Low-degree Testing or Distance to Reed-Solomon Codes

Cdric Tavernier

Projet codes, INRIA Rocquencourt

B.P. 105, 78150 Le Chesnay, France

email : Cedric.Tavernier@inria.fr

Abstract

We consider the field $\mathbb{F}_q$. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ for which we only know a fraction of input and output. We suppose that q is large. We would like to give an answer to the following question: does there exist a polynomial of degree d which is very closed to the function f, and we would like to give an approximation of this distance, or equivalently, if we consider the smallest linear code of block length $q-1$ containing both $ev(f)$ and every codeword of the Reed-Solomon code $[q-1, d+1]_q$ we would like to give an approximation of the minimal distance between this last code and the Reed-Solomon code $[q-1, d+1]_q$.

1 Introduction, The Basic Univariate Test

We want to test whether f is a polynomial of total degree d. M. Kiwi [2] describe equivalent tests that achieve this goal. Let P_d denote the set of polynomials from $\mathbb{F}_q$ to $\mathbb{F}_q$ of total degree d, and $C_f(d)$ the smallest linear code of block length $q-1$ containing both $ev(f)$ and every codeword of the Reed-Solomon code $C(d) = [q-1, d+1]_q$, $C_f(d) \stackrel{def}{=} \{\phi ev(f) + \theta g \mid g \in C \text{ and } \phi, \theta \in \mathbb{F}_q\}$. Here is these equivalent tests.

- Basic Univariate Test [3]: Randomly pick $d+2$ distinct points $x_0, \ldots, x_{d+1}$ in $\mathbb{F}_q$. Then, accept if there exists a polynomial in P_d that agrees with f on $x_0, \ldots, x_{d+1}$, and reject otherwise.

- Basic Univariate Test: let $C(d)$ be the code whose elements are of the form $(p(x) : x \in \mathbb{F}_q)$ where p ranges over P_d. Randomly choose a dual codeword $\lambda \in C(d)^\perp$ of weight $d+2$. Then, accept if $\lambda \in C_f(d)^\perp$, and reject otherwise.

Recall that the minimal distance of a code C is the minimum weight of the codewords in C, and is denoted $\mathrm{wt}(C)$. We denote $\rho\mathrm{wt}(C)$ the relative minimum distance of a code C as the minimal distance of a code C divided by its block length. So if we denote $\Delta(f, P_d)$ the normalized distance, we see that $\Delta(f, P_d) = \rho\mathrm{wt}(C_f(d) \setminus C(d))$.

Theorem 1 *[3] Given a positive integer d, a finite field $\mathbb{F}_q$ of size at least $d+2$ and a function $f : \mathbb{F}_q \to \mathbb{F}_q$, if f satisfies*

$$Pr\left[\exists g \in \mathbb{F}_{2^n}^{(d)}[x] \text{ such that } g(x_i) = f(x_i)\ \forall i \in \{0, \ldots, d+1\}\right] \geq 1 - \delta,$$

where the probability is taken over the uniform distribution over all $d+2$-tuples $\{x_0, \ldots, x_{d+1}\}$ of distinct elements from $\mathbb{F}_q$, then $\Delta(f, P_d) \leq \delta$ thus $\rho wt(C_f(d) \setminus C(d)) \leq \delta$.

The testers above establish that univariate testing can be done in polynomial time (in d), and probes f in only $\mathcal{O}(d)$ places [3], but from the point of view of testing it is not very useful, since it is not very "different" from interpolation.

2 Test based on evenly spaced points over prime field

We now describe a tester which only works for fields of the form $\mathbb{F}_p$ for a prime p [3].

Definition 1 *We say that a set of points $\{x_0, \ldots, x_n\}$ is evenly spaced if $\exists h$ such that $x_i = x_0 + i * h$.*

Lemma 1 *Given a positive integer d and a prime $p \geq d+2$. The points $\{(x_i, y_i) | i \in \{0, \ldots, d+1\}; x_i = x + i * h; x_i, y_i \in \mathbb{F}_p\}$ lie on a degree d polynomial if and only if $\sum_{i=0}^{d+1} \alpha_i y_i = 0$, where $\alpha_i = (-1)^{(i+1)} \binom{d+1}{i}$.*

Theorem 2 *Given a positive integer d, a prime $p \geq d+2$ and a function $f : \mathbb{F}_p \to \mathbb{F}_p$ such that*

$$\underset{x,h \in \mathbb{F}_{2^n}}{P}\left[\sum_{i=0}^{d+1} \alpha_i \cdot f(x_i) = 0\right] \geq 1 - \delta \quad \text{where} \quad \delta \leq \frac{1}{2(d+2)^2},$$

then $\Delta(f, P_d) \leq 2\delta$, or equivalently $\rho wt(C_f(d) \setminus C(d)) \leq 2\delta$.

In particular, the bound above implies that the tester resulting from this theorem would need to probe f in $\mathcal{O}(d^3)$. We get the following Evenly-Spaced-Test:

Repeat $\mathcal{O}(d^2 \log(1/\beta))$ times

Pick $x, h \in \mathbb{F}_p \times \mathbb{F}_p$ and verify that $\sum_{i=0}^{d+1} \alpha_i \cdot f(x + i * h) = 0$

Reject if any of the test fails.

Theorem 3 *If the output of a program can be expressed by a low-degree polynomial correctly on all its inputs from $\mathbb{F}_p$, then it is passed by Evenly-Spaced-Test. If the output of the program is not $\mathcal{O}(\frac{1}{d^2})$-close to a univariate polynomial, then with probability $1-\beta$, it is rejected by Evenly-Spaced-Test.*

3 Evenly-Spaced-Test for Extension of Prime Fields

We now extend the last results to the field $\mathbb{F}_q = \mathbb{F}_{p^n}$. ω denote a primitive element of $\mathbb{F}_{p^n}$.

Definition 2 *We say that a set of distinct points $\{x_0, \ldots, x_n\}$ is regularly spaced if there exist $x, h, \omega \in \mathbb{F}_{p^n} \times \mathbb{F}^*_{p^n} \times \mathbb{F}^*_{p^n}$, such that $x_0 = x$ et $x_i = x + \omega^{i-1} * h$ pour $i \in \{1, \ldots, d+1\}$.*

Theorem 4 *Let d an integer such that $p^n > d+1$ and a function $f : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$. Let $\{x_0, \ldots, x_{d+1}\}$ a regularly-spaced set with $x_0 = x$ and $x_i = x + h \cdot \omega^{i-1}$. Let $y_i = f(x_i)$, $i \in \{0, \ldots, d+1\}$. The set of (x_i, y_i) lie on a degree at most d polynomial if and only if $\sum_{i=0}^{d+1} \alpha_i(\omega, d) \cdot y_i = 0$ where α_i are given by the following recurrence $B_1^0 = B_1^1 = 1$, $B_i^0 = B_{i-1}^0/\omega^{d-i+2}$, $B_i^i = B_{i-1}^{i-1}/(\omega^{i-1} - \omega^d)$ and $B_i^t = B_{i-1}^{t-1}/A_{i-1}^{t-1} - B_{i-1}^t/A_{i-1}^t$ where $A_i^t = \omega^{t-1} - \omega^{t+d-i}$ $t \in \{0, \ldots, i\}$, then $\alpha_t(\omega, d) = B_{d+1}^t$.*

Proof: By linearity we can consider that we test the polynomial X^d. For $j \in \{1, \ldots, d\}$ et $s \in \{1, \ldots, d-j+2\}$, we define the function $f^{(j)}(x_{s-1}, \ldots, x_{s+j-1}) = \frac{f^{(j-1)}(x_{s-1}, \ldots, x_{s+j-2}) - f^{(j-1)}(x_s, \ldots, x_{s+j-1})}{x_{s-1} - x_{s+j-1}}$ with $f^{(0)}(x_i) = f(x_i) = x_i^d$, $i \in \{0, \ldots, d+1\}$. We show this theorem by recurrence: If $j = 1$ we see that $f^{(j)}(x_{s-1}, x_s)$ is the sum of all monomial in x_{s-1}, x_s of degree $d-1$, we suppose that $f^{(j)}(x_{s-1}, \ldots, x_{s+j-1})$ is the sum of all monomial of degree $n-j$. Now at rank $j+1$, for any monomial $x_{s-1}^{i_{s-1}} x_s^{i_s} \ldots x_{s+j-1}^{i_{s+j-1}}$ of $f^{(j)}(x_{s-1}, \ldots, x_{s+j-1})$ we have the monomial $x_{s+j}^{i_{s-1}} x_s^{i_s} \ldots x_{s+j-1}^{i_{s+j-1}}$ of $f^{(j)}(x_{s-1}, \ldots, x_{s+j-1})$ with $i_{s-1} + \ldots + i_{s+j-1} = n-j$, and $x_{s-1}^{i_{s-1}} x_s^{i_s} \ldots x_{s+j-1}^{i_{s+j-1}} - x_{s+j}^{i_{s-1}} x_s^{i_s} \ldots x_{s+j-1}^{i_{s+j-1}} = (x_{s-1} - x_{s+j}) \cdot M_{s-1,s+j}^{i_{s-1}-1} \cdot x_s^{i_s} \ldots x_{s+j-1}^{i_{s+j-1}}$ where $M_{s-1,s+j}^{i_{s-1}-1}$ is the sum of all monomials of degree $i_{s-1} - 1$ in x_{s-1}, x_{s+j}, so we see that $M_{s-1,s+j}^{i_{s-1}-1} \cdot x_s^{i_s} \ldots x_{s+j-1}^{i_{s+j-1}}$

is a sum of monomial of degree $n-j-1$ in $x_s, \ldots, x_{s+j-1}$. We get that $f^{(j+1)}$ is the set of all monomials of degree $n-j-1$. Thus if f is a polynomial of degree at most d then $f^{(d+1)}(x_0, \ldots, x_{d+1}) = 0$ The construction of $f^{(j)}$ immediately gives the proof of the converse and states that there exists $\alpha_i(\omega, d)$ which never depends of h since $x_i - x_j = h \cdot (\omega^{i-1} - \omega^{j-1})$ and such that $\sum_{i=0}^{d+1} \alpha_i(\omega, d) \cdot y_i = 0$.

Theorem 5 *Given a positive integer d, a integer n such that $p^n \geq d+2$ and a function $f : \mathbb{F}_{p^n} \rightarrow \mathbb{F}_{p^n}$ such that*

$$\underset{x,h \in \mathbb{F}_{p^n}}{P} \left[\sum_{i=0}^{d+1} \alpha_i(\omega, d) \cdot f(x_i) = 0 \right] \geq 1 - \delta \quad \textit{ou} \quad \delta \leq \frac{1}{2(d+2)^2},$$

then $\Delta(f, P_d) \leq 2\delta$, or equivalently $\rho wt(C_f(d) \setminus C(d)) \leq 2\delta$.

4 Extending the tester to multivariate polynomials

Theorem 6 *Given a finite field $\mathbb{F}_q$, such that $q > md$ and a function $f : \mathbb{F}_q^m \rightarrow \mathbb{F}_q$ such that*

$$\underset{x,h \in \mathbb{F}_q^m}{P} \left[\sum_{i=0}^{d+1} \alpha_i(\omega, d) \cdot f(x_i) = 0 \right] \geq 1 - \delta \quad \textit{where} \quad \delta \leq \frac{1}{2(d+2)^2},$$

then $\Delta(f, P_d^n) \leq 2\delta$, or equivalently $\rho wt(C_f(d) \setminus C(d)) \leq 2\delta$. Here $C(d)$ denote the Reed-Muller code $R[d,m]_q$.

In conclusion we can say that the theorems 3 is true for these last cases and the proof is similar to Sudan's proof. Unfortunately These tests above are usefull only if the probability δ is very clothed to 0.

References

[1] T. Jakobsen. Cryptanalysis of block ciphers with probalistic non linear relations of low degree. In H. Krawczyk, editor, *Crypto'98*, number 1462 in LNCS, pages 347–362. Springer, 1998.

[2] M. Kiwi. Testing and weight distribution of dual codes. In *Technical Report TR-97-010*, 1997.

[3] M. Sudan. *Efficient Checking of Polynomial and proofs and the hardness of Approximation Problems*. PhD thesis, University of California, Berkeley, 1992.

[4] M. Sudan. Improved low degree testing and its application. In *Technical Report*, 1997.