Testing low-degree trigonometric polynomials

Martijn Baartse

Brandenburg University of Technology, Cottbus-Senftenberg, Germany

CSR 2014

Joint work with Klaus Meer

(work supported by DFG, GZ:ME 1424/7-2)

Real number model developed by Blum, Shub and Smale in 1989.

The BSS model focusses on algebraic algorithms.

Basic entities:	Real numbers
Operations:	$+, -, *, :$
Test:	$x \geq 0?$

Real number model developed by Blum, Shub and Smale in 1989.

The BSS model focusses on algebraic algorithms.

Basic entities:	Real numbers
Operations:	$+, -, *, :$
Test:	$x \geq 0$?

Alternative approach: recursive analysis

Definition

The class $\mathrm{NP}_{\mathbb{R}}$ is the set of languages $L \subset \mathbb{R}^* := \bigcup_{n \geq 1} \mathbb{R}^n$ for which there exists a verifier V with the properties

Definition

The class $\mathrm{NP}_{\mathbb{R}}$ is the set of languages $L \subset \mathbb{R}^* := \bigcup_{n \geq 1} \mathbb{R}^n$ for which there exists a verifier V with the properties

- if $x \in L$ then there exists $y \in R^*$ such that V accepts (x, y) in time polynomial in the size of x
- if $x \notin L$ then V rejects (x, y) for every $y \in R^*$

Definition

The class $NP_{\mathbb{R}}$ is the set of languages $L \subset \mathbb{R}^* := \bigcup_{n \geq 1} \mathbb{R}^n$ for which there exists a verifier V with the properties

- if $x \in L$ then there exists $y \in R^*$ such that V accepts (x, y) in time polynomial in the size of x
- if $x \notin L$ then V rejects (x, y) for every $y \in R^*$

Theorem

The problem whether a system of quadratic polynomials has a real common zero (QPS) is $NP_{\mathbb{R}}$-complete

Line of research: how do important classical theorems behave in the BSS model? What happens to the proofs?

Line of research: how do important classical theorems behave in the BSS model? What happens to the proofs?

- Better understanding of the relationship between both models.
- New questions which can be interesting on their own.

Line of research: how do important classical theorems behave in the BSS model? What happens to the proofs?

- Better understanding of the relationship between both models.
- New questions which can be interesting on their own.

Example

- $NP_{\mathbb{R}}$ is decidable in single exponential time (Grigoriev & Vorobjov, Renegar, Heintz et al, ...)
- Toda's theorem (Basu & Zell)
- $PCP_{\mathbb{R}}$ theorem (Baartse & Meer 2013)

Theorem (ALMSS 1992, Algebraic proof)

Every $L \in NP$ has a probabilistic verifier that uses $O(\log(n))$ random bits to make $O(1)$ queries to the certificate such that

- *for all $x \in L$ there is a certificate that is accepted and*
- *for all $x \notin L$ every certificate is rejected with high probability.*

In short: $NP = PCP(\log n, 1)$.

Theorem (ALMSS 1992, Algebraic proof)

Every $L \in NP$ has a probabilistic verifier that uses $O(\log(n))$ random bits to make $O(1)$ queries to the certificate such that

- *for all $x \in L$ there is a certificate that is accepted and*
- *for all $x \notin L$ every certificate is rejected with high probability.*

In short: $NP = PCP(\log n, 1)$.

Theorem (Dinur 2005, Combinatorial proof)

$NP = PCP(\log n, 1)$

Theorem (Baartse, Meer 2013, along the lines of Dinur)

$NP_{\mathbb{R}} = PCP_{\mathbb{R}}(\log n, 1)$

Theorem (Baartse, Meer 2013, along the lines of Dinur)

$NP_{\mathbb{R}} = PCP_{\mathbb{R}}(\log n, 1)$

Question

Can the $\mathrm{PCP}_{\mathbb{R}}$ theorem also be proven along the lines of ALMSS?

Theorem (Baartse, Meer 2013, along the lines of Dinur)

$NP_{\mathbb{R}} = PCP_{\mathbb{R}}(\log n, 1)$

Question

Can the $PCP_{\mathbb{R}}$ theorem also be proven along the lines of ALMSS?

To what extend can the coding techniques used by ALMSS be applied in the BSS model? Are there alternatives?

Essential in ALMSS:

Given $g : F^k \to F$ (finite field),

is there a polynomial P with low degree

such that for most $x \in F^k$,

$g(x) = P(x)$?

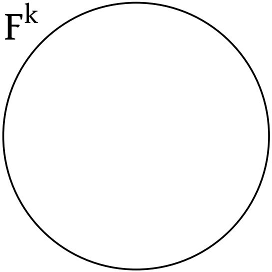
Essential in ALMSS:

Given $g : F^k \to F$(finite field),

is there a polynomial P with low degree

such that for most $x \in F^k$,

$g(x) = P(x)$?



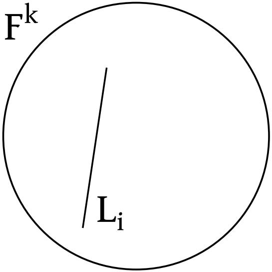
Essential in ALMSS:

Given $g : F^k \to F$ (finite field),

is there a polynomial P with low degree

such that for most $x \in F^k$,

$g(x) = P(x)$?



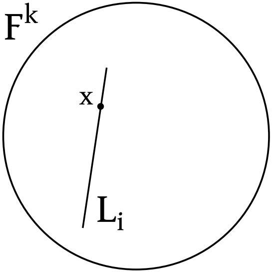
Essential in ALMSS:

Given $g : F^k \to F$ (finite field),

is there a polynomial P with low degree

such that for most $x \in F^k$,

$g(x) = P(x)$?



Essential in ALMSS:

Given $g : F^k \to F$(finite field),

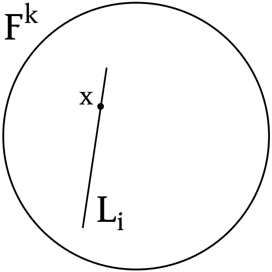
is there a polynomial P with low degree

such that for most $x \in F^k$,

$g(x) = P(x)$?

Line test:

Does g agree with p_{L_i} on x?



Theorem (Rubinfeld, Sudan)

If there exist univariate polynomials $p_{L_1}, \ldots, p_{L_m}$ with low degree such that $Pr[p_{L_i}$ agrees with g on $x] \geq 1 - \delta$, then there exists a polynomial $P : F^k \rightarrow F$ with low degree that agrees with g on all but a 2δ fraction of arguments.

Theorem (Rubinfeld, Sudan)

If there exist univariate polynomials $p_{L_1}, \ldots, p_{L_m}$ with low degree such that $Pr[p_{L_i}$ agrees with g on $x] \geq 1 - \delta$, then there exists a polynomial $P : F^k \to F$ with low degree that agrees with g on all but a 2δ fraction of arguments.

Theorem (Friedl, Hatsagi, Shen)

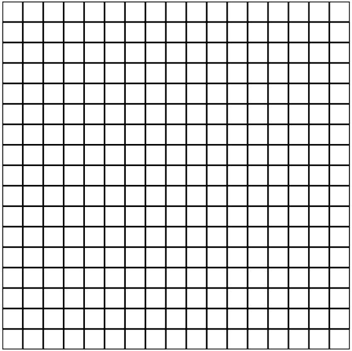
Let $A \subseteq \mathbb{R}$ be finite. Given $g : A^k \to \mathbb{R}$, performing $O(k)$ line tests establishes that g is close to a low-degree polynomial.

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.

Example:

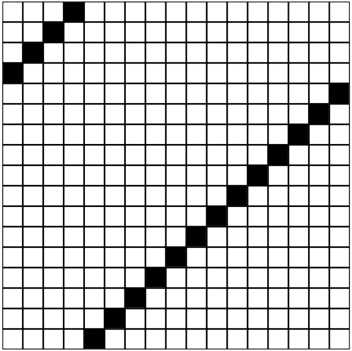
Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.



$g(x, y) = xy^2$

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0,\ldots,16\}^2 \to \mathbb{R}$.

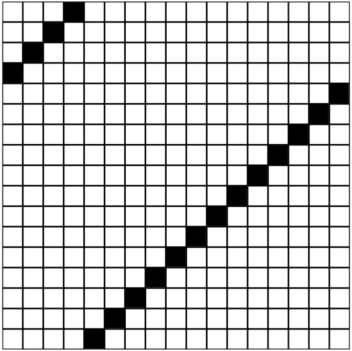


$g(x,y) = xy^2$

$L = \{(t+4,t) | t \in F\}$

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.



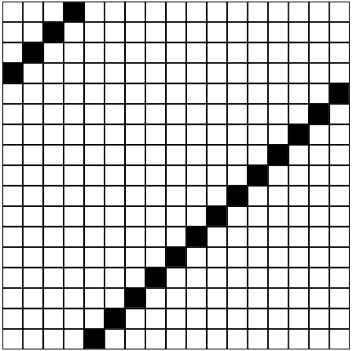
$$g(x, y) = xy^2$$

$$L = \{(t + 4, t) | t \in F\}$$

$$g_L(t) = (t + 4)t^2$$

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.



$$g(x, y) = xy^2$$

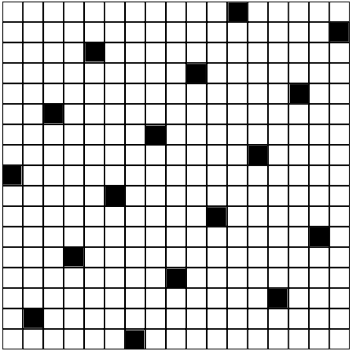
$$L = \{(t+4, t) | t \in F\}$$

$$g_L(t) = (t+4)t^2$$

$$g_L(t) = \begin{cases} (t+4)t^2 & t \leq 12 \\ (t-13)t^2 & t > 12 \end{cases}$$

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.

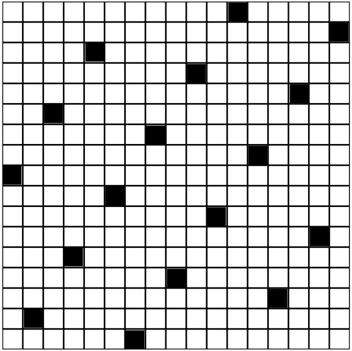


$g(x, y) = xy^2$

$L = \{(2t + 1, 3t + 1) | t \in F\}$

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.



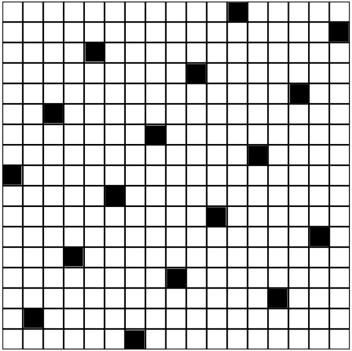
$$g(x, y) = xy^2$$

$$L = \{(2t + 1, 3t + 1) | t \in F\}$$

$$g_L(t) = (2t + 1)(3t + 1)^2$$

Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0,\dots,16\}^2 \to \mathbb{R}$.



$$g(x,y) = xy^2$$

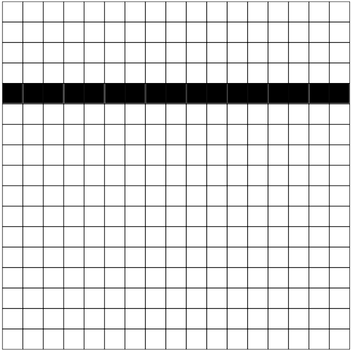
$$L = \{(2t+1, 3t+1) | t \in F\}$$

$$g_L(t) = (2t+1)(3t+1)^2$$

$$g_L(t) = \begin{cases} (2t+1)(3t+1)^2 & t \leq 5 \\ (2t+1)(3t-16)^2 & 5 < t \leq 7 \\ (2t-16)(3t-16)^2 & 7 < t \leq 10 \\ (2t-16)(3t-33)^2 & 10 < t \end{cases}$$

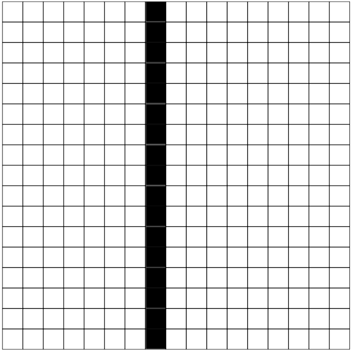
Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.



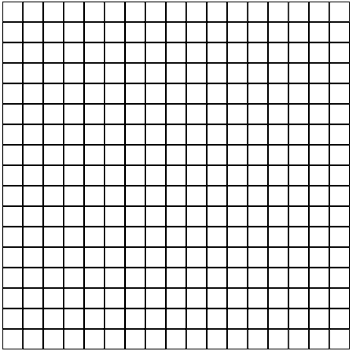
Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0, \ldots, 16\}^2 \to \mathbb{R}$.



Example:

Let F be the finite field with 17 elements. We look at the differences between considering the "same" function as function from F^2 to F and as function from $\{0,\ldots,16\}^2 \to \mathbb{R}$.



$$
\begin{aligned}
g : \{0,1,\ldots,16\}^k &\to \mathbb{R} \\
x &\mapsto \begin{cases} 0 & x_1 < 8 \\ 1 & x_1 \geq 8 \end{cases}
\end{aligned}
$$

Solution:

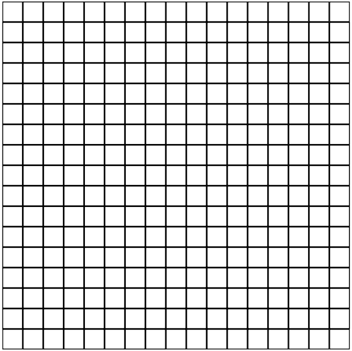
Use trigonometric polynomials with appropriate period.

The difference between the multiplication and addition in F and the multiplication and addition in $\mathbb{R}$ becomes irrelevant.

Solution:

Use trigonometric polynomials with appropriate period.

The difference between the multiplication and addition in F and the multiplication and addition in $\mathbb{R}$ becomes irrelevant.

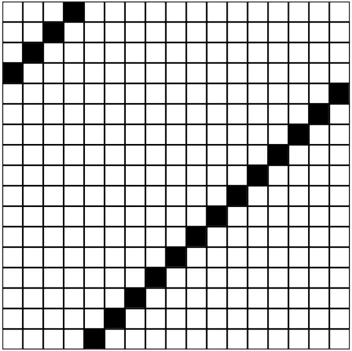


$$h(x, y) = \sin\left(\frac{2\pi}{|F|}x\right)\cos\left(2\frac{2\pi}{|F|}y\right)$$

Solution:

Use trigonometric polynomials with appropriate period.

The difference between the multiplication and addition in F and the multiplication and addition in $\mathbb{R}$ becomes irrelevant.



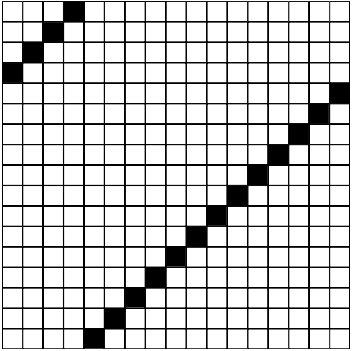
$$h(x,y) = \sin\left(\frac{2\pi}{|F|}x\right)\cos\left(2\frac{2\pi}{|F|}y\right)$$

$$L = \{(t+4,t) | t \in F\}$$

Solution:

Use trigonometric polynomials with appropriate period.

The difference between the multiplication and addition in F and the multiplication and addition in $\mathbb{R}$ becomes irrelevant.



$$h(x, y) = \sin(\tfrac{2\pi}{|F|}x)\cos(2\tfrac{2\pi}{|F|}y)$$

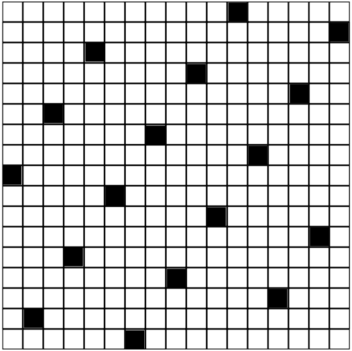
$$L = \{(t+4, t) | t \in F\}$$

$$h_L(t) = \sin(\tfrac{2\pi}{|F|}(t+4))\cos(2\tfrac{2\pi}{|F|}t)$$

Solution:

Use trigonometric polynomials with appropriate period.

The difference between the multiplication and addition in F and the multiplication and addition in $\mathbb{R}$ becomes irrelevant.



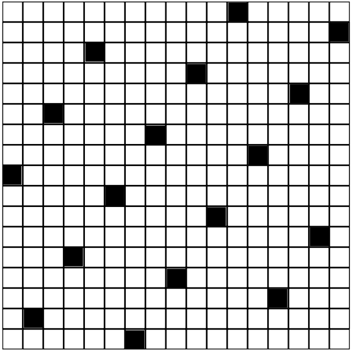
$$h(x, y) = \sin(\tfrac{2\pi}{|F|}x)\cos(2\tfrac{2\pi}{|F|}y)$$

$$L = \{(2t+1, 3t+1) | t \in F\}$$

Solution:

Use trigonometric polynomials with appropriate period.

The difference between the multiplication and addition in F and the multiplication and addition in $\mathbb{R}$ becomes irrelevant.



$$h(x,y) = \sin\left(\frac{2\pi}{|F|}x\right)\cos\left(2\frac{2\pi}{|F|}y\right)$$

$$L = \{(2t+1, 3t+1) | t \in F\}$$

$$h_L = \sin\left(\frac{2\pi}{|F|}(2t+1)\right)\cos\left(2\frac{2\pi}{|F|}(3t+1)\right)$$

- Only lines with small directional vector are suitable for a test.
- Not possible to copy the proof for polynomials from F^k to F.

- Only lines with small directional vector are suitable for a test.
- Not possible to copy the proof for polynomials from F^k to F.

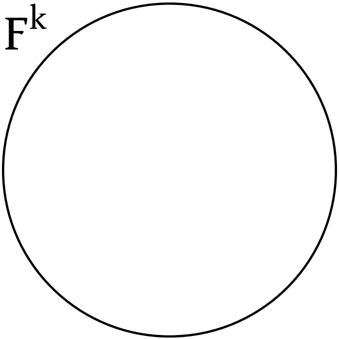
Outline

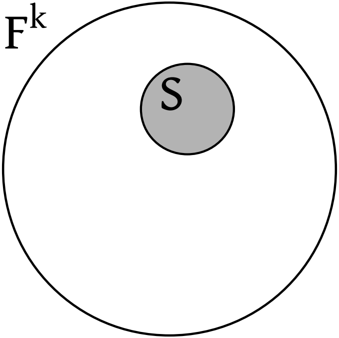
- The suitable lines connect F^k well. Let $G = (V, E)$ be the graph with $V = F^k$ and $(x, y) \in E$ if there is a suitable line connecting x and y. The graph G is an expander with expansion parameter $\lambda(G)$ close to 1.

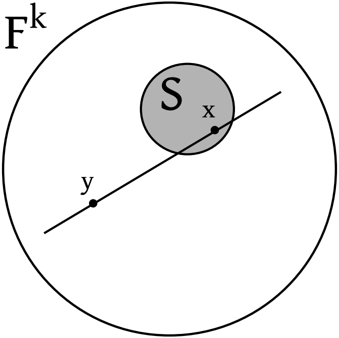
- Only lines with small directional vector are suitable for a test.
- Not possible to copy the proof for polynomials from F^k to F.

Outline

- The suitable lines connect F^k well. Let $G = (V, E)$ be the graph with $V = F^k$ and $(x, y) \in E$ if there is a suitable line connecting x and y. The graph G is an expander with expansion parameter $\lambda(G)$ close to 1.
- If $f : F^k \rightarrow \mathbb{R}$ is ϵ-close to a polynomial, then the probability that the line test rejects is about ϵ, but only if ϵ is small.


F^k


F^k
S


F^k
S
x
y

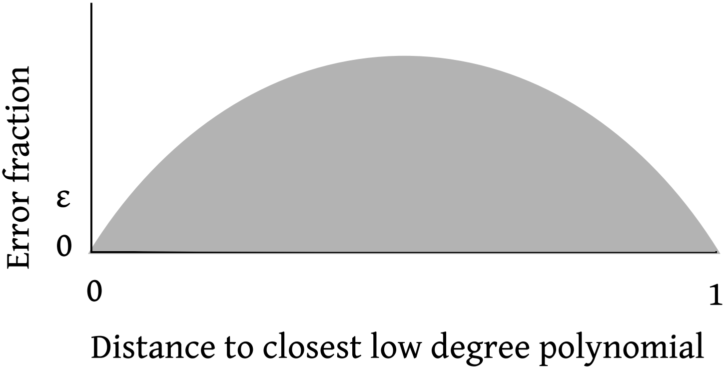
In case f has distance almost 1 to any polynomial we reason as follows. We construct a finite sequence $f_1, f_2, \ldots, f_n$ such that

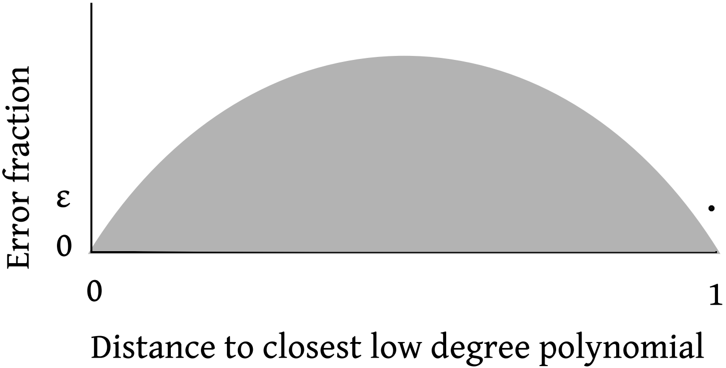
In case f has distance almost 1 to any polynomial we reason as follows. We construct a finite sequence $f_1, f_2, \ldots, f_n$ such that

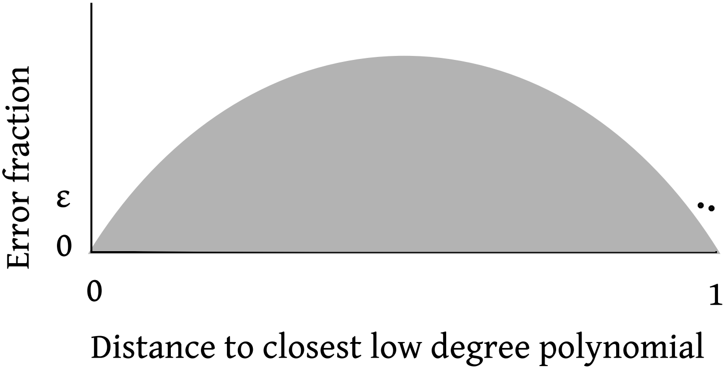
- $f_1 = f$ and f_n is a polynomial
- f_i is very close to f_{i+1}

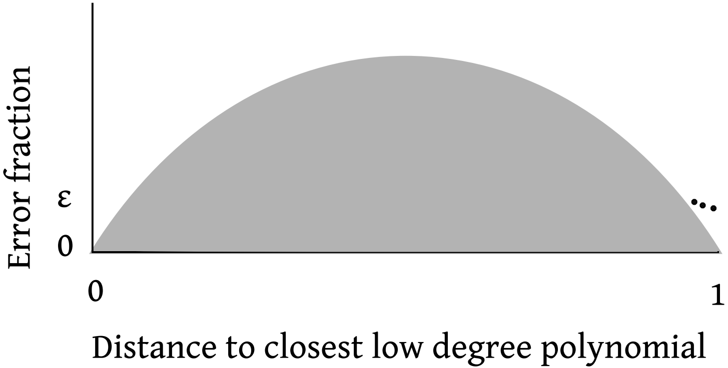
In case f has distance almost 1 to any polynomial we reason as follows. We construct a finite sequence $f_1, f_2, \ldots, f_n$ such that

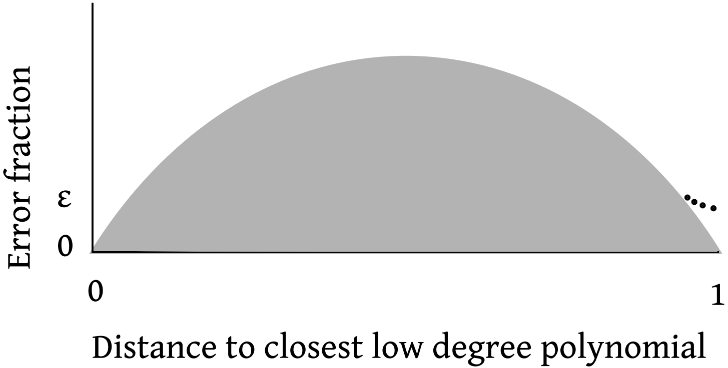
- $f_1 = f$ and f_n is a polynomial
- f_i is very close to f_{i+1}
- for every f_i the probability that the line test rejects is at most two times the probability that the line test rejects f.

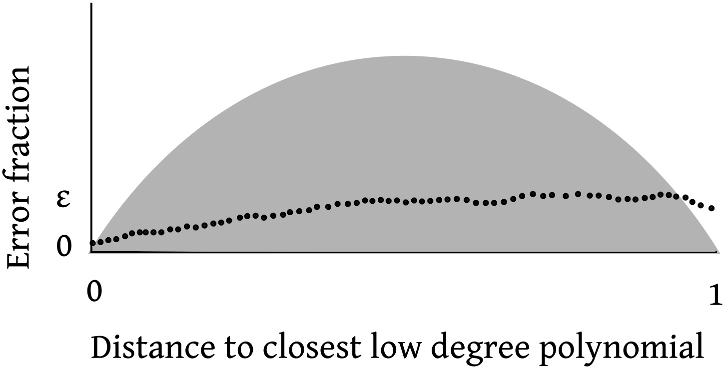

Error fraction
ε
0
0
1
Distance to closest low degree polynomial

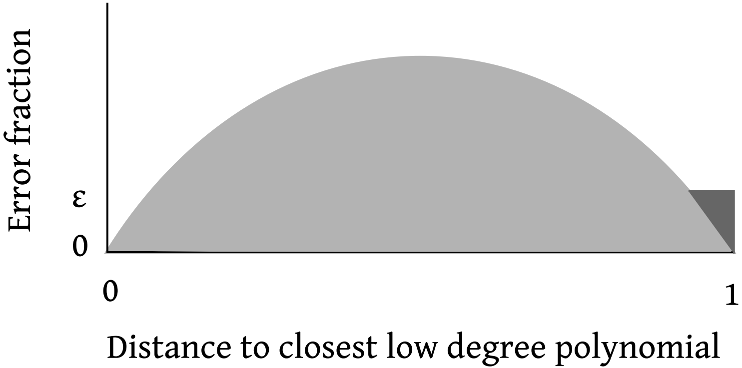

Error fraction
ε
0
0
1
Distance to closest low degree polynomial

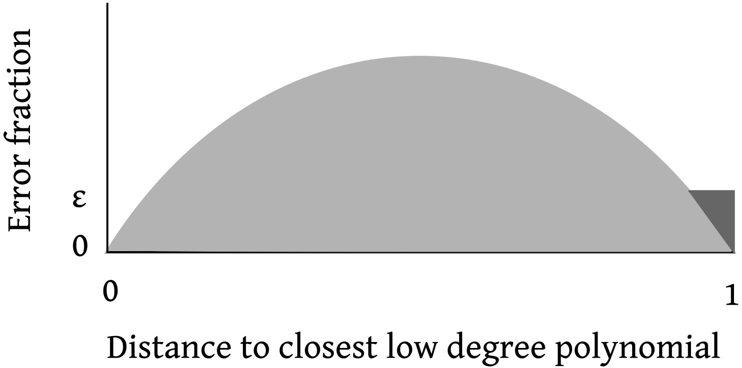

Error fraction
ε
0
0
1
Distance to closest low degree polynomial


Error fraction
ε
0
0
1
Distance to closest low degree polynomial


Error fraction
ε
0
0
1
Distance to closest low degree polynomial


Error fraction
ε
0
0
1
Distance to closest low degree polynomial


Error fraction
ε
0
0
1
Distance to closest low degree polynomial



Theorem

If the line test finds an error with probability less than ϵ, then $g : F^k \to \mathbb{R}$ is close to a low degree trigonometric polynomial.

Theorem (All details)

Let F be a finite field with q elements where q is a prime number. Let $d \in \mathbb{N}$, $h := 10^{15}$ and $k > 3h$ such that $q \geq 10^4(2hkd+1)^3$. There exists a probabilistic verification algorithm in the BSS-model of computation over the reals with the following properties:

- *The verifier gets as input a function value table of a multivariate function $f : F^k \to \mathbb{R}$ and a proof string π consisting of at most q^{2k} segments (blocks). Each segment consists of $2hkd + k + 1$ real components. Such a segment is seen as specifying a degree hkd polynomial by its coefficients and claiming that this is the restriction of f to the corresponding line.*
  The verifier first uniformly generates $O(k \cdot \log q)$ random bits; next, it uses the random bits to determine a point $x \in F^k$ together with one segment in the proof string it wants to read. Finally, using the values of $f(x)$ and those of the chosen segment it performs a line test. According to the outcome of the test the verifier either accepts or rejects the input.
  The running time of the verifier is polynomially bounded in the quantity $k \cdot \log q$, i.e., polylogarithmic in the input size $O(k \cdot q^{2k})$.
- *For every function value table representing a trigonometric max-degree d polynomial there exists a proof string such that the verifier accepts with probability 1.*
- *For any $0 < \epsilon < 10^{-19}$ and for every function value table whose distance to a closest max-degree $2hkd$ polynomial is at least 2ϵ the probability that the verifier rejects is at least ϵ, no matter what proof string is given.*

Further questions:

- What remains to be done in the proof of the $PCP_{\mathbb{R}}$ theorem?

Further questions:

- What remains to be done in the proof of the $\mathrm{PCP}_{\mathbb{R}}$ theorem?
  - segmentation procedure

Further questions:

- What remains to be done in the proof of the $\text{PCP}_{\mathbb{R}}$ theorem?
  - segmentation procedure
  - segmentable sum check

Further questions:

- What remains to be done in the proof of the $PCP_{\mathbb{R}}$ theorem?
  - segmentation procedure
  - segmentable sum check
- Is there a way to test algebraic polynomials while querying only a constant number of segments?

Further questions:

- What remains to be done in the proof of the $PCP_{\mathbb{R}}$ theorem?
  - segmentation procedure
  - segmentable sum check
- Is there a way to test algebraic polynomials while querying only a constant number of segments?
- Can the number of queries in the $PCP_{\mathbb{R}}$ theorem be reduced to a small number?