The main purpose of this section is to prove a stability result like that of Sect. 2.1 applicable to univariate polynomials. We require such a stability result in order to provide an approximate relative error test for univariate polynomials. Our stability result for polynomials, as well as its proof, is an extension of an argument in [AB83] generalized in [EKR96] to the absolute error case over finite rational domains.

We adopt the standard convention of denoting the *forward difference operator* by ∇_t. Recall that $\nabla_t g(x)=g(x{+}t)-g(x)$. Let ∇_t^d be the operator corresponding to d applications of ∇_t. For $\vec{t}\in\mathbb{R}^d$ let $\nabla_{\vec{t}}$ be the operator corresponding to the applications of $\nabla_{t_1},\ldots,\nabla_{t_d}$. It is easy to check that; ∇_t is linear, ∇_{t_1} and ∇_{t_2} commute, $\nabla_{t_1,t_2}=\nabla_{t_2,t_1}=\nabla_{t_1+t_2}-\nabla_{t_1}-\nabla_{t_2}$, and that $\nabla_t^d g(x)=\sum_{k=0}^d(-1)^{d-k}\binom{d}{k}g(x{+}kt)$.

The usefulness of the difference operator in testing was recognized by Rubinfeld and Sudan [RS92]. Its utility is mostly based on two facts; (1) $\nabla_t g(x)$ can be computed efficiently, (2) g is a degree d–1 polynomial over a vector space V, if and only if, $\nabla_t^d g(x)=0$ for all $x\in V$ and $t\in\mathbb{Z}$ (see [BF90] for a more general form of this fact). In [EKR96] it was shown that if the latter interpolation identity was approximately true, modulo an absolute error term, over a large bounded subset of the integers, then g was close, again modulo an absolute error term, to a degree d–1 polynomial over a smaller and coarser sub-domain. The reason that the closeness could only be obtained on a coarser sub-domain is that whereas the interpolation identity uses evenly spaced points, in order to prove stability, a more general condition with arbitrarily spaced points is needed. The lemmas stated below yield the same conclusion, but now modulo a relative error term. Both of the following statements are similar to results derived in [EKR96]. Their proofs follow directly from arguments developed in [AB83, Gaj90, EKR96], thus we omit them.

Lemma 5 *Let $a>0$, $\mu_d=\mathrm{lcm}\{1,\ldots,d\}$, and g be a real valued function over $D_{\mu_d\cdot d(d+1)n}$. Let $f\colon D_{dn}\to\mathbb{R}$ be such that $f(x)=g(\mu_d\cdot x)$. If for all $x,t\in D_{\mu_d\cdot dn}$,*

$$|\nabla_t^d g(x)| \;\le\; \frac{\theta}{(\mu_d d)^p 2^d}\max\{a,|x|^p,|t|^p\}\,,$$

then for all $\vec{t}\in(D_n)^d$,

$$|\nabla_{\vec{t}} f(0)| \;\le\; \theta\max\{a,|t_1|^p,\ldots,|t_d|^p\}\,.$$

Lemma 6 *Let d be a positive integer, $p\in[0,1)$, $\theta>0$, and $C_p=(1{+}2^p)/(2{-}2^p)$. Let $a>0$ and $f\colon D_{dn}\to\mathbb{R}$ be such for all $\vec{t}\in(D_n)^d$,*

$$|\nabla_{\vec{t}} f(0)| \;\le\; \theta\max\{a,|t_1|^p,\ldots,|t_d|^p\}\,.$$

Then, there exists a polynomial $h_{d-1}\colon D_n\to\mathbb{R}$ of degree at most d–1 such that for all $x\in D_n$,

$$|f(x)-h_{d-1}(x)| \;\le\; \theta\prod_{i=1}^{d-1}(1{+}iC_p)\max\{a,|x|^p\}\,.$$

3 Robustness with Relative Error

3.1 Linearity

In this section we first prove approximate robustness in the relative error sense for the functional equation $f(x{+}y)-f(x)-f(y)=0$. We then prove Theorem 2. Before proceeding we need to introduce some notation. Recall that the median of a set $S\subseteq\mathbb{R}$ is the smallest value of a such that $\Pr_{x\in S}[x\ge a]$ is at most $1/2$. For a function $f\colon X\to\mathbb{R}$ we denote by $\mathrm{Med}_{x\in X}(f(x))$ the median of the values taken by f when x varies in X. To prove Theorem 2, we associate to P a function $g\colon D_{2n}\to\mathbb{R}$ such that $g(x)=\mathrm{Med}_{y\in D_{|x|}}(P(x{+}y)-$

$P(y))$ if $|x| \geq \sqrt{\delta}n$, and $g(x) = \mathrm{Med}_{y \in D_{\sqrt{\delta}n}}(P(x+y) - P(y))$ otherwise. Note that the size of the set over which the median is taken is proportional to the size of x except when x is less than $\sqrt{\delta}n$, in which case the median is taken over $D_{\sqrt{\delta}n}$. The latter is the main departure of our proof technique from traditional analyzes of absolute error approximate testers. For the ease of exposition, we shall only prove the particular case of Theorem 2 where $\beta(x,y) = \theta \max\{|x|^p, |y|^p\}$ for some $\theta > 0$. In the full version of the paper we consider the more general case. Below we state two lemmas, whose proofs are in Appendix C, and derive from them the particular case of Theorem 2 we desire.

Lemma 7 *Let $\phi(z) = \max\{\sqrt{\delta}n, |z|\}$. Under the hypothesis of Theorem 2, if $x \in D_n$ is randomly chosen, then $|P(x) - g(x)| > \theta\phi(x)^p$ with probability at most $\delta/6$.*

Lemma 8 *Let $\phi(z) = \max\{\sqrt{\delta}n, |z|\}$. Under the hypothesis of Theorem 2, if $x, y \in D_n$, then $|g(x+y) - g(x) - g(y)| \leq 16\theta \max\{\phi(x)^p, \phi(y)^p\}$.*

To prove Theorem 2 observe that under its hypothesis Lemma 8 and Theorem 1 imply that there is a linear map $T: \mathbb{Z} \to \mathbb{R}$ such that $|g(x) - T(x)| \leq 16C_p\theta\phi(x)^p$ for all x in D_n. Since $1 \leq C_p$, Lemma 7 implies that if $x \in D_n$ is randomly chosen, then $|P(x) - T(x)| > 17\theta C_p\phi(x)^p$ with probability at most $\delta/6 \leq \sqrt{\delta}/6$. To conclude the proof observe that $\Pr_{x \in D_n}[\phi(x) = |x|] \geq 1 - \sqrt{\delta}$.

3.2 Polynomials

In this section we prove approximate robustness, in the relative error sense, for the interpolation identity $\nabla_t^d f(x) = 0$. As explained in Sect. 2.3, we establish such a result on a coarser domain than the one where this identity approximately holds. From this, if kD_n denotes $\{kx \in \mathbb{Z} : x \in D_n\}$, we get:

Theorem 5 *Let $\theta > 0$, $p \in [0,1)$, $C_p = (1+2^p)/(2-2^p)$, $\delta \in [0,1]$, and d be a positive integer. Furthermore, let $\mu_d = \mathrm{lcm}\{1, \ldots, d\}$, and $P: D_{2(d+1)^3\mu_d n} \to \mathbb{R}$ be such that*

$$\Pr_{x,t}\left[|\nabla_t^d P(x)| > \theta \max\{|x|^p, |t|^p\}\right] \quad \leq \quad \delta/(16(d+1)^5)\,,$$

where x and t are randomly chosen in $D_{d(d+1)^2\mu_d n}$ and $D_{d(d+1)\mu_d n}$ respectively. Then, there exists a constant $C = 2^{\Theta(d\log(dC_p))}$ and a polynomial $h_{d-1}: \mu_d D_n \to \mathbb{R}$ of degree at most $d-1$ such that

$$\Pr_{x \in \mu_d D_n}\left[|P(x) - h_{d-1}(x)| > C\theta|x|^p\right] \quad \leq \quad \mu_{d-1}\delta + d\sqrt{\delta}\,.$$

Remark 1 *Under a stronger hypothesis, an $O(1)d\sqrt{\delta}$ instead of the $\mu_{d-1}\sqrt{\delta} + d\delta$ bound can be achieved.*

To prove Theorem 5 we proceed as in the proof of Theorem 2. Indeed, let $m = \mu_d \cdot dn$, $\alpha_k = (-1)^{k+1}\binom{d}{k}$, and associate to P a function $g: D_{(d+1)m} \to \mathbb{R}$ whose value at x is $\mathrm{Med}_{t \in D_{|x|}}\left(\sum_{k=1}^d \alpha_k P(x+kt)\right)$ if $|x| \geq \sqrt{\delta}m$, and $\mathrm{Med}_{t \in D_{\sqrt{\delta}m}}\left(\sum_{k=1}^d \alpha_k P(x+kt)\right)$ otherwise. (Observe that $\nabla_t^d P(x) = 0$, if and only if, $P(x) = \sum_{k=1}^d \alpha_k P(x+kt)$.) Thence, Theorem 5 follows from Lemma 5, Lemma 6, and the following two lemmas:

Lemma 9 *Let $\phi(z) = \max\{\sqrt{\delta}m, |z|\}$, where $m = \mu_d \cdot dn$. Under the hypothesis of Theorem 5, if $x \in \mu_d D_n$ is randomly chosen, then $|P(x) - g(x)| > \theta\phi(x)^p$ with probability at most $\mu_d\delta/(4(d+1))$.*

Lemma 10 *Let $\phi(z) = \max\{\sqrt{\delta}m, |z|\}$, where $m = \mu_d \cdot dn$. Under the hypothesis of Theorem 5, if $x, t \in D_m$, then $|\nabla_t^d g(x)| \leq 2^d O(d^4)\theta \max\{\phi(x)^p, \phi(t)^p\}$.*

4 Testing with Relative Error

In this section we show how to put together the results derived so far and obtain approximate relative error testers. First, we introduce some basic terminology. Let $\mathcal{F}$ be a collection of real valued functions over D. For $P, f, \beta: D \to \mathbb{R}$ let

- $\mathrm{Dist}_D(P, f, \beta) = \Pr_{x \in D}[|P(x) - f(x)| > \beta(x)]$ — the *β-relative distance of P from f on D.*
- $\mathrm{Dist}_D(P, \mathcal{F}, \beta) = \mathrm{Inf}_{f \in \mathcal{F}} \mathrm{Dist}_D(P, f, \beta)$ — the *β-relative distance of P from $\mathcal{F}$ on D.*

Definition 1 *Let $0 \leq \delta < \delta' \leq 1$, $D' \subseteq D$, and $\mathcal{F}$ be a collection of real valued functions defined over D. Let β and β' be real valued functions also defined over D. A $(D, \beta, \delta; D', \beta', \delta')$–self–tester for $\mathcal{F}$ is a probabilistic oracle program T such that on input $\gamma > 0$ (the confidence parameter) and when allowed to make calls to a program $P: D \to \mathbb{R}$ is such that;*

- *If $\mathrm{Dist}_D(P, \mathcal{F}, \beta) \leq \delta$, then*

$$\Pr\left[T^P(\gamma) \text{ outputs } PASS\right] \quad \geq \quad 1 - \gamma\,.$$

- *If $\mathrm{Dist}_{D'}(P, \mathcal{F}, \beta') \geq \delta'$, then*

$$\Pr\left[T^P(\gamma) \text{ outputs } FAIL\right] \quad \geq \quad 1 - \gamma\,.$$

(Both of the probabilities above are taken over the internal coin tosses of T.)

Usually one requires that a tester be different and simpler than any correct program for the function purportedly computed by P. A convenient, although sometimes too restrictive, way of enforcing this is to have the tester comply with the *little–oh property* [BK89],

i.e., have its running time be asymptotically less than that of the program being tested, where each call to the program counts as one time step in the tester's computation. Also, it is commonly assumed that the tester is faultless and performs exact computations. Nevertheless, our results remain valid in a less restrictive model similar to the one described in [ABC$^+$93].

In what follows it will sometimes be convenient to allow a tester to have access to another oracle function ψ. In such a case we say that the tester has *ψ–help*. Initially, we build testers which receive as help a *c–testable error term of degree $p \in \mathbb{R}$*, i.e., such valid error terms $\beta(\cdot,\cdot)$ for which $\beta(s,s)+\beta(t,t)+\beta(s+t,s+t) \leq c\beta(s,t)$ for some constant c. For the sake of clarity of exposition, from now on we restrict our discussion to the 4–testable error terms such as $\theta\max\{|s|^p,|t|^p\}$ or $\theta(|s|^p+|t|^p)$, where $\theta > 0$. We henceforth will abuse notation and, whenever clear from context, will interpret a function of two variables like $\beta(\cdot,\cdot)$ as the function of one variable that evaluates to $\beta(z,z)$ at z.

The results presented in previous sections concerning linear functions allow us to prove the following:

Theorem 6 *Let $c, c' > 0$ be such that $6c \leq 1/2$ and $(6c'/7)^2 \geq 2$. Let $0 \leq \delta \leq 1/c'$, $\beta(\cdot,\cdot)$ be a 4–testable error term of degree $0 < p < 1$, and $C_p = (1+2^p)/(2-2^p)$. Then, there is a $(D_{8n}, \beta/4, c\delta/384; D_n, 17C_p\beta, c'\sqrt{\delta})$–self–tester with $\beta(\cdot,\cdot)$–help for the class of real valued linear functions over D_{8n}. Moreover, the tester satisfies the little–oh property.*

Proof: Let N be a fixed positive integer whose value will be determined later. The tester T performs N independent rounds of the following experiment; randomly choose $x, y \in D_{4n}$ and verify whether $|P(x+y)-P(x)-P(y)| > \beta(x,y)$. If the inequality is satisfied we say that the round fails. If more than a $\delta/384$ fraction of the rounds fail, then T outputs FAIL, otherwise T outputs PASS. Given that T has oracle access to both P and β, that it can add/subtract and perform comparisons exactly and efficiently, T satisfies the little–oh property.

Suppose the linear function $l\colon D_{8n} \to \mathbb{R}$ is such that $\mathrm{Dist}_{D_{8n}}(P,l,\beta/4) \leq c\delta/384$. Then, by the halving principle, we have that

$$\begin{aligned}
\Pr_{x\in D_{4n}}\left[|P(x)-l(x)| > \tfrac{\beta(x,x)}{4}\right] &\leq \frac{2c\delta}{384},\\
\Pr_{y\in D_{4n}}\left[|P(y)-l(y)| > \tfrac{\beta(y,y)}{4}\right] &\leq \frac{2c\delta}{384},\\
\Pr_{x,y\in D_{4n}}\left[|P(x+y)-l(x+y)| > \tfrac{\beta(x+y,x+y)}{4}\right] &\leq \frac{2c\delta}{384}.
\end{aligned}$$

Hence, since $\beta(s,s)+\beta(t,t)+\beta(s+t,s+t) \leq 4\beta(s,t)$, the union bound implies that a round fails with a probability of at most $6c\delta/384 \leq \frac{1}{2}(\delta/384)$. A standard Chernoff bound argument yields that if $N = \Omega(\frac{1}{\delta}\log\frac{1}{\gamma})$ the probability that T outputs FAIL is at most γ. Suppose now that $\mathrm{Dist}_{D_n}(P,l,17C_p\beta) > c'\sqrt{\delta}$ for all real valued linear functions over D_n. Then, Theorem 2 implies that the probability that a round fails is at least $(6c'/7)^2(\delta/384) \geq 2(\delta/384)$. Again, if $N = \Omega(\frac{1}{\delta}\log\frac{1}{\gamma})$ the desired conclusion follows from a Chernoff bound. ∎

The self–tester of Theorem 6 needs oracle access to the error function. In the context of this work, this is an unrealistic assumption. Also, the tester will not comply with the little–oh property if it has to evaluate a hard to compute help function. We would like to have testers that achieve their goals, comply with the little–oh property, and do not have oracle access to the error function. Surprisingly, this is feasible, as our next stated result shows, provided the testable error function $\beta(\cdot,\cdot)$ is such that for some positive constants λ and λ' there is a function $\varphi(\cdot,\cdot)$ that is *(λ,λ')–equivalent* to $\beta(\cdot,\cdot)$, i.e., $\lambda\varphi(s,t) \geq \beta(s,t) \geq \lambda'\varphi(s,t)$ for all integers s,t. In addition, evaluating φ should be asymptotically faster than executing the program being tested. For example, let k and k' be positive integers and let $\lg(n)$ denote the length of an integer n in binary. (Note that $\lg(n) = \lceil\log_2(|n|+1)\rceil$ or equivalently $\lg(0) = 0$ and $\lg(n) = \lfloor\log_2(|n|)\rfloor + 1$ if $n \neq 0$.) Then, $\beta(s,t) = 2^{k'}(|s|^{1/2^k} + |t|^{1/2^k})$ or $\beta(s,t) = 2^{k'}\max\{|s|^{1/2^k},|t|^{1/2^k}\}$ are testable error terms of degree $1/2^k$ which are $(1,1/2)$–equivalent to $\varphi(s,t) = 2^{k'}(2^{\lceil\lg(s)/2^k\rceil} + 2^{\lceil\lg(t)/2^k\rceil})$ and $\varphi(s,t) = 2^{k'+\max\{\lceil\lg(s)/2^k\rceil,\lceil\lg(t)/2^k\rceil\}}$ respectively. The computation of these latter functions requires only counting and shifting bits.

Theorem 7 *Under the same hypothesis of Theorem 6, if $\varphi(\cdot,\cdot)$ is (λ,λ')–equivalent to $\beta(\cdot,\cdot)$, then there is a $(D_{8n}, \beta/(4\lambda), c\delta/384\ ;\ D_n, 17C_p\beta/\lambda', c'\sqrt{\delta})$–self–tester (without help) for the class of real valued linear functions over D_{8n}. Moreover, the tester satisfies the little–oh property provided φ is easy to compute relative to the cost of executing the program being tested.*

Proof: The proof is almost identical to the proof of Theorem 6 except that now the tester T performs N independent rounds of the following experiment; randomly choose $x, y \in D_{4n}$ and verify whether $|P(x+y)-P(x)-P(y)| > \varphi(x,y)$. ∎

Similar results follow for the class of polynomials based on the results presented in Sect. 2.3 and Sect. 3.2.

5 Final Comments

The error terms considered in this work do not depend on the function f purportedly computed by the program P which we wish to test. We leave open the following:

Problem: For a program P purportedly computing a function in the class of real valued functions $\mathcal{F}$, and given constants $c > c' > 0$, find a simple and efficient self–tester for P which, with high probability,

- Outputs PASS if $\Pr_{x\in D}\left[|P(x) - f(x)| > c|f(x)|\right]$ is at most δ for some function $f \in \mathcal{F}$.
- Outputs FAIL if $\Pr_{x\in D'}\left[|P(x) - f(x)| > c'|f(x)|\right]$ is at least δ' for all functions $f \in \mathcal{F}$.

In particular, what can be said when $\mathcal{F}$ is; (1) the class of real valued linear functions, (2) the class of real valued polynomials of degree at most d, and (3) the class whose only member is the map $x \in D \subseteq \mathbb{R} \to x^{-1}$.

Acknowledgments: We would like to thank Stéphane Boucheron for useful discussions.

References

[AB83] M. Albert and J. Baker. Functions with bounded nth difference. *Ann. Polonici Mathematici*, 43:93–103, 1983.

[ABC+93] S. Ar, M. Blum, B. Codenotti, and P. Gemmell. Checking approximate computations over the reals. In *Proc. 25th STOC*, pp. 786–795, 1993.

[ALM+92] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and intractability of approximation problems. In *Proc. 33rd FOCS*, pp. 14–23, 1992.

[BF90] D. Beaver and J. Feigenbaum. Hiding instances in multioracle queries. In *Proc. 7th STACS*, LNCS 415, pp. 37–48. Springer–Verlag, 1990.

[BK89] M. Blum and S. Kannan. Designing programs that check their work. In *Proc. 21st STOC*, pp. 86–97, 1989.

[BLR90] M. Blum, M. Luby, and R. Rubinfeld. Self-testing/correcting with applications to numerical problems. In *Proc. 22nd STOC*, pp. 73–83, 1990.

[Blu88] M. Blum. Designing programs to check their work. Technical Report TR-88-009, ICSI, 1988.

[BW94] M. Blum and H. Wasserman. Program result-checking: A theory of testing meets a test of theory. In *Proc. 35th FOCS*, pp. 382–392, 1994.

[Cop89] D. Coppersmith. Manuscript. See discussion in [BLR90], December 1989.

[EKR96] F. Ergün, S. Ravi Kumar, and R. Rubinfeld. Approximate checking of polynomials and functional equations. In *Proc. 37th FOCS*, pp. 592–601, 1996.

[For95] G. L. Forti. Hyers–Ulam stability of functional equations in several variables. *Aeq. Mathematicae*, 50:143–190, 1995.

[Gaj90] Z. Gajda. Local stability of the functional equation characterizing polynomial functions. *Ann. Polonici Mathemtici*, 42:119–137, 1990.

[GGR96] O. Goldreich, S. Goldwasser, and D. Ron. Property testing and its connection to learning and approximation. In *Proc. 37th FOCS*, pp. 339–348, 1996.

[GLR+91] P. Gemmell, R. Lipton, R. Rubinfeld, M. Sudan, and A. Wigderson. Self-testing/correcting for polynomials and for approximate functions. In *Proc. 23rd STOC*, pp. 32–42, 1991.

[HR92] D. H. Hyers and T. M. Rassias. Approximate homomorphisms. *Aeq. Mathematicae*, 44:125–153, 1992.

[HS92] D. H. Hyers and P. Šemrl. On the behaviour of mappings which do not satisfy Hyers–Ulam stability. *Proc. American Mathematical Society*, 114(4):989–993, April 1992.

[Hye41] D. H. Hyers. On the stability of the linear functional equation. *Proc. of the National Academy of Science, U.S.A.*, 27:222–224, 1941.

[Knu98] D. E. Knuth. *The Art of Computer Programming*, Vol. 2, Seminumerical Algorithms. Addison-Wesley, third edition, 1998.

[Lip91] R. Lipton. *New directions in testing*, Vol. 2 of *Series in Discrete Mathematics and Theoretical Computer Science*, pp. 191–202. ACM/AMS, 1991.

[Ras78] T. M. Rassias. On the stability of the linear mapping in Banach spaces. *Proc. of the American Mathematical Society*, 72(2):297–300, November 1978.

[RS92] R. Rubinfeld and M. Sudan. Testing polynomial functions efficiently and over rational domains. In *Proc. 3rd SODA*, pp. 23–32, 1992.

[RS96] R. Rubinfeld and M. Sudan. Robust characterizations of polynomials with applications to program testing. *SIAM J. on Computing*, 25(2):252–271, April 1996.

[Rub90] R. Rubinfeld. *A mathematical theory of self-checking, self-testing and self-correcting programs*. PhD thesis, University of California, Berkeley, 1990.

[Rub94] R. Rubinfeld. On the robustness of functional equations. In *Proc. 35th FOCS*, pp. 288–299, 1994.

[Sko83] F. Skof. Sull'approssimazione delle applicazioni localmente δ-additive. *Atti della Accademia delle Sciencze di Torino*, 117:377–389, 1983. (In Italian.)

A Appendix: Tightness

Let n be a positive integer, $0 < p < 1$, $0 < \delta \leq 1/4$, $\theta, c > 0$, let $\beta(x) = \theta|x|^p$, and consider the function $P\colon \mathbb{Z} \to \mathbb{R}$ such that

$$P(x) \;=\; \begin{cases} -\theta(\sqrt{\delta}n)^p & \text{if } -\sqrt{\delta}n \leq x < 0\,, \\ \theta(\sqrt{\delta}n)^p & \text{if } 0 < x \leq \sqrt{\delta}n\,, \\ 0 & \text{otherwise}\,. \end{cases}$$

Observe that if $|x|$ or $|y|$ is greater than $\sqrt{\delta}n$ then $|P(x+y) - P(x) - P(y)| \leq \theta \max\{|x|^p, |y|^p\}$. Hence, if $n' \geq n$, with probability at most δ it holds that $|P(x+y) - P(x) - P(y)| > \theta \max\{|x|^p, |y|^p\}$ when x, y are randomly chosen in $D_{n'}$. A lengthy analysis shows that if T is a linear function then $|P(x) - T(x)| > c\beta(x)$ with probability greater than $\sqrt{\delta}/(\max\{1, 2c\})^{1/p}$ when $x \in D_n$ is randomly chosen.

B Appendix: Proof of Lemma 4

Proof of Lemma 4: Let $x \in \mathbb{Z}$. By definition of h and since $r_{2x} = 2r_x - n(q_{2x} - 2q_x)$ we have that

$$\begin{aligned} |h(2x) - 2h(x)| \;&=\; |g(2r_x - n(q_{2x} - 2q_x)) - 2g(r_x) \\ &\qquad + (q_{2x} - 2q_x)g(n)|\,. \end{aligned}$$

Our objective is to bound the RHS of this equality by $(1+2^p)\beta(x)$. Note that $q_{2x}-2q_x \in \{-1,0,1\}$. We consider three cases depending on the value that this latter quantity takes.

CASE 1: Assume $q_{2x}-2q_x = 0$. Then, since $r_x \in D_n$, the hypothesis implies that $|h(2x)-2h(x)| = |g(2r_x)-2g(r_x)| \leq \beta(r_x,r_x)$. To conclude note that $\beta(r_x,r_x) \leq \beta(x,x)$.

CASE 2: Assume now that $q_{2x}-2q_x = 1$. Hence, $r_{2x} = 2r_x-n$ and

$$\begin{aligned} |h(2x)-2h(x)| &\leq |g(2r_x)-2g(r_x)| \\ &\quad + |g(2r_x-n)+g(n)-g(2r_x)| \\ &\leq \beta(r_x,r_x)+\beta(2r_x-n,n)\,, \end{aligned}$$

where the first inequality is due to the triangle inequality and the second inequality follows, since $r_x, r_{2x} = 2r_x-n, n \in D_n$, from the hypothesis. But, $r_{2x} = 2r_x-n$ is at least $-n$, thus r_x can not be negative implying that $x \geq 0$. Hence, since $2x \geq 0$, we get that $r_{2x} \geq 0$ implying that $2r_x \geq n$. Moreover, $|2r_x-n| = |r_{2x}| \leq n$. Thus, $\beta(2r_x-n,n) \leq \beta(n,n) \leq \beta(2r_x,2r_x) \leq 2^p\beta(r_x,r_x)$. Observing that $\beta(r_x,r_x) \leq \beta(x,x)$ we obtain the desired conclusion.

CASE 3: Assume $q_{2x}-2q_x = -1$. Hence, $r_{2x} = 2r_x+n$ which is at most n, thus r_x can not be positive. Thus, $r_x+n \in D_n$ and

$$\begin{aligned} |h(2x)-2h(x)| &\leq |g(2r_x+n)-g(r_x+n)-g(r_x)| \\ &\quad + |g(r_x+n)-g(r_x)-g(n)| \\ &\leq \beta(r_x+n,r_x)+\beta(r_x,n)\,, \end{aligned}$$

where the first inequality is due to the triangle inequality and the second one follows, since $r_x+n, r_x, n \in D_n$, from the hypothesis. Since r_x is not positive, $x \leq 0$. Hence, since $2x \leq 0$, we get that $r_{2x} \leq 0$ implying that $2r_x \leq -n$. It follows that $|r_x+n| \leq |r_x|$. Thus, $\beta(r_x+n,r_x) \leq \beta(r_x,r_x)$ and $\beta(r_x,n) \leq \beta(2r_x,2r_x) \leq 2^p\beta(r_x,r_x)$. Observing that $\beta(r_x,r_x) \leq \beta(x,x)$ we obtain the desired conclusion. ∎

C Appendix: Proofs of Lemma 7 and Lemma 8

For the sake of future reference, below we state a fact that we will repeatedly use.

Fact 1 [Halving principle] *Let Ω and S denote finite sets such that $S \subseteq \Omega$, and let ψ be a boolean function defined over Ω. Then,*

$$\Pr_{x\in S}[\psi(x)] \leq \frac{|\Omega|}{|S|}\Pr_{x\in\Omega}[\psi(x)]\,.$$

The choice of name for the observation is due to the fact that when Ω is twice the size of S, then $\Pr_{x\in\Omega}[\psi(x)]$ is at least one half of $\Pr_{x\in S}[\psi(x)]$.

Proof of Lemma 7: Let $P_{x,y} = P(x+y)-P(x)-P(y)$. Observe that by definition of g and Markov's inequality we have that

$$\begin{aligned} &\Pr_{x\in D_n}[|g(x)-P(x)| > \theta\phi(x)^p] \\ &= \Pr_{x\in D_n}\left[|\operatorname*{Med}_{y\in D_{\phi(x)}}(P_{x,y})| > \theta\phi(x)^p\right] \\ &\leq 2\Pr_{x\in D_n, y\in D_{\phi(x)}}[|P_{x,y}| > \theta\phi(x)^p]\,. \end{aligned}$$

But, $\phi(x) \geq \phi(y) \geq |y|$ and $\phi(x) \geq |x|$ together with the halving principle imply that

$$\begin{aligned} &\Pr_{x\in D_n, y\in D_{\phi(x)}}[|P_{x,y}| > \theta\phi(x)^p] \\ &\leq 32\Pr_{x,y\in D_{4n}}[|P_{x,y}| > \theta\max\{|x|^p,|y|^p\}]\,. \end{aligned}$$

The hypothesis implies the desired conclusion. ∎

Proof of Lemma 8: First we will show that, for all $c \in D_{2n}$ and $I \subseteq D_{\phi(c)}$ such that $|I| \geq \sqrt{\delta}n+1$,

$$\Pr_{y\in I}[|g(c)-(P(c+y)-P(y))| > 4\theta\phi(c)^p] < 1/3\,. \quad (2)$$

Let $P_{x,y} = P(x+y)-P(x)-P(y)$. Note that Markov's inequality implies that

$$\begin{aligned} &\Pr_{y\in I}[|g(c)-(P(c+y)-P(y))| > 4\theta\phi(c)^p] \\ &\leq 2\Pr_{y\in I, z\in D_{\phi(c)}}[|P_{c+y,z}-P_{c+z,y}| > 4\theta\phi(c)^p]\,. \end{aligned}$$

Observe now that if y and z are randomly chosen in I and $D_{\phi(c)}$ respectively, then from the union bound we conclude that

$$\begin{aligned} &\Pr_{y,z}[|P_{c+y,z}-P_{c+z,y}| > 4\theta\phi(c)^p] \\ &\leq \Pr_{y,z}[|P_{c+z,y}| > 2\theta\phi(c)^p] + \Pr_{y,z}[|P_{c+y,z}| > 2\theta\phi(c)^p]\,. \end{aligned}$$

But, $\phi(c) \geq |y|, |z|$ so $2\phi(c) \geq |c+y|, |c+z|$. Hence, the halving principle implies that

$$\begin{aligned} &\Pr_{y,z}[|P_{c+z,y}| > 2\theta\phi(c)^p] + \Pr_{y,z}[|P_{c+y,z}| > 2\theta\phi(c)^p] \\ &\leq 2\tfrac{|D_{4n}|^2}{|I|\cdot|D_{\phi(c)}|}\Pr_{u,v\in D_{4n}}[|P_{u,v}| > \theta\max\{|u|^p,|v|^p\}]\,. \end{aligned}$$

Since $(|D_{4n}|^2/|I|\cdot|D_{\phi(c)}|) < 32/\delta$, the hypothesis implies (2).

Now, to prove the lemma, let $a,b \in D_n$ and let $G_{c,y} = g(c)-(P(c+y)-P(y))$. Without loss of generality, assume $|a| \leq |b|$. If $a \geq 0$ (respectively $a < 0$), by (2), with nonzero probability there is a $y \in \{-\sqrt{\delta}n,\ldots,0\}$ (respectively $y \in \{0,\ldots,\sqrt{\delta}n\}$) for which we have that $|G_{a,y}| \leq 4\theta\phi(a)^p$, $|G_{b,a+y}| \leq 4\theta\phi(b)^p$, and $|G_{a+b,y}| \leq 4\theta\phi(a+b)^p$. Hence, since $\phi(a+b)^p \leq \phi(a)^p+\phi(b)^p$, we conclude that $|g(a+b)-g(a)-g(b)| \leq |G_{a+b,y}-G_{a,y}-G_{b,a+y}|$ is upper bounded by $16\theta\max\{\phi(a)^p,\phi(b)^p\}$. ∎