Electronic Colloquium on Computational Complexity, Report No. 6 (2015)

Dense Testers: Almost Linear Time and Locally Explicit Constructions

Nader H. Bshouty
Department of Computer Science
Technion, Israel
bshouty@cs.technion.ac.il

January 6, 2015

Abstract

We develop a new notion called $(1-\epsilon)$-*tester for a set* $\mathcal{M}$ *of functions* $f:\mathcal{A}\to\mathcal{C}$. A $(1-\epsilon)$-tester for $\mathcal{M}$ maps each element $\boldsymbol{a}\in\mathcal{A}$ to a finite number of elements $B_{\boldsymbol{a}}=\{\boldsymbol{b}_1,\ldots,\boldsymbol{b}_t\}\subset\mathcal{B}$ in a smaller sub-domain $\mathcal{B}\subset\mathcal{A}$ where for every $f\in\mathcal{M}$ if $f(\boldsymbol{a})\neq 0$ then $f(\boldsymbol{b})\neq 0$ for at least $(1-\epsilon)$ fraction of the elements $\boldsymbol{b}$ of $B_{\boldsymbol{a}}$. I.e., if $f(\boldsymbol{a})\neq 0$ then $\mathbf{Pr}_{\boldsymbol{b}\in B_{\boldsymbol{a}}}[f(\boldsymbol{b})\neq 0]\geq 1-\epsilon$. The *size* of the $(1-\epsilon)$-tester is $\max_{\boldsymbol{a}\in\mathcal{A}}|B_{\boldsymbol{a}}|$. The goal is to minimize this size, construct $B_{\boldsymbol{a}}$ in deterministic almost linear time and access and compute each map in poly-log time.

We use tools from elementary algebra and algebraic function fields to build $(1-\epsilon)$-testers of small size in deterministic almost linear time. We also show that our constructions are locally explicit, i.e., one can find any entry in the construction in time poly-log in the size of the construction and the field size. We also prove lower bounds that show that the sizes of our testers and the densities are almost optimal.

Testers were used in [Bshouty, Testers and its application, ITCS 2014] to construct almost optimal perfect hash families, universal sets, cover-free families, separating hash functions, black box identity testing and hitting sets. The dense testers in this paper shows that such constructions can be done in almost linear time, are locally explicit and can be made to be dense.

ISSN 1433-8092

Contents

1 Introduction 4

2 Preliminary Definitions and Results 5

2.1 Multivariate Polynomial 5

2.1.1 Classes of Multivariate Polynomials 6

2.1.2 Multivariate Form 6

2.2 Algebraic Complexity 7

2.2.1 Complexity of Constructing Irreducible Polynomials and $\mathbb{F}_{q^t}$ 7

3 Dense Tester 8

3.1 Definition of $(1-\epsilon)$-Tester 9

3.2 Preliminary Results for Testers 10

3.3 Preliminary Results for Polynomials of Degree d 12

4 Lower Bounds 19

4.1 Lower Bound for the Size 19

4.2 Lower Bound on the Density 22

5 Constructions of Dense Testers 24

5.1 Dense Testers for Large Fields 24

5.2 Testers for Small Fields 33

6 Almost Linear Time Constructions and Locally Explicit 38

6.1 Dense Testers for Very Small t and Large q 38

6.2 Dense Testers for any t and Large q 42

6.3 Dense Testers for any t and Small q 44

7 Appendices 47

7.1 Appendix A 47

7.2 Appendix B 49

7.3 Appendix C 51

1 Introduction

A $(1-\epsilon)$-*tester* of a class of multivariate polynomials $\mathcal{M}$ over n variables is a set L of maps from a "complex" (algebraic) structure $\mathcal{A}^n$ (such as algebra over a field, algebraic function field, modules) to a "simple" algebraic structure (such as field or ring) $\mathcal{B}^n$ that for every $f \in \mathcal{M}$ preserve the property $f(\boldsymbol{a}) \neq 0$ for at least $(1-\epsilon)$ fraction of the maps, i.e., for all $f \in \mathcal{M}$ and $\boldsymbol{a} \in \mathcal{A}^n$ if $f(\boldsymbol{a}) \neq 0$ then $f(\ell(\boldsymbol{a})) \neq 0$ for at least $(1-\epsilon)$ fraction of the maps $\ell \in L$. See a formal definition in Section 2.

In this paper we study $(1-\epsilon)$-testers when $\mathcal{A}$, the domain of the functions in $\mathcal{M}$, is a field and $\mathcal{B} \subset \mathcal{A}$ is a small subfield. We use tools from elementary algebra and algebraic function fields to construct testers of almost optimal size $|L|$ in almost linear time.

A construction is *globally explicit* if it runs in deterministic polynomial time in the size of the construction and poly-log in the size of the field. A *locally explicit construction* is a construction where one can find any entry in the construction in deterministic poly-log time in the size of the construction and the size of the field. In particular, a locally explicit construction is also globally explicit. The constructions in this paper are locally explicit constructions and runs in almost linear time in the size of the construction.

We also give lower bounds that show that the size of our constructions and their densities are almost optimal.

One application of $(1-\epsilon)$-testers is the following: Suppose we need to construct a small set of vectors $S \subset \Sigma^n$ for some alphabet Σ that at least $(1-\epsilon)$ fraction of its elements satisfy some property P. We map Σ into a field $\mathbb{F}$ and find a set of functions $\mathcal{M}_P$ where $S \subset \mathbb{F}^n$ satisfies property P if and only if S is a hitting set for $\mathcal{M}_P$, i.e., for every $f \in \mathcal{M}_P$ there is $\boldsymbol{a} \in S$ such that $f(\boldsymbol{a}) \neq 0$. We then extend $\mathbb{F}$ to a larger field $\mathbb{K}$ (or $\mathbb{F}$-algebra $\mathcal{A}$). Find $S' \subset \mathbb{K}^n$ that is a hitting set of density $(1-\epsilon_1)$ for $\mathcal{M}_P$ (which supposed to be easier). Then use $(1-(\epsilon-\epsilon_1))$-tester to change the hitting set $S' \subset \mathbb{K}^n$ over $\mathbb{K}$ to a hitting set $S \subset \mathbb{F}^n$ over $\mathbb{F}$ of density $(1-\epsilon)$.

Non-dense Testers were first studied in [3]. They were used to give a polynomial time constructions of almost optimal perfect hash families, universal sets, cover-free families, separating hash functions, black box identity testing and hitting sets. Dense Testers were first mentioned in [3] (see section 7 conclusion and future work) where the application for new pseudorandom generators are also mentioned as one of our future work. In [8], Guruswami and Xing, independently, used the same technique for similar construction. The results in this paper show that all the constructions in [3] can be constructed in almost linear time, are locally explicit and can be changed to be dense.

In this paper we consider two main classes of multivariate polynomials over finite fields $\mathbb{F}_q$ with q elements. The first class is $\mathcal{P}(\mathbb{F}_q, n, d)$, the class of all multivariate polynomials with n variables and total degree d. The second class is $\mathcal{HLF}(\mathbb{F}_q, n, d)$, the class of multilinear forms of degree d. That is, the set of all multivariate polynomials f with dn variables $x_{i,j}$, $i = 1, \ldots, d$, $j = 1, \ldots, n$ where each monomial in f is of the form $x_{1,i_1}x_{2,i_2}\cdots x_{d,i_d}$. All the constructions in [3] are based on testers for the above two classes.

In Section 2 we give some preliminary results. In Section 3 we give the definition of dense tester and prove some preliminary results for dense testers. In Section 4 we give lower bounds for the size of dense testers and for their density. In Section 5 we give the (non-polynomial time) constructions of dense testers. The almost linear time locally explicit constructions are given in Section 6. In Subsection 6.1 and 6.2 we give constructions of dense testers for $\mathcal{P}(\mathbb{F}_q,n,d)$, $q\ge d+1$, from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ with optimal density of size within a factor of $poly(d/\epsilon)$ of the optimal size. In [3] we show that no such tester exists when $q\le d$. In Subsection 6.3 we give constructions of dense testers for $\mathcal{HLF}(\mathbb{F}_q,n,d)$, from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ for any q.

2 Preliminary Definitions and Results

In this section we give some definitions and results from the literature that will be used throughout the paper

2.1 Multivariate Polynomial

In this section we define the set of multivariate polynomials over a field $\mathbb{F}$.

Let $\mathbb{F}$ be a field and $\boldsymbol{x}=(x_1,\ldots,x_n)$ be indeterminates (or variables) over the field $\mathbb{F}$. The ring of *multivariate polynomials* in the indeterminates $x_1,\ldots,x_n$ over $\mathbb{F}$ is $\mathbb{F}[x_1,\ldots,x_n]$ (or $\mathbb{F}[\boldsymbol{x}]$). Let $\boldsymbol{i}=(i_1,\ldots,i_n)\in\mathbb{N}^n$. We denote by $\boldsymbol{x}^{\boldsymbol{i}}$ the *monomial* $x_1^{i_1}\cdots x_n^{i_n}$. Every multivariate polynomial f in $\mathbb{F}[\boldsymbol{x}]$ can be represented as

$$f(\boldsymbol{x})=\sum_{\boldsymbol{i}\in I}a_{\boldsymbol{i}}\boldsymbol{x}^{\boldsymbol{i}} \tag{1}$$

for some finite set $I\subset\mathbb{N}^n$ and $a_{\boldsymbol{i}}\in\mathbb{F}\backslash\{0\}$ for all $\boldsymbol{i}\in I$.

When the field $\mathbb{F}$ is infinite, the representation in (1) is unique. Not every function $f':\mathbb{F}^n\to\mathbb{F}$ can be represented as multivariate polynomial. Take for example a function $f'(x_1)$ with one variable that has infinite number of roots.

When the field $\mathbb{F}$ is finite, then using, for example, Lagrange interpolation, every function $f':\mathbb{F}^n\to\mathbb{F}$ can be represented as multivariate polynomial $f\in\mathbb{F}[\boldsymbol{x}]$. There may be many representations for the same function $f':\mathbb{F}^n\to\mathbb{F}$ but a unique one that satisfies $I\subseteq\{0,1,\ldots,|\mathbb{F}|-1\}^n$. This follows from the fact that $x^{|\mathbb{F}|}=x$ in $\mathbb{F}$. We denote this unique representation by $R(f')$ and denote f' by $F(f)$. In this paper, functions and their representations in $\mathbb{F}[\boldsymbol{x}]$ are used exchangeably. So by $R(f)$ we mean $R(F(f))$.

For a monomial M when we say that M is a *monomial in* f we mean that $R(M)$ is a monomial that appears in $R(f)$. The constant $a_{\boldsymbol{i}}\in\mathbb{F}\backslash\{0\}$ in (1) is called the *coefficient* of the monomial $\boldsymbol{x}^{\boldsymbol{i}}$ in f and it is the coefficient of $R(\boldsymbol{x}^{\boldsymbol{i}})$ in $R(f)$. When $\boldsymbol{x}^{\boldsymbol{i}}$ is not a monomial in f then we say that its coefficient is 0.

The *degree*, $\deg(M)$, of a monomial $M = \boldsymbol{x}^{\boldsymbol{i}}$ is $i_1 + i_2 + \cdots + i_n$. The *degree of* x_j *in* M, $\deg_{x_j}(M)$ is i_j. Therefore,

$$\deg(M) = \sum_{i=1}^{n} \deg_{x_i}(M).$$

Let $f \in \mathbb{F}[\boldsymbol{x}]$ and let $g = R(f)$. The *degree* (or *total degree*) $\deg(f)$ is the maximum degree of the monomials in g. The degree of x_i in f, $\deg_{x_i}(f)$, is the maximum degree of x_i in the monomials in g, i.e., the degree of g when written as a univariate polynomial in the variable x_i. The *variable degree* of f is the maximum over the degree of each variable in f, i.e., $\max_i \deg_{x_i}(f)$. The size of f, size(f), is the number of monomials in g.

2.1.1 Classes of Multivariate Polynomials

In this section we define classes of multivariate polynomials that will be studied in the sequel.

We first define

1. $\mathcal{P}(\mathbb{F}, n)$ is the class of all multivariate polynomials in $\mathbb{F}[x_1, \ldots, x_n]$ of variable degree at most $|\mathbb{F}| - 1$. When $\mathbb{F}$ is finite, every functions $f : \mathbb{F}^n \to \mathbb{F}$ can be represented by some multivariate polynomial in $\mathcal{P}(\mathbb{F}, n)$. When $\mathbb{F}$ is infinite $\mathcal{P}(\mathbb{F}, n) = \mathbb{F}[x_1, \ldots, x_n]$.
2. $\mathcal{P}(\mathbb{F}, n, (d, r))$ is the class of all multivariate polynomials in $\mathcal{P}(\mathbb{F}, n)$ of degree at most d and variable degree at most r.
3. $\mathcal{P}(\mathbb{F}, n, d) = \mathcal{P}(\mathbb{F}, n, (d, |\mathbb{F}| - 1))$ is the class of all multivariate polynomials in $\mathcal{P}(\mathbb{F}, n)$ of degree at most d.
4. $\mathcal{HP}(\mathbb{F}, n)$ is the class of all homogeneous polynomials in $\mathcal{P}(\mathbb{F}, n)$. A multivariate polynomial is called *homogeneous multivariate polynomial* if all its monomials have the same degree. In the same way as above one can define $\mathcal{HP}(\mathbb{F}, n, (d, r))$ and $\mathcal{HP}(\mathbb{F}, n, d)$.

2.1.2 Multivariate Form

Let $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ where $\boldsymbol{y}_i = (y_{i,1}, \ldots, y_{i,n})$ are indeterminates over $\mathbb{F}$ for $i = 1, \ldots, m$. A *multivariate form* in $\boldsymbol{y}$ is a multivariate polynomial in $\boldsymbol{y}$. That is, an element of

$$\mathbb{F}[y_{1,1}, \ldots, y_{1,n}, \ldots, y_{m,1}, \ldots, y_{m,n}].$$

We denote this class by $\mathbb{F}[\boldsymbol{y}]$ or $\mathbb{F}[\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m]$. Let $\mathcal{HLF}(\mathbb{F}, n, m)$ be the class of all multilinear forms f over $\boldsymbol{y} = (\boldsymbol{y}_1, \ldots, \boldsymbol{y}_m)$ where each monomial in f contains exactly one variable from $\boldsymbol{y}_i$ for every i. In [3], polynomials in $\mathcal{HLF}(\mathbb{F}, n, m)$ are called (n, m)-*multilinear polynomials.* Notice that $\mathcal{HLF}(\mathbb{F}, n, 2)$ is the class of bilinear forms $\boldsymbol{y}_1^T A \boldsymbol{y}_2$ where $A \in \mathbb{F}^{n \times n}$.

2.2 Algebraic Complexity

In this section we give some known results in algebraic complexity that will be used in the sequel

2.2.1 Complexity of Constructing Irreducible Polynomials and $\mathbb{F}_{q^t}$

In some applications the construction of irreducible polynomials of degree n over $\mathbb{F}_q$ and the construction of the field $\mathbb{F}_{q^t}$ is also needed and their complexity must be included in the overall time complexity of the problem.

To construct the field $\mathbb{F}_{q^t}$ one should construct an irreducible polynomial $f(x)$ of degree t in $\mathbb{F}_q[x]$ and then use the representation $\mathbb{F}_{q^t} = \mathbb{F}_q[x]/(f(x))$. For a comprehensive survey on this problem see [14] Chapter 3. See also [1, 5, 13]. We give here the results that will be used in this paper.

Lemma 1. *Let $\mathbb{F}_q$ be a field of characteristic p. There is an algorithm that constructs an irreducible polynomial of degree t with T arithmetic operations in the field $\mathbb{F}_q$ where T is as described in the following table.*

Type	**Field**	**Assumption**	*Time* $= T$	$T = \tilde{O}$
Probabilistic	*Any*	–	$O\left(t^2 \log^{2+\epsilon} t + t \log q \log^{1+\epsilon} t\right)$	$\tilde{O}(t^2)$
Deterministic	*Any*	–	$O\left(p^{1/2+\epsilon} t^{3+\epsilon} + (\log q)^{2+\epsilon} t^{4+\epsilon}\right)$	$\tilde{O}(p^{1/2} t^3 + t^4)$
Deterministic	*Any*	*ERH*	$O(\log^2 q + t^{4+\epsilon} \log q)$	$\tilde{O}(t^4)$
Deterministic	$\mathbb{F}_2$	–	$O(t^{3+\epsilon})$	$\tilde{O}(t^3)$

Here ERH stands for the Extended Riemann Hypothesis and ϵ is any small constant.

Here $\tilde{O}(M)$ means $O(M \cdot t^\epsilon \cdot poly(\log q))$. In the sequel when we give a complexity for constructing a field or irreducible polynomial then $\tilde{O}(M)$ means $O(M \cdot t^\epsilon \cdot poly(\log M, \log q))$ but for all the constructions in this paper $\tilde{O}(M)$ will mean $O(M \cdot poly(\log M, \log q))$.

In Lemma 14 one should construct many irreducible polynomials of certain degree. We now prove the following result

Lemma 2. *There is a deterministic algorithm that runs in time*

$$\tilde{O}(mt + t^3 p^{1/2} + t^4)$$

(and $\tilde{O}(mt + t^4)$ assuming ERH) and construct m distinct irreducible polynomials of degree t in $\mathbb{F}_q[x]$ and their roots.

Proof. By Lemma 1, $\mathbb{F}_{q^t}$ can be constructed in time $O\left(t^{3+\epsilon} p^{1/2+\epsilon} + (\log q)^{2+\epsilon} t^{4+\epsilon}\right)$. It is known that a normal basis $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{t-1}}\}$ in $\mathbb{F}_{q^t}$ can be constructed in time $O(t^3 + t \log t \log\log t \log q)$, [9, 11].

For any $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_t) \in \mathbb{F}_q^t$, the element

$$\beta_{\boldsymbol{\lambda}} := \lambda_1 \alpha + \lambda_2 \alpha^q + \lambda_3 \alpha^q + \cdots + \lambda_{t-1} \alpha^{q^{t-1}}$$

is a root of an irreducible polynomial of degree t if and only if $\beta_{\boldsymbol{\lambda}}, \beta_{\boldsymbol{\lambda}}^q, \beta_{\boldsymbol{\lambda}}^{q^2}, \ldots, \beta_{\boldsymbol{\lambda}}^{q^{t-1}}$ are distinct. It is easy to see that this is true if and only if the vectors

$$\boldsymbol{\lambda}^0 := \boldsymbol{\lambda},\ \boldsymbol{\lambda}^1 := (\lambda_t, \lambda_1, \ldots, \lambda_{t-1}),\ \boldsymbol{\lambda}^2 := (\lambda_{t-1}, \lambda_t, \lambda_1, \ldots, \lambda_{t-2}), \cdots, \boldsymbol{\lambda}^{t-1} := (\lambda_2, \lambda_3, \ldots, \lambda_t, \lambda_1)$$

are distinct. Such $\boldsymbol{\lambda}$ is called a vector of period t.

If we have a vector $\boldsymbol{\lambda}$ of period t then $\beta_{\boldsymbol{\lambda}}$ is a root of irreducible polynomial $f_{\beta_{\boldsymbol{\lambda}}}(x)$ of degree t where $f_{\beta_{\boldsymbol{\lambda}}}(x) \equiv (x - \beta_{\boldsymbol{\lambda}})(x - \beta_{\boldsymbol{\lambda}}^q) \cdots (x - \beta_{\boldsymbol{\lambda}}^{q^{t-1}})$. The coefficients of the polynomial $f_{\beta_{\boldsymbol{\lambda}}}(x)$ can be computed in time $O(t \log^2 t \log\log t)$. See Theorem A in [14] and references within. Therefore, it remains to construct m vectors of period t.

Now choose any total order $<$ on $\mathbb{F}_q$ and consider the lexicographic order in $\mathbb{F}_q^t$ with respect to $<$ and consider the sequence of all the elements of $\mathbb{F}_q^t$ with this order. It is easy to see that for any two consecutive elements $\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \in \mathbb{F}_q^t$ in this sequence there is at least one $\boldsymbol{\lambda}_i$, $i \in \{1, 2\}$ of period t. Also, each irreducible polynomial $f_{\beta_{\boldsymbol{\lambda}}}$ of degree t can be constructed by exactly t elements (i.e., $\boldsymbol{\lambda}^0, \boldsymbol{\lambda}^1, \ldots, \boldsymbol{\lambda}^{t-1}$) in the sequence. This implies that the first $2tm$ elements in this sequence generate at least m distinct irreducible polynomials. □

The following result will be used for the local explicit constructions and is proved in Appendix A.

Lemma 3. *Let $r = \lfloor q^{t-2}/2t \rfloor$. There is a total order on a set of r irreducible polynomials of degree t in $\mathbb{F}_q[x]$ and a deterministic algorithm that with an input m runs in time*

$$\tilde{O}(t^3 p^{1/2} + t^4)$$

and constructs the mth irreducible polynomial in that order with its roots.

The time is $\tilde{O}(t^4)$ assuming ERH.

Throughout this paper, the complexities are given without the assumption of ERH. When ERH is assumed then just drop the $p^{1/2}$ from the complexities.

3 Dense Tester

In this section we define $(1 - \epsilon)$-testers and give some preliminary results.

3.1 Definition of $(1-\epsilon)$-Tester

In this section we define $(1-\epsilon)$-tester. We will assume that all the $\mathbb{F}$-algebras in this paper are commutative, although most of the results are also true for noncommutative $\mathbb{F}$-algebras.

Let $\mathbb{F}$ be a field and $\mathcal{A}$ and $\mathcal{B}$ be two $\mathbb{F}$-algebras. Let $0 \le \epsilon < 1$ and $\overline{\epsilon} = 1-\epsilon$. Let $\mathcal{M} \subseteq \mathbb{F}[x_1, x_2, \ldots, x_n]$ be a class of multivariate polynomial. Let $S \subseteq \mathcal{A}$ and $R \subseteq \mathcal{B}$ be linear subspaces over $\mathbb{F}$ and $L = \{\boldsymbol{l}_1, \ldots, \boldsymbol{l}_\nu\}$ be a set of (not necessarily linear) maps $\boldsymbol{l}_i : S^n \to R^n$, $i = 1, \ldots, \nu$. We say that L is $(\mathcal{M}, S, R)$-$\overline{\epsilon}$-*tester* if for every $\boldsymbol{a} = (a_1, \ldots, a_n) \in S^n$ and $f \in \mathcal{M}$ we have

$$f(\boldsymbol{a}) \neq 0 \implies \mathbf{Pr}_{\boldsymbol{l}\in L}[f(\boldsymbol{l}(\boldsymbol{a})) \neq 0] \ge \overline{\epsilon}$$

where the probability is uniform over the choices of $\boldsymbol{l} \in L$.

The integer $\nu = |L|$ is called the *size of the* $\overline{\epsilon}$*-tester*. The minimum size of such tester is denoted by $\nu_R^\circ(\mathcal{M}, S, \overline{\epsilon})$. If no such tester exists then we write $\nu_R^\circ(\mathcal{M}, S, \overline{\epsilon}) = \infty$. When S and R are known from the context we then just say that L is $\overline{\epsilon}$*-tester for* $\mathcal{M}$.

An $(\mathcal{M}, S, R)$*-tester* is an $(\mathcal{M}, S, R)$-$\overline{\epsilon}$-tester for some $\epsilon < 1$. Tester was studied in [3]. The minimum size of an $(\mathcal{M}, S, R)$-tester is denoted by $\nu_R^\circ(\mathcal{M}, S)$. Obviously we have

$$\nu_R^\circ\left(\mathcal{M}, S, \frac{1}{\nu_R^\circ(\mathcal{M}, S)}\right) = \nu_R^\circ(\mathcal{M}, S). \qquad (2)$$

Obviously, L is an $(\mathcal{M}, S, R)$-$\overline{\epsilon}$-*tester* if and only if for every $L' \subseteq L$ where $|L'| = \lfloor \epsilon |L| \rfloor + 1$, L' is $(\mathcal{M}, S, R)$*-tester.*

We say that the $\overline{\epsilon}$-tester L is *componentwise* if for every $\boldsymbol{l}_i \in L$ we have $\boldsymbol{l}_i(\boldsymbol{a}) = (l_{i,1}(a_1), \ldots, l_{i,n}(a_n))$ for some $l_{i,j} : S \to R$. A componentwise tester is called *linear* if each $l_{i,j}$ is a linear map and is called *reducible* if $\mathcal{A}$ and $\mathcal{B}$ has identity elements $1_\mathcal{A}$ and $1_\mathcal{B}$, respectively, $1_\mathcal{A} \in S$ and $l_{i,j}(1_\mathcal{A}) = 1_\mathcal{B}$ for all $l_{i,j}$.

We will also allow $L = \{l_1, \ldots, l_\nu\}$ to be a set of maps $l_i : S \to R$, for $i = 1, \ldots, \nu$ (rather than maps $S^n \to R^n$). In that case $\boldsymbol{l}_i : S^n \to R^n$ is defined as $\boldsymbol{l}_i(\boldsymbol{a}) = (l_i(a_1), \ldots, l_i(a_n))$ where $\boldsymbol{a} = (a_1, \ldots, a_n) \in S^n$. In such case we call the $\overline{\epsilon}$-tester a *symmetric* $\overline{\epsilon}$*-tester.*

In this paper we will mainly study $\overline{\epsilon}$-testers for the class of multilinear forms of degree d and multivariate polynomials of degree d.

We will use the following abbreviations

The Expression	Abbreviation	or the Abbreviation
$\nu_R^\circ(\mathcal{P}(\mathbb{F}, n, d), S, \overline{\epsilon})$	$\nu_R^{\mathcal{P}}(d, S, \overline{\epsilon})$	$\nu_R^{\mathcal{P}}((d, \mathbb{F}), S, \overline{\epsilon})$
$\nu_R^\circ(\mathcal{HP}(\mathbb{F}, n, d), S, \overline{\epsilon})$	$\nu_R^{\mathcal{HP}}(d, S, \overline{\epsilon})$	$\nu_R^{\mathcal{HP}}((d, \mathbb{F}), S, \overline{\epsilon})$
$\nu_R^\circ(\mathcal{HLF}(\mathbb{F}, n, m), S, \overline{\epsilon})$	$\nu_R(m, S, \overline{\epsilon})$	$\nu_R((m, \mathbb{F}), S, \overline{\epsilon})$

In the abbreviations $\nu_R^{\mathcal{P}}(d,S,\bar\epsilon)$, (respectively, $\nu_R^{\mathcal{HP}}(d,S,\bar\epsilon)$ and $\nu_R(m,S,\bar\epsilon)$) we assume that the ground field $\mathbb{F}$ is known from the context, e.g., when $R=\mathbb{F}$. Otherwise, we write $\nu_R^{\mathcal{P}}((d,\mathbb{F}),S,\bar\epsilon)$, (respectively, $\nu_R^{\mathcal{HP}}((d,\mathbb{F}),S,\bar\epsilon)$ and $\nu_R((m,\mathbb{F}),S,\bar\epsilon)$)

Notice that we omitted the parameter n from the abbreviation. This is because, for the classes we will study here, the value of ν_R° is monotone non-decreasing in n and we are interested in the worst case size of such testers. So one can define $\nu_R^{\mathcal{P}}(d,S,\bar\epsilon)=\lim_{n\to\infty}\nu_R^{\mathcal{P}}(\mathcal{P}(\mathbb{F},n,d),S,\bar\epsilon)$.

3.2 Preliminary Results for Testers

In this section we prove some preliminary results on $\bar\epsilon$-testers that will be frequently used in the sequel.

The first two Lemmas follows from the definition of $\bar\epsilon$-tester

Lemma 4. *Let $\mathcal{A}$ and $\mathcal{B}$ be commutative $\mathbb{F}$-algebras. Let $S_1\subseteq S_2\subseteq\mathcal{A}$, $R_2\subseteq R_1\subseteq\mathcal{B}$ be linear subspaces over $\mathbb{F}$, $\mathcal{N}\subseteq\mathcal{M}\subseteq\mathbb{F}[x_1,\ldots,x_n]$ and $\epsilon_1\ge\epsilon_2$. If L is $(\mathcal{M},S_2,R_2)$-$\bar\epsilon_2$-tester then it is $(\mathcal{N},S_1,R_1)$-$\bar\epsilon_1$-tester. In particular,*

$$\nu_{R_1}^\circ(\mathcal{N},S_1,\bar\epsilon_1)\le\nu_{R_2}^\circ(\mathcal{M},S_2,\bar\epsilon_2).$$

Lemma 5. *Let $\mathcal{A},\mathcal{B}$ and $\mathcal{C}$ be commutative $\mathbb{F}$-algebras. Let $S_1\subseteq\mathcal{A}$, $S_2\subseteq\mathcal{B}$ and $S_3\subseteq\mathcal{C}$ be linear subspaces over $\mathbb{F}$ and $\mathcal{M}\subseteq\mathbb{F}[x_1,\ldots,x_n]$. If L_1 is a $(\mathcal{M},S_1,S_2)$-$\bar\epsilon_1$-tester and L_2 is a $(\mathcal{M},S_2,S_3)$-$\bar\epsilon_2$-tester then $L_2\circ L_1:=\{\boldsymbol{l}_2(\boldsymbol{l}_1)\mid\boldsymbol{l}_1\in L_1,\boldsymbol{l}_2\in L_2\}$ is $(\mathcal{M},S_1,S_3)$-$(\bar\epsilon_1\bar\epsilon_2)$-tester. In particular,*

$$\nu_{S_3}^\circ(\mathcal{M},S_1,\bar\epsilon_1\bar\epsilon_2)\le\nu_{S_3}^\circ(\mathcal{M},S_2,\bar\epsilon_1)\cdot\nu_{S_2}^\circ(\mathcal{M},S_1,\bar\epsilon_2).$$

In particular we have

Corollary 6. *Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ and $\mathcal{A}$ be a $\mathbb{K}$-algebra. Let $\mathcal{M}\subseteq\mathbb{F}[x_1,\ldots,x_n]$. Then*

$$\nu_{\mathbb{F}}^\circ(\mathcal{M},\mathcal{A},\bar\epsilon_1\bar\epsilon_2)\le\nu_{\mathbb{F}}^\circ(\mathcal{M},\mathbb{K},\bar\epsilon_1)\cdot\nu_{\mathbb{K}}^\circ(\mathcal{M},\mathcal{A},\bar\epsilon_2).$$

In particular, for any integers m_1 and m_2 we have

$$\nu_{\mathbb{F}_q}^\circ(\mathcal{M},\mathbb{F}_{q^{m_1m_2}},\bar\epsilon_1\bar\epsilon_2)\le\nu_{\mathbb{F}_q}^\circ(\mathcal{M},\mathbb{F}_{q^{m_1}},\bar\epsilon_1)\cdot\nu_{\mathbb{F}_{q^{m_1}}}^\circ(\mathcal{M},\mathbb{F}_{q^{m_1m_2}},\bar\epsilon_2).$$

The above results are also true for componentwise, linear, reducible (assuming 1 is in all the sets) and symmetric $\bar\epsilon$-testers. We state this in the following

Lemma 7. *The results in Lemma 4, Lemma 5 and Corollary 6 are also true for componentwise, linear, reducible and symmetric $\bar\epsilon$-tester.*

Since $\epsilon_1+\epsilon_2 \ge \overline{\overline{\epsilon}_1\overline{\epsilon}_2}$, by Lemma 4, 5 and Corollary 6 we also have

$$\nu^\circ_{S_3}(\mathcal{M},S_1,\overline{\epsilon_1+\epsilon_2}) \le \nu^\circ_{S_3}(\mathcal{M},S_2,\overline{\epsilon}_1)\cdot \nu^\circ_{S_2}(\mathcal{M},S_1,\overline{\epsilon}_2), \tag{3}$$

$$\nu^\circ_{\mathbb{F}}(\mathcal{M},\mathcal{A},\overline{\epsilon_1+\epsilon_2}) \le \nu^\circ_{\mathbb{F}}(\mathcal{M},\mathbb{K},\overline{\epsilon}_1)\cdot \nu^\circ_{\mathbb{K}}(\mathcal{M},\mathcal{A},\overline{\epsilon}_2) \tag{4}$$

and

$$\nu^\circ_{\mathbb{F}_q}(\mathcal{M},\mathbb{F}_{q^{m_1m_2}},\overline{\epsilon_1+\epsilon_2}) \le \nu^\circ_{\mathbb{F}_q}(\mathcal{M},\mathbb{F}_{q^{m_1}},\overline{\epsilon}_1)\cdot \nu^\circ_{\mathbb{F}_{q^{m_1}}}(\mathcal{M},\mathbb{F}_{q^{m_1m_2}},\overline{\epsilon}_2). \tag{5}$$

We now prove

Lemma 8. *Let $\mathcal{A}$ be a commutative $\mathbb{F}$-algebra and $S\subseteq\mathcal{A}$ be a linear subspace over $\mathbb{F}$. Let*

$$\mathcal{M}\subseteq \mathbb{F}[\boldsymbol{x}]\mathbb{F}[\boldsymbol{y}] := \left\{ \sum_{i=1}^s h_i(\boldsymbol{x})g_i(\boldsymbol{y}) \;\middle|\; h_i\in\mathbb{F}[\boldsymbol{x}], g_i\in\mathbb{F}[\boldsymbol{y}], s\in\mathbb{N}\right\}$$

be a set of multivariate polynomials where $\boldsymbol{x}=(x_1,\ldots,x_n)$ and $\boldsymbol{y}=(y_1,\ldots,y_m)$ are distinct indeterminates. Let

$$\mathcal{M}_{\boldsymbol{x}} = \left\{ \sum_{i=1}^s \lambda_i h_i(\boldsymbol{x}) \;\middle|\; \sum_{i=1}^s h_i(\boldsymbol{x})g_i(\boldsymbol{y})\in\mathcal{M},\ \boldsymbol{\lambda}\in\mathbb{F}^s, s\in\mathbb{N}\right\}$$

and

$$\mathcal{M}_{\boldsymbol{y}} = \left\{ \sum_{i=1}^s \lambda_i g_i(\boldsymbol{y}) \;\middle|\; \sum_{i=1}^s h_i(\boldsymbol{x})g_i(\boldsymbol{y})\in\mathcal{M},\ \boldsymbol{\lambda}\in\mathbb{F}^s, s\in\mathbb{N}\right\}.$$

If $L_{\boldsymbol{x}}$ is a $(\mathcal{M}_{\boldsymbol{x}},S,\mathbb{F})$-$\overline{\epsilon}_{\boldsymbol{x}}$-tester and $L_{\boldsymbol{y}}$ is a $(\mathcal{M}_{\boldsymbol{y}},S,\mathbb{F})$-$\overline{\epsilon}_{\boldsymbol{y}}$-tester then $L_{\boldsymbol{x}}\times L_{\boldsymbol{y}}$ is a $(\mathcal{M},S,\mathbb{F})$-$(\overline{\epsilon}_{\boldsymbol{x}}\overline{\epsilon}_{\boldsymbol{y}})$-tester. In particular,

$$\nu^\circ_{\mathbb{F}}(\mathcal{M},S,\overline{\epsilon}_{\boldsymbol{x}}\overline{\epsilon}_{\boldsymbol{y}}) \le \nu^\circ_{\mathbb{F}}(\mathcal{M}_{\boldsymbol{x}},S,\overline{\epsilon}_{\boldsymbol{x}})\cdot \nu^\circ_{\mathbb{F}}(\mathcal{M}_{\boldsymbol{y}},S,\overline{\epsilon}_{\boldsymbol{y}}).$$

Proof. Suppose for some $f(\boldsymbol{x},\boldsymbol{y})=\sum_{i=1}^s h_i(\boldsymbol{x})g_i(\boldsymbol{y})\in\mathcal{M}$ and $(\boldsymbol{a},\boldsymbol{b})\in S^{n+m}$ we have

$$\mathbf{Pr}_{(\boldsymbol{l_x},\boldsymbol{l_y})\in L_{\boldsymbol{x}}\times L_{\boldsymbol{y}}}\left[f(\boldsymbol{l_x}(\boldsymbol{a}),\boldsymbol{l_y}(\boldsymbol{b}))\ne 0\right] < \overline{\epsilon}_{\boldsymbol{x}}\overline{\epsilon}_{\boldsymbol{y}}.$$

By Markov bound we have that more than $\epsilon_{\boldsymbol{x}}|L_{\boldsymbol{x}}|$ of the elements $\boldsymbol{l_x}\in L_{\boldsymbol{x}}$ satisfies

$$\mathbf{Pr}_{\boldsymbol{l_y}\in L_{\boldsymbol{y}}}\left[f(\boldsymbol{l_x}(\boldsymbol{a}),\boldsymbol{l_y}(\boldsymbol{b}))\ne 0\right] < \overline{\epsilon}_{\boldsymbol{y}}.$$

Since $f(\boldsymbol{l_x}(\boldsymbol{a}),\boldsymbol{y})\in\mathcal{M}_{\boldsymbol{y}}$ and $L_{\boldsymbol{y}}$ is an $(\mathcal{M}_{\boldsymbol{y}},S,\mathbb{F})$-$\overline{\epsilon}_{\boldsymbol{y}}$-tester it follows that for more than $\epsilon_{\boldsymbol{x}}|L_{\boldsymbol{x}}|$ of the elements $\boldsymbol{l_x}\in L_{\boldsymbol{x}}$ we have $f(\boldsymbol{l_x}(\boldsymbol{a}),\boldsymbol{b})=0$. Let ℓ be any linear map in $\mathcal{A}^*$. Then for more than $\epsilon_{\boldsymbol{x}}|L_{\boldsymbol{x}}|$ of the elements $\boldsymbol{l_x}\in L_{\boldsymbol{x}}$ we have

$$\sum_{i=1}^s h_i(\boldsymbol{l_x}(\boldsymbol{a}))\ell(g_i(\boldsymbol{b})) = \ell(f(\boldsymbol{l_x}(\boldsymbol{a})),\boldsymbol{b}))=0.$$

Since $\sum_{i=1}^s h_i(\boldsymbol{x})\ell(g_i(\boldsymbol{b})) \in \mathcal{M}_{\boldsymbol{x}}$ and $L_{\boldsymbol{x}}$ is an $(\mathcal{M}_{\boldsymbol{x}}, S, \mathbb{F})$-$\bar{\epsilon}_{\boldsymbol{x}}$-tester we have $\sum_{i=1}^s h_i(\boldsymbol{a})\ell(g_i(\boldsymbol{b})) = 0$. Notice that this is true for any linear map $\ell \in \mathcal{A}^*$. Now let $\{\omega_1, \ldots, \omega_r\} \subset \mathcal{A}$ be a basis for Span $_{\mathbb{F}}\{g_1(\boldsymbol{b}), \ldots, g_s(\boldsymbol{b})\}$, the linear subspace spanned by $\{g_1(\boldsymbol{b}), \ldots, g_s(\boldsymbol{b})\}$ over $\mathbb{F}$. Let ℓ_{ω_i}, $i = 1, \ldots, s$, be linear maps in $\mathcal{A}^*$ such that $g_i(\boldsymbol{b}) = \sum_{j=1}^r \ell_{\omega_j}(g_i(\boldsymbol{b}))\omega_j$. Then

$$\begin{aligned} f(\boldsymbol{a}, \boldsymbol{b}) &= \sum_{i=1}^s h_i(\boldsymbol{a}) g_i(\boldsymbol{b}) \\ &= \sum_{i=1}^s h_i(\boldsymbol{a}) \sum_{j=1}^r \ell_{\omega_j}(g_i(\boldsymbol{b}))\omega_j \\ &= \sum_{j=1}^r \omega_j \sum_{i=1}^s h_i(\boldsymbol{a}) \ell_{\omega_j}(g_i(\boldsymbol{b})) = 0. \end{aligned}$$

□

Lemma 9. *Lemma 8 is also true for componentwise, linear and reducible $\bar{\epsilon}$-testers and not necessarily true for symmetric $\bar{\epsilon}$-testers.*

For an indeterminate X over $\mathbb{F}$ and an integer $k \geq 1$, let $\mathbb{F}[X]_k$ be the linear space of all polynomials in $\mathbb{F}[X]$ of degree at most k.

Lemma 10. *Let $\mathbb{K}/\mathbb{F}$ be a field extension and $\alpha \in \mathbb{K}$ algebraic over $\mathbb{F}$ of degree t. Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and X be indeterminates over $\mathbb{F}$ and $\mathcal{M} \subseteq \mathbb{F}[\boldsymbol{x}]$. There is a linear symmetric reducible $(\mathcal{M}, \mathbb{F}(\alpha)$ $, \mathbb{F}[X]_{t-1})$-1-tester of size 1. In particular,*

$$\nu^{\circ}_{\mathbb{F}_q[X]_{t-1}}(\mathcal{M}, \mathbb{F}_{q^t}, 1) = 1.$$

Proof. Every element in $\mathbb{F}(\alpha)$ can be written as $\omega_0 + \omega_1\alpha + \cdots + \omega_{t-1}\alpha^{t-1}$ where $\omega_i \in \mathbb{F}$ for $i = 0, 1, \ldots, t-1$. Define the map $l_X : \mathbb{F}(\alpha) \to \mathbb{F}[X]_{t-1}$, $l_X(\omega_0 + \omega_1\alpha + \cdots + \omega_{t-1}\alpha^{t-1}) = \omega_0 + \omega_1 X + \cdots + \omega_{t-1}X^{t-1}$. Notice that for $a \in \mathbb{F}(\alpha)$, $l_X(a)|_{X \leftarrow \alpha} = a$. Therefore, for $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{F}(\alpha)^n$ and $f \in \mathcal{M}$ if $f(l_X(a_1), \ldots, l_X(a_n)) = 0$ then

$$f(\boldsymbol{a}) = f(l_X(a_1)|_{X \leftarrow \alpha}, \ldots, l_X(a_n)|_{X \leftarrow \alpha}) = f(l_X(a_1), \ldots, l_X(a_n))|_{X \leftarrow \alpha} = 0.$$

This gives a symmetric $(\mathcal{M}, \mathbb{F}(\alpha), \mathbb{F}[X]_{t-1})$-1-tester of size 1. Since l_X is a linear map and $l_X(1) = 1$ the tester is also reducible. □

3.3 Preliminary Results for Polynomials of Degree d

In this section we prove some results related to testers for $\mathcal{P}(\mathbb{F}_q, n, d)$, $\mathcal{HP}(\mathbb{F}_q, n, d)$ and $\mathcal{HLF}(\mathbb{F}_q, n, d)$. We remind the reader that $\nu_R^{\mathcal{P}}(d, S, \bar{\epsilon}) = \nu_R^{\circ}(\mathcal{P}(\mathbb{F}, n, d), S, \bar{\epsilon})$, $\nu_R^{\mathcal{HP}}(d, S, \bar{\epsilon}) = \nu_R^{\circ}(\mathcal{HP}(\mathbb{F}, n, d), S, \bar{\epsilon})$ and $\nu_R(m, S, \bar{\epsilon}) = \nu_R^{\circ}(\mathcal{HLF}(\mathbb{F}, n, m)\ , S, \bar{\epsilon})$.

Important Note 1: Throughout this paper, we will, without stating explicitly in the results, identify every inequality in $\nu_R^{\mathcal{P}}, \nu_R^{\mathcal{HP}}$ or ν_R with its corresponding construction and time complexity. For example, when we write

$$\nu_{\mathbb{F}}(d_1+d_2, S, \bar{\epsilon}_1\bar{\epsilon}_2) \le \nu_{\mathbb{F}}(d_1, S, \bar{\epsilon}_1)\cdot \nu_{\mathbb{F}}(d_2, S, \bar{\epsilon}_2)$$

we also mean the following two statements:

1. From $(\mathcal{HLF}(\mathbb{F}, n, d_1),\ S, \mathbb{F})$-$\bar{\epsilon}_1$-tester of size s_1 and $(\mathcal{HLF}(\mathbb{F}, n, d_2)\ , S, \mathbb{F})$-$\bar{\epsilon}_2$-tester of size s_2 one can construct in deterministic **linear time** (if not explicitly stated otherwise) a $(\mathcal{HLF}(\mathbb{F}, n,$ $d_1+d_2), S, \mathbb{F})$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester of size s_1s_2.
2. If any entry of any map (i.e., $\boldsymbol{l}(\boldsymbol{a})_i$ for any $\boldsymbol{l}\in L$ and any $\boldsymbol{a}\in S^n$) of the $(\mathcal{HLF}(\mathbb{F}, n, d_1),\ S, \mathbb{F})$-$\bar{\epsilon}_1$-tester can be constructed and computed in time T_1 and any entry of any map of the $(\mathcal{HLF}(\mathbb{F}, n, d_2)$ $, S, \mathbb{F})$-$\bar{\epsilon}_2$-tester can be constructed and computed in time T_2 then any entry of any map of the $(\mathcal{HLF}(\mathbb{F}, n,\ d_1+d_2), S, \mathbb{F})$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester can be constructed and computed in time $T_1+T_2+O(1)$.

Important Note 2: In this paper, the time of the construction is the time of constructing all the maps in the tester L. Denote this time by T'. The time of constructing and computing any entry of any map is the worst-case time complexity, over i and all $\boldsymbol{l}\in L$, of computing the ith entry $\boldsymbol{l}(\boldsymbol{a})_i$. Denote this time by T''. Obviously, the complexity of computing $\boldsymbol{l}(\boldsymbol{a})$ is at most nT'' and the time of constructing and computing all the maps is less than $T'+|L|\cdot nT''$.

We also remind the reader that $\tilde{O}(M)$ means $O(M\cdot poly(\log M, \log q))$. Here $poly(\log q)$ is added for the complexity of the arithmetic computations in the ground field $\mathbb{F}_q$.

First we prove

Lemma 11. *We have*

1. $\nu_R(d, S, \bar{\epsilon}) \le \nu_R^{\mathcal{HP}}(d, S, \bar{\epsilon}) \le \nu_R^{\mathcal{P}}(d, S, \bar{\epsilon})$.
2. $\nu_{\mathbb{F}_q}^{\mathcal{P}}(d, \mathbb{F}_{q^{m_1m_2}}, \bar{\epsilon}_1\bar{\epsilon}_2) \le \nu_{\mathbb{F}_q}^{\mathcal{P}}(d, \mathbb{F}_{q^{m_1}}, \bar{\epsilon}_1)\cdot \nu_{\mathbb{F}_{q^{m_1}}}^{\mathcal{P}}(d, \mathbb{F}_{q^{m_1m_2}}, \bar{\epsilon}_2)$.
3. $\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^{m_1m_2}}, \bar{\epsilon}_1\bar{\epsilon}_2) \le \nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^{m_1}}, \bar{\epsilon}_1)\cdot \nu_{\mathbb{F}_{q^{m_1}}}(d, \mathbb{F}_{q^{m_1m_2}}, \bar{\epsilon}_2)$.
4. $\nu_{\mathbb{F}}(d_1+d_2, S, \bar{\epsilon}_1\bar{\epsilon}_2) \le \nu_{\mathbb{F}}(d_1, S, \bar{\epsilon}_1)\cdot \nu_{\mathbb{F}}(d_2, S, \bar{\epsilon}_2)$.

Proof. *1* follows from Lemma 4. *2* and *3* follows from Corollary 6. *4* follows from Lemma 8. □

The following lemma gives an upper bound for the size of a dense tester when the ground field $\mathbb{F}_q$ is very large. In the sequel we show that this bound is tight.

Lemma 12. *We have*

1. *$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)$ and $\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)$.*
2. *If $q\ge d(t-1)+1$ then for any r such that $q\ge r\ge d(t-1)+1$ and $\epsilon=d(t-1)/r$ we have*
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)\le\frac{d(t-1)}{\epsilon}.$$
3. *If $q\ge d(t-1)$ then for any r such that $q+1\ge r\ge d(t-1)+1$ and $\epsilon=d(t-1)/r$ we have*
$$\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)\le\frac{d(t-1)}{\epsilon}.$$
4. *For $r\ne q+1$ the above results are also true for linear symmetric reducible testers. For $r=q+1$ result 3 is also true for linear symmetric testers.*

Proof. By Lemma 5 and 10,
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)\cdot\nu^{\mathcal{P}}_{\mathbb{F}_q[X]_{t-1}}(d,\mathbb{F}_{q^t},1)=\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon).$$
In the same way $\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)$.

We now prove *2.* For every $f\in\mathcal{P}(\mathbb{F}_q,n,d)$ and $(z_1,\ldots,z_n)\in\mathbb{F}_q[X]^n_{t-1}$ we have $f(z_1,\ldots,z_n)\in\mathbb{F}_q[X]_{d(t-1)}$. Let $q\ge d(t-1)+1$. Choose $F\subseteq\mathbb{F}_q$ of size r, where $q\ge r\ge d(t-1)+1$. Define for every $\beta\in F$ the map $l_\beta:\mathbb{F}_q[X]_{t-1}\to\mathbb{F}_q$ where $l_\beta(z)=z(\beta)$. If $f(z_1,\ldots,z_n)\ne 0$ then since $f(z_1,\ldots,z_n)\in\mathbb{F}_q[X]_{d(t-1)}$ we have $l_\beta(f(z_1,\ldots,z_n))=f(l_\beta(z_1),\ldots,l_\beta(z_n))=0$ for at most $d(t-1)$ elements $\beta\in F$. This gives a linear symmetric $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_q[X]_{t-1},\mathbb{F}_q)$-$\bar\epsilon$-tester of size r. Therefore, for $q\ge d(t-1)+1$,
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar\epsilon)\le r=\frac{d(t-1)}{\epsilon}.$$
Notice that the tester is also reducible since $l_\beta(1)=1$.

We now prove *3.* For r such that $q\ge r\ge d(t-1)+1$ the proof is as above. It remains to prove the statement for $r=q+1$. Consider $f\in\mathcal{HP}(\mathbb{F}_q,n,d)$ and $(z_1,\ldots,z_n)\in\mathbb{F}_q[X]^n_{t-1}$. Let $F=\mathbb{F}_q\cup\{\infty\}$ and define for $z\in\mathbb{F}_q[X]_{t-1}$, $l_\beta(z)=z(\beta)$ if $\beta\in\mathbb{F}_q$ and $l_\infty(z)$ to be the coefficient of X^{t-1} in z. Let $L=\{l_\beta\mid\beta\in\mathbb{F}_q\cup\{\infty\}\}$. It is easy to see that the coefficient of $X^{d(t-1)}$ in $f(z_1,\ldots,z_n)$ is $f(l_\infty(z_1),\ldots,l_\infty(z_n))$.

Now suppose $f(z_1,\ldots,z_n)\ne 0$. We have two cases: If $f(l_\infty(z_1),\ldots,l_\infty(z_n))\ne 0$ then since $f(z_1,\ldots,z_n)$ is of degree $d(t-1)$ it can have at most $d(t-1)$ roots in $\mathbb{F}_q$. Otherwise, $f(l_\infty(z_1),\ldots,\ l_\infty(z_n))=0$. Then $f(z_1,\ldots,z_n)$ is of degree at most $d(t-1)-1$ and can have at most $d(t-1)-1$ roots in $\mathbb{F}_q$. In both cases we have that for at most $d(t-1)$ elements $l\in L$, $f(l(z_1),\ \ldots,l(z_n))=0$. This gives a linear symmetric $(\mathcal{HP}(\mathbb{F}_q,n,d),\mathbb{F}_q[X]_{t-1},\mathbb{F}_q)$-$\bar\epsilon$-tester of complexity r which implies the result. Notice that the tester is not reducible because $l_\infty(1)=0\ne 1$. □

As a consequence of Lemma 12 we get

Corollary 13. *We have*

1. *If $q \ge d(t-1)+1$ then for any $\epsilon < 1$ such that*
$$\epsilon \ge \frac{d(t-1)}{q}$$
we have
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar{\epsilon}) \le \left\lceil \frac{d(t-1)}{\epsilon} \right\rceil .$$

2. *If $q \ge d(t-1)$ then for any any $\epsilon < 1$ such that*
$$\epsilon \ge \frac{d(t-1)}{q+1}$$
we have
$$\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le \nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar{\epsilon}) \le \left\lceil \frac{d(t-1)}{\epsilon} \right\rceil .$$

3. *Testers of the above densities and sizes can be constructed in linear time $\tilde{O}(dt/\epsilon)$ and any entry of any of the above maps can be constructed and computed in time $\tilde{O}(t)$.*

Proof. We prove *1*. The proof of *2* is similar.

Let $1 > \epsilon > d(t-1)/(d(t-1)+1)$. By Lemma 7 and Theorem 29 in [3] we have $\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t}) = d(t-1)+1$ and by Lemma 4 and (2) we have
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},1/(d(t-1)+1)) = \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t}) = d(t-1)+1 = \left\lceil \frac{d(t-1)}{\epsilon} \right\rceil .$$

Now let $d(t-1)/(d(t-1)+1) \ge \epsilon \ge d(t-1)/q$ and let $r = \lceil d(t-1)/\epsilon \rceil$. Let $\epsilon_1 = d(t-1)/r$. Since $d(t-1)+1 \le r = \lceil d(t-1)/\epsilon \rceil \le q$ and $\epsilon_1 \le \epsilon$, by Lemma 4 and Lemma 12 we have
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1) \le \left\lceil \frac{d(t-1)}{\epsilon} \right\rceil .$$

Notice that all the constructions in Lemma 4 and Lemma 12 runs in linear time in td/ϵ. Computing one entry in a map requires substituting an element of $\mathbb{F}_q$ in a polynomial of degree t. This takes time $\tilde{O}(t)$. This implies *3*. □

The next result shows how to reduce $\bar{\epsilon}$-testers for degree d polynomials in $\mathbb{F}_{q^t}$ to $\bar{\epsilon}$-testers for degree d polynomials in $\mathbb{F}_{q^k}$ where $k = O(\log((d/\epsilon)t)/\log q)$. Notice that when $k = O(\log((d/\epsilon)t)/\log q)$ then $|\mathbb{F}_{q^k}| = poly(dt/\epsilon)$. This reduction will be used to construct $\bar{\epsilon}$-testers with almost (within $poly(d/\epsilon)$) optimal size in polynomial time.

For any positive integer k, let $N_q(k)$ denotes the number of monic irreducible polynomials of degree k over $\mathbb{F}_q$. It is known that

$$kN_q(k) = \sum_{r|k} \mu\left(\frac{k}{r}\right) q^r \tag{6}$$

where μ is the Moebius function

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^t & n \text{ is the product of } t \text{ distinct primes} \\ 0 & \text{otherwise} \end{cases}$$

and

$$q^{k-1} < kN_q(k) \le q^k. \tag{7}$$

See for example [10].

We remind the reader that $\nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}((d, \mathbb{F}_q), \mathbb{F}_q[X]_{t-1}, \bar{\epsilon}_1)$ is $\nu^{\circ}_{\mathbb{F}_{q^k}}(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_q[X]_{t-1}, \bar{\epsilon}_1)$ which is different than $\nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}(d, \mathbb{F}_q[X]_{t-1}, \bar{\epsilon}_1) = \nu^{\circ}_{\mathbb{F}_{q^k}}(\mathcal{P}(\mathbb{F}_{q^k}, n, d), \mathbb{F}_q[X]_{t-1}, \bar{\epsilon}_1)$. This notation is used when the ground field is not evident from the context.

We now prove the following

Lemma 14. *We have*

1. *For any finite field $\mathbb{F}_q$, any $0 < \epsilon_1, \epsilon_2 < 1$ and integers k and t such that*

   $$kN_q(k) \ge \frac{dt - d + 1}{\epsilon_1},$$

   we have

   $$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}_1\bar{\epsilon}_2) \le \left\lceil \frac{dt - d + 1}{\epsilon_1 \cdot k} \right\rceil \cdot \nu^{\mathcal{P}}_{\mathbb{F}_q}\left(d, \mathbb{F}_{q^k}, \bar{\epsilon}_2\right).$$

2. *Given a $(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_{q^k}, \mathbb{F}_q)$-$\bar{\epsilon}_2$-tester of size s, one can construct a $(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester of size*

   $$S := \left\lceil \frac{dt - d + 1}{\epsilon_1 \cdot k} \right\rceil \cdot s$$

   in time

   $$\tilde{O}\left(S + k^3 p^{1/2} + k^4\right).$$

3. *If constructing and computing any entry of any map in the $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^k},\mathbb{F}_q)$-$\bar{\epsilon}_2$-tester takes time T then constructing and computing any entry of any map in the $(\mathcal{P}(\mathbb{F},n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester takes time*
$$\tilde{O}(T+t+k^3p^{1/2}+k^4).$$

4. *If the $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^k},\mathbb{F}_q)$-$\bar{\epsilon}_2$-tester is componentwise (respectively, linear, reducible and symmetric tester) then the $(\mathcal{P}(\mathbb{F},n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester is componentwise (respectively, linear, reducible and symmetric tester).*

Proof. By Lemma 12 and Lemma 5 we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1\bar{\epsilon}_2)\le\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_q[X]_{t-1},\bar{\epsilon}_1\bar{\epsilon}_2)\le\nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}((d,\mathbb{F}_q),\mathbb{F}_q[X]_{t-1},\bar{\epsilon}_1)\cdot\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^k},\bar{\epsilon}_2).$$

We now prove

$$\nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}((d,\mathbb{F}_q),\mathbb{F}_q[X]_{t-1},\bar{\epsilon}_1)\le\left\lceil\frac{dt-d+1}{\epsilon_1\cdot k}\right\rceil.$$

Let $\mathcal{R}$ be the set of all monic irreducible polynomials of degree k. Since

$$deg\left(\prod_{g\in\mathcal{R}}g\right)=kN_q(k)\ge\frac{dt-d+1}{\epsilon_1},$$

we can choose $\mathcal{R}'\subseteq\mathcal{R}$ such that

$$\frac{dt-d+1}{\epsilon_1}\le deg\left(\prod_{g\in\mathcal{R}'}g\right)<\frac{dt-d+1}{\epsilon_1}+k.$$

Let $\mathcal{R}''$ be any subset of $\mathcal{R}'$ where

$$dt-d+1\le deg\left(\prod_{g\in\mathcal{R}''}g\right)<dt-d+1+k.$$

Let $f\in\mathcal{P}(\mathbb{F}_q,n,d)$, $z_1,\ldots,z_n\in\mathbb{F}_q[X]_{t-1}$ and $F(X):=f(z_1,\ldots,z_n)\in\mathbb{F}_q[X]_{dt-d}$. Now $F\equiv 0$ if and only if F mod $(\prod_{g\in\mathcal{R}''}g)\equiv 0$ if and only if F mod $g\equiv 0$ for all $g\in\mathcal{R}''$. It is known that F mod $g\equiv 0$ if and only if $F(\beta)=f(z_1(\beta),\ldots,z_n(\beta))=0$ for one root $\beta\in\mathbb{F}_{q^k}$ of g. See for example Theorem 3.33 (ii) in [10].

Define for every $g\in\mathcal{R}'$ a map $l_\beta:\mathbb{F}_q[X]\to\mathbb{F}_{q^k}$ where $\beta\in\mathbb{F}_{q^k}$ is a root for g and $l_\beta(z)=z(\beta)$. Let L be the set of all such maps. Then $|L|=|\mathcal{R}'|$. We have shown that if $f(z_1,\ldots,z_n)\ne 0$ then $f(l(z_1),\ldots,l(z_n))=0$ for at most $|\mathcal{R}''|-1$ maps l in L.

Therefore,

$$\nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}\left((d,\mathbb{F}_q),\mathbb{F}_q[X]_{t-1},1-\frac{|\mathcal{R}''|-1}{|\mathcal{R}'|}\right)\le|\mathcal{R}'|\le\left\lceil\frac{dt-d+1}{\epsilon_1\cdot k}\right\rceil.$$

Since

$$\frac{|\mathcal{R}''|-1}{|\mathcal{R}'|}\le\frac{\frac{dt-d+1+k}{k}-1}{\frac{dt-d+1}{\epsilon_1 k}}=\epsilon_1,$$

the result follows from Lemma 4. This implies *1*.

We now describe the construction algorithm and give the time complexity. The input of the algorithm is some representation $\mathbb{F}_{q^t}\simeq\mathbb{F}_q[\alpha]/(f_1(\alpha))$ for some irreducible polynomial $f_1(x)\in\mathbb{F}_q[x]$ of degree t and a $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^k},\mathbb{F}_q)$-$\bar{\epsilon}_2$-tester of size s. Also the field $\mathbb{F}_{q^k}$ has some representation $\mathbb{F}_{q^k}\simeq\mathbb{F}_q[\beta]/(f_2(\beta))$ for some irreducible polynomial $f_2(x)\in\mathbb{F}_q[x]$ of degree k. The algorithm first define a map $\mathbb{F}_{q^t}$ to $\mathbb{F}_q[X]_{t-1}$ that replaces α with X. The algorithm then constructs $\mathcal{R}'$ which is a set of $O(dt/(k\epsilon_1))$ irreducible polynomials of degree k and finds one root in $\mathbb{F}_{q^k}$ for each polynomial. By Lemma 2, this takes time $\tilde{O}((dt/\epsilon_1)+k^3p^{1/2}+k^4\log^2 q)$. Then it constructs the maps l_β for each root β. This takes linear time $O(dt/(\epsilon_1 k))$. Then it uses Lemma 5 which takes linear time in the total size $O(sdt/(\epsilon_1 k))$. Since $s\ge k$ we have $\tilde{O}(dt/\epsilon_1)=\tilde{O}(S)$. This gives the time complexity. This implies *2*

For accessing one map l_β in the tester we need to construct the ith irreducible polynomial. By Lemma 3, this can be done in time $O(k^3p^{1/2}+k^4)$. Computations in the fields $\mathbb{F}_{q^t}$ and $\mathbb{F}_{q^k}$ and the map from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q[X]_{t-1}$ take time $\tilde{O}(t)$. This gives the complexity $\tilde{O}(t+k^3p^{1/2}+k^4)$. This implies *3*

By Lemma 7, *4* is immediate from the construction. □

We note that a slightly better bound can be obtained if $\mathcal{R}$ is the set of all the monic irreducible polynomials of degree at most k. When k divides t, a better bound is proved in the following. We will not use this result in this paper so we will not bother the reader with an almost linear time or local explicit construction and just give the proof for the poly-time construction

Lemma 15. *For any finite field $\mathbb{F}_q$, any $0<\epsilon_1,\epsilon_2<1$ and integers k and t such that $k|t$ and*

$$kq^k>\frac{d(t-k)}{\epsilon_1},$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1\bar{\epsilon}_2)\le\left\lceil\frac{d(t-k)}{\epsilon_1\cdot k}\right\rceil\cdot\nu^{\mathcal{P}}_{\mathbb{F}_q}\left(d,\mathbb{F}_{q^k},\bar{\epsilon}_2\right).$$

Given a $(\mathcal{P}(\mathbb{F},n,d),\mathbb{F}_{q^k},\mathbb{F}_q)$-$\bar{\epsilon}_2$-tester of size s, one can construct a $(\mathcal{P}(\mathbb{F},n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester of size $s\cdot\lceil d(t-k)/(\epsilon_1\cdot k)\rceil$ in time $(sd/\epsilon_1)\cdot poly(t,k,p,\log q)$.

Proof. By Corollary 6 we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1\bar{\epsilon}_2)\le \nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}(d,\mathbb{F}_{(q^k)^{t/k}},\bar{\epsilon}_1)\cdot \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,t,\mathbb{F}_{q^k},\bar{\epsilon}_2).$$

Let $r=\lceil d(t-k)/(\epsilon_1 k)\rceil$. By Lemma 12, since $q^k\ge r\ge d(t/k-1)+1$ for $\epsilon'=d(t/k-1)/r$, we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}(d,\mathbb{F}_{(q^k)^{t/k}},\overline{\epsilon_1})\le \nu^{\mathcal{P}}_{\mathbb{F}_{q^k}}(d,\mathbb{F}_{(q^k)^{t/k}},\overline{\epsilon'})\le \frac{d(t/k-1)}{\epsilon'}\le r.$$

Given a $(\mathcal{P}(\mathbb{F},n,d),\mathbb{F}_{q^k},\mathbb{F}_q)$-$\bar{\epsilon}_2$-tester where $\mathbb{F}_{q^k}=\mathbb{F}_q[u]/(g(u))$ where $g(u)$ is irreducible polynomial in $\mathbb{F}_q$ of degree k. By Lemma 1 the field $\mathbb{F}_{(q^k)^{t/k}}$ can be constructed in time $poly(p,t/k,k\log q)$. By Lemma 12 the $(\mathcal{P}(\mathbb{F},n,d),\mathbb{F}_{(q^k)^{t/k}},\mathbb{F}_{q^k})$-$\bar{\epsilon}_1$-tester can be constructed in time $O(dt/\epsilon_1)$. □

4 Lower Bounds

In this section we give some lower bounds for the complexity of $\bar{\epsilon}$-tester. Then we give some lower bound for the density $\bar{\epsilon}$ for which an $\bar{\epsilon}$-tester exists.

4.1 Lower Bound for the Size

We first prove

Theorem 16. *Let $\mathbb{F}$ be a field and $\mathcal{A}$ and $\mathcal{B}$ be two $\mathbb{F}$-algebras. Let $0\le\epsilon<1$ and $\mathcal{M}\subseteq\mathbb{F}[x_1,x_2,\ldots,x_n]$ be a class of multivariate polynomial. Let $S\subseteq\mathcal{A}$ and $R\subseteq\mathcal{B}$ be linear subspaces. Then*

$$\nu^{\circ}_R(\mathcal{M},S,\bar{\epsilon})\ge\frac{\nu^{\circ}_R(\mathcal{M},S)-1}{\epsilon}.$$

In particular,

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon})\ge\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon})\ge\frac{d(t-1)}{\epsilon},$$

and for $q=o(d)$

$$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon})\ge\frac{\left(1+\frac{1}{q-1}-\frac{1}{(q-1)q^{t-1}}\right)^{d-1}}{\epsilon}\cdot t=\frac{2^{\Omega\left(\frac{1}{q}\right)d}}{\epsilon}\cdot t.$$

Proof. If L is an optimal $(\mathcal{M},S,R)$-$\bar{\epsilon}$-tester then any $L'\subseteq L$ of size $|L'|=\lfloor\epsilon|L|\rfloor+1$ is a $(\mathcal{M},S,R)$-tester. Therefore,

$$\lfloor\epsilon|L|\rfloor+1\ge\nu^{\circ}_R(\mathcal{M},S).$$

Since $\lfloor\epsilon|L|\rfloor+1\le\epsilon|L|+1$ the result follows.

The other results follows from Theorem 27 and 29 in [3]. □

By Theorem 16 and Corollary 13 we have

Corollary 17. *We have*

1. *If* $q\ge d(t-1)+1$ *then for any* $\epsilon<1$ *such that*
$$\epsilon\ge\frac{d(t-1)}{q}$$
we have
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)=\left\lceil\frac{d(t-1)}{\epsilon}\right\rceil.$$

2. *If* $q\ge d(t-1)$ *then for any* $\epsilon<1$ *such that*
$$\epsilon\ge\frac{d(t-1)}{q+1}$$
we have
$$\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)=\left\lceil\frac{d(t-1)}{\epsilon}\right\rceil.$$

We say that C is a *hitting set* over $\mathbb{F}_q$ for $\mathcal{M}$ of density $1-\epsilon$ if $C\subseteq\mathbb{F}_q^n$ and for every $f\in\mathcal{M}$ there are at least $(1-\epsilon)|C|$ elements c in C such that $f(c)\neq 0$.

For $(\mathcal{HLF}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar\epsilon$-tester we give the following better bound

Theorem 18. *For any* q, d *and* t *we have*
$$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\ge\frac{t-1}{\left(1-\frac{1}{q}+\frac{q-1}{q(q^t-1)}\right)^{d-1}-(1-\epsilon)}.$$

Proof. Consider the class of functions
$$\mathcal{M}=\left\{\left(\prod_{i=1}^{d-1}\sum_{m=1}^{t}\lambda_{i,m}y_{i,m}\right)(y_{d,k}-y_{d,j})\;\middle|\;\boldsymbol{\lambda}_i\in P^t(\mathbb{F}_q)\text{ for all }i=1,\ldots,d-1,\ 1\le k<j\le q^t\right\},$$
where $P^t(\mathbb{F}_q)$ is the t-dimensional projective space over $\mathbb{F}_q$. For $\boldsymbol{\lambda}=(\boldsymbol{\lambda}_1,\boldsymbol{\lambda}_2\ldots,\boldsymbol{\lambda}_{d-1})\in P^t(\mathbb{F}_q)^{d-1}$ we denote $f_{\boldsymbol{\lambda}}=\prod_{i=1}^{d-1}(\sum_{m=1}^t\lambda_{i,m}y_{i,m})$. Let $\mathcal{M}'=\{(y_{d,k}-y_{d,j})\mid 1\le k<j\le q^t\}$.

Obviously, $\mathcal{M}\subseteq\mathcal{HLF}(\mathbb{F}_q,n,d)$ where $n=q^t$. Let $L=\{\boldsymbol{l}_1,\ldots,\boldsymbol{l}_\nu\}$ be a $(\mathcal{HLF}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar\epsilon$-tester of minimum size. Then L is an $(\mathcal{M},\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar\epsilon$-tester. Let α be a primitive element of $\mathbb{F}_{q^t}$ and consider the assignment $\boldsymbol{z}=(\boldsymbol{z}_1,\ldots,\boldsymbol{z}_d)\in(\mathbb{F}_{q^t}^n)^d$ where $\boldsymbol{z}_i=(\alpha^0,\alpha^1,\ldots,\alpha^{t-1},0,\ldots,0)\in\mathbb{F}_{q^t}^n$ for all $i=1,2,\ldots,d-1$ and $\boldsymbol{z}_d=(0,\alpha^0,\alpha^1,\ldots,\alpha^{q^t-2})\in\mathbb{F}_{q^t}^n$. Let $\boldsymbol{c}_i=\boldsymbol{l}_i(\boldsymbol{z})\in(\mathbb{F}_q^n)^d$ for $i=1,\ldots,\nu$ and

$C = \{\boldsymbol{c}_i \mid i = 1, 2, \ldots, \nu\}$. Since $f(\boldsymbol{z}) \neq 0$ for all $f \in \mathcal{M}$ and L is a $(\mathcal{M}, \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester, for every $f \in \mathcal{M}$ there are at least $(1-\epsilon)|C|$ elements $\boldsymbol{c} \in C$ such that $f(\boldsymbol{c}) \neq 0$. Therefore, C is a hitting set over $\mathbb{F}_q$ for $\mathcal{M}$ of density $1-\epsilon$.

Notice that if for some $\boldsymbol{c} \in C$ and some $i = 1, 2, \ldots, d-1$ we have $(c_{i,1}, c_{i,2}, \ldots, c_{i,t}) = 0$ then $f(\boldsymbol{c}) = 0$ for all $f \in \mathcal{M}$ and then $C\backslash\{\boldsymbol{c}\}$ is a hitting set over $\mathbb{F}_q$ for $\mathcal{M}$ of density at least $\bar{\epsilon}$. Therefore we may assume w.l.o.g that $(c_{i,1}, c_{i,2}, \ldots, c_{i,t}) \neq 0$ for all $\boldsymbol{c} \in C$ and $i = 1, 2, \ldots, d-1$.

Now for every $\boldsymbol{\lambda} \in P^t(\mathbb{F}_q)^{d-1}$ consider the set $C_{\boldsymbol{\lambda}} = \{\boldsymbol{c} \in C \mid f_{\boldsymbol{\lambda}}(\boldsymbol{c}) \neq 0\}$. For every $C_{\boldsymbol{\lambda}} = \{\boldsymbol{c}^{(1)}, \ldots, \boldsymbol{c}^{(r)}\}$ consider the set

$$D_{\boldsymbol{\lambda}} = \left\{ (c_{d,i}^{(1)}, \ldots, c_{d,i}^{(r)}) \;\middle|\; i = 1, \ldots, q^t \right\}.$$

Since for any $1 \le k < j \le q^t$, C is a hitting set for $f_{\boldsymbol{\lambda}}(y_{d,k} - y_{d,j})$ of density $1-\epsilon$, for every $1 \le k < j \le q^t$ there are at least $(1-\epsilon)|C|$ elements $\boldsymbol{c} \in C_{\boldsymbol{\lambda}}$ such that $c_{d,k} \neq c_{d,j}$. Thus, $D_{\boldsymbol{\lambda}}$ is a code of Hamming distance $(1-\epsilon)|C|$. By the Singleton bound, [12], we have

$$t = \frac{\log |D_{\boldsymbol{\lambda}}|}{\log q} \le |C_{\boldsymbol{\lambda}}| - (1-\epsilon)|C| + 1$$

and therefore $|C_{\boldsymbol{\lambda}}| \ge (t-1) + (1-\epsilon)|C|$. Now it is easy to see that since $(c_{i,1}, c_{i,2}, \ldots, c_{i,t}) \neq 0$ for all $\boldsymbol{c} \in C$ and $i = 1, 2, \ldots, d-1$, every $\boldsymbol{c} \in C$ appears in exactly

$$\left(\frac{q^t - 1}{q-1} - \frac{q^{t-1} - 1}{q-1} \right)^{d-1} = \left(\frac{q^t - q^{t-1}}{q-1} \right)^{d-1}$$

sets of $\{C_{\boldsymbol{\lambda}} \mid \boldsymbol{\lambda} \in P^t(\mathbb{F}_q)^{d-1}\}$. Therefore

$$\begin{aligned}
|C| \ge \frac{\sum_{\boldsymbol{\lambda}} |C_{\boldsymbol{\lambda}}|}{\left(\frac{q^t - q^{t-1}}{q-1}\right)^{d-1}} \quad &\ge \quad \frac{|P^t(\mathbb{F}_q)^{d-1}| \cdot ((t-1) + (1-\epsilon)|C|)}{\left(\frac{q^t - q^{t-1}}{q-1}\right)^{d-1}} \\
&= \quad \frac{\left(\frac{q^t - 1}{q-1}\right)^{d-1} \cdot ((t-1) + (1-\epsilon)|C|)}{\left(\frac{q^t - q^{t-1}}{q-1}\right)^{d-1}} \\
&= \quad \left(\frac{q^t - 1}{q^t - q^{t-1}} \right)^{d-1} ((t-1) + (1-\epsilon)|C|).
\end{aligned}$$

Therefore,

$$\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) = \nu = |C| \ge \frac{t-1}{\left(1 - \frac{1}{q} + \frac{q-1}{q(q^t-1)}\right)^{d-1} - (1-\epsilon)}.$$

This proves the result.

□

Note that for $Y = 1 - 1/q + (q-1)/(q(q^t - 1))$ and $\bar{\epsilon} = \delta Y^d$ for some $\delta < 1$ the bounds in Theorem 16 and Theorem 18 are

$$\frac{t}{(1-\delta Y^d)Y^{d-1}}, \quad \frac{t-1}{(1-\delta Y)Y^{d-1}}$$

respectively. Therefore the later bound is slightly better than the former.

4.2 Lower Bound on the Density

How small ϵ can be? In the following we give a lower bound for ϵ.

Theorem 19. *We have*

1. *If there is a $(\mathcal{HLF}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester of finite size then*

   $$\epsilon \geq 1 - \left(1 - \frac{1}{q} + \frac{q-1}{q(q^t-1)}\right)^d.$$

   For $d = o(q)$

   $$\epsilon \geq \frac{d}{q} - \Theta\left(\frac{d^2}{q^2}\right).$$

   Therefore if $\bar{\epsilon} > (1 - 1/q + (q-1)/(q(q^t-1)))^d$ then $\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) = \infty$.

2. *If there is a $(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester of finite size then*

   $$\epsilon \geq \frac{d}{q}.$$

   Therefore if $\bar{\epsilon} > 1 - d/q$ then for any t we have $\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) = \infty$.

3. *For $d \geq q$ and any t and ϵ we have $\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) = \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}) = \infty$.*

4. *If there is a $(\mathcal{HP}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester of finite size then*

   $$\epsilon \geq \frac{d}{q+1}.$$

   Therefore, if $\bar{\epsilon} > 1 - d/(q+1)$ then for any t we have $\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) = \infty$.

5. *For $d \geq q+1$ and any t and ϵ we have $\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) = \nu^{\mathcal{HP}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}) = \infty$.*

Proof. We first prove *1*. Consider the class of functions

$$\mathcal{M} = \left\{ \prod_{i=1}^{d} \sum_{m=1}^{t} \lambda_{i,m} y_{i,m} \;\middle|\; \boldsymbol{\lambda}_i \in P^t(\mathbb{F}_q) \text{ for all } i = 1, \ldots, d \right\},$$

where $P^t(\mathbb{F}_q)$ is the t-dimensional projective space over $\mathbb{F}_q$. For $\boldsymbol{\lambda} = (\boldsymbol{\lambda}_1, \boldsymbol{\lambda}_2 \ldots, \boldsymbol{\lambda}_d) \in P^t(\mathbb{F}_q)^d$ we denote $f_{\boldsymbol{\lambda}} = \prod_{i=1}^{d}(\sum_{m=1}^{t} \lambda_{i,m} y_{i,m})$. Obviously, $\mathcal{M} \subseteq \mathcal{HLF}(\mathbb{F}_q, n, d)$. Let $L = \{\boldsymbol{l}_1, \ldots, \boldsymbol{l}_\nu\}$ be a $(\mathcal{HLF}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester of minimum size. Then L is an $(\mathcal{M}, \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester. Let α be an element of degree t in $\mathbb{F}_{q^t}$ and consider the assignment $\boldsymbol{z} = (\boldsymbol{z}_1, \ldots, \boldsymbol{z}_d) \in (\mathbb{F}_{q^t}^n)^d$ where $\boldsymbol{z}_i = (\alpha^0, \alpha^1, \ldots, \alpha^{t-1}, 0, \ldots, 0) \in \mathbb{F}_{q^t}^n$ for all $i = 1, 2, \ldots, d$. Notice that $f(\boldsymbol{z}) \neq 0$ for all $f \in \mathcal{M}$. Let $S = \{\boldsymbol{l}_1(\boldsymbol{z}), \ldots, \boldsymbol{l}_\nu(\boldsymbol{z})\} \subseteq (\mathbb{F}_q^n)^d$. We now show that there is $f \in \mathcal{M}$ such that $|\{\boldsymbol{a} \in S \mid f(\boldsymbol{a}) \neq 0\}| \leq (1 - 1/q + (q-1)/(q^{t+1} - q))^d |S|$.

Define a sequence of sets $S = S_0 \supseteq S_1 \supseteq \ldots \supseteq S_d$ recursively as follows: For the set S_i, $i > 0$, consider the functions $\sum_{j=1}^{t} \lambda_{i,j} y_{i,j}$ where $\boldsymbol{\lambda}_i \in P^t(\mathbb{F}_q)$. There is $\boldsymbol{\lambda}_i' \in P^t(\mathbb{F}_q)$ such that $f_i = \sum_{j=1}^{t} \lambda_{i,j}' y_{i,j}$ is zero on at least $|S_{i-1}|(q^{t-1} - 1)/(q^t - 1)$ elements of S_{i-1}. Define $S_i = S_{i-1} \backslash \{\boldsymbol{a} \in S_{i-1} \mid f_i(\boldsymbol{a}) = 0\}$. Then

$$|S_i| \leq \frac{q^t - q^{t-1}}{q^t - 1} |S_{i-1}| = \left(1 - \frac{1}{q} + \frac{q-1}{q(q^t - 1)}\right) |S_{i-1}|.$$

Then $f = f_1 f_2 \cdots f_d \in \mathcal{M}$ is not zero only on the elements of S_d and $|S_d| \leq (1 - 1/q + (q-1)/(q^{t+1} - q))^d |S|$. This implies the result.

To prove *2* we take the class

$$\mathcal{M} = \{f \mid f = f_1 f_2 \cdots f_d,\ f_i = x_1 - \beta_i,\ \beta_i \in \mathbb{F}_q\} \subset \mathcal{P}(\mathbb{F}_q, n, d).$$

Let $L = \{\boldsymbol{l}_1, \ldots, \boldsymbol{l}_\nu\}$ be a $(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester of minimum size. Let $S = \{\boldsymbol{l}_1(\boldsymbol{z}), \ldots, \boldsymbol{l}_\nu(\boldsymbol{z})\} \subseteq \mathbb{F}_q^n$ where $\boldsymbol{z} = (\alpha, 0, 0, \ldots, 0) \in \mathbb{F}_{q^t}^n$ and $\alpha \in \mathbb{F}_{q^t} \backslash \mathbb{F}_q$. Then $f(\boldsymbol{z}) \neq 0$ for all $f \in \mathcal{M}$ and there are $\beta_1, \beta_2, \ldots, \beta_d \in \mathbb{F}_q$ such that f is not zero on at most $1 - d/q$ fraction of the elements of S.

3 follows from Lemma 28 in [3].

To prove *4* we take a function of the form $f = f_1 f_2 \cdots f_d \in \mathcal{HP}(\mathbb{F}_q, n, d)$ where $f_i = \gamma_i x_1 - \beta_i x_2$, $(\gamma_i, \beta_i) \in \mathbb{F}_q^2 \backslash \{(0,0)\}$ and $\boldsymbol{z} = (1, \alpha, 0, \ldots, 0)$ where $\alpha \in \mathbb{F}_{q^t} \backslash \mathbb{F}_q$. It is easy to see that there is such function that is not zero on at most $1 - d/(q+1)$ fraction of the elements of S.

5 follows from Lemma 28 in [3]. □

We note here that for *4* in Theorem 19 the following slightly better bound

$$\left(1 - \frac{1}{q}\right)^d \left(1 + \frac{1}{q^t - 1}\right) = 1 - \frac{d}{q} + \Theta\left(\frac{d^2}{q^2}\right)$$

can be proved if we take $f = \prod_{i=1}^{d} \sum_{j=1}^{t} \lambda_{i,j} x_j$ where $(\lambda_{i,j})_{i,j}$ is a matrix of rank d.

5 Constructions of Dense Testers

In this section we give some constructions of dense testers.

In Subsection 5.1 we give several constructions for testers for $\mathcal{P}(\mathbb{F}_q, n, d)$ from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$. By Theorem 19, such constructions exist if $q \geq d+1$ and $\bar{\epsilon} \leq 1 - d/q$. Our constructions give testers of sizes that are within *poly*(d/ϵ) factor from optimal with any density $\bar{\epsilon} \leq 1 - d/q - d/q^2 - o(d/q^2)$.

In Subsection 5.2 we give a construction for tester for $\mathcal{HLF}(\mathbb{F}_q, n, d)$ from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ for any q. Theorem 16 and Theorem 19 show that the size of such tester is at least $(1 + 1/(q-1))^d t$ and its density is at most $\bar{\epsilon} \leq (1 - 1/q)^d$. We give a tester of size $(1 + (\log q)/q)^d t$ of density $\bar{\epsilon} \leq (1 - (\log q)/q)^d$.

Section 6 shows how to construct such testers in almost linear time and shows that such constructions are locally explicit.

5.1 Dense Testers for Large Fields

In this section we use algebraic function fields to construct an $\bar{\epsilon}$-testers for large fields.

We prove

Theorem 20. *For any $q \geq d+1$, any t, any constant c and any $\epsilon > d/q + d/q^2 + d/q^{2^2} + \cdots + d/q^{2^c} + 8d/(q^{2^{c+1}} - 1)$, we have*

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \leq poly\left(\frac{d}{\epsilon}\right) \cdot t.$$

In particular, the bound holds for $\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon})$ and $\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon})$.

The exact *poly*(d/ϵ) is given in the following two theorems. Theorem 21 is for $q > 10 \cdot d$ and Theorem 22 is for $d+1 \leq q \leq 10d$. Notice that by Theorem 19, $\epsilon \geq d/q$ and therefore when $d+1 \leq q \leq 10d$ we have $\epsilon = O(1)$ and *poly*$(d/\epsilon) =$ *poly*(d). This is why ϵ does not appear in the size of the testers in Theorem 22.

Theorem 21. *For any $q \geq 10 \cdot d$ and any constant $c > 1$ we have the following results*

q	t	ϵ	$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\epsilon)=O(\cdot)$	*Result*
P.S.	*I.S.*	$\epsilon \ge \frac{d}{\sqrt{q}-1}$	$\frac{d}{\epsilon}\cdot t$	*Lemma 30*
$-$	*I.S.*	$\epsilon \ge 2\frac{d}{q}$	$\left(\frac{d}{\epsilon}\right)^2\cdot t$	*Lemma 31*
$-$	$-$	$\epsilon \ge 8\frac{d}{q}$	$\left(\frac{d}{\epsilon}\right)^3\cdot t$	*Lemma 32*
$-$	$-$	$\epsilon \ge c\frac{d}{q}$	$\left(\frac{d}{\epsilon}\right)^4\cdot t$	*Lemma 33*
$-$	$-$	$\epsilon \ge \frac{d}{q}+o\left(\frac{d}{q}\right)$	$\left(\frac{d}{\epsilon}\right)^{4+o(1)}\cdot t$	*Lemma 33*
$-$	$-$	$\epsilon \ge \frac{d}{q}+O\left(\frac{d}{q^2}\right)$	$\left(\frac{d}{\epsilon}\right)^9\cdot t$	*Lemma 34*
$-$	$-$	$\epsilon \ge \frac{d}{q}+\frac{d}{q^2}+o\left(\frac{d}{q^2}\right)$	$\left(\frac{d}{\epsilon}\right)^{9+o(1)}\cdot t$	*Lemma 34*

In the table, P.S. stands for "perfect square" and I.S. stands for "for infinite sequence of integers".

Theorem 22. *For any $10\cdot d \ge q = d+\delta$ where $\delta \ge 1$ and any constant $c<1$ we have the following results*

t	ϵ	$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\epsilon)=O(\cdot)$
I.S.	$\epsilon \ge 1-\frac{c\delta}{q}=\frac{d}{q}+(1-c)\frac{\delta}{q}$	$d^3\cdot t$
$-$	$\epsilon \ge 1-\frac{c\delta}{q}=\frac{d}{q}+(1-c)\frac{\delta}{q}$	$d^4\cdot t$
I.S.	$\epsilon \ge 1-\frac{\delta}{q}+o\left(\frac{\delta}{q}\right)=\frac{d+o(\delta)}{q}$	$d^{3+o(1)}\cdot t$
$-$	$\epsilon \ge 1-\frac{\delta}{q}+o\left(\frac{\delta}{q}\right)=\frac{d+o(\delta)}{q}$	$d^{4+o(1)}\cdot t$

In Theorem 19 we have shown that for $\epsilon < d/q$ or $q < d+1$ there is no $\bar{\epsilon}$-tester for $\mathcal{P}(\mathbb{F}_q,n,d)$. This shows that the bound $q \ge d+1$ in Theorem 20 and 22 is tight and ϵ is almost tight. In Theorem 16 we have shown that $\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \ge d(t-1)/\epsilon$. So the size of our $\bar{\epsilon}$-tester is within a $poly(d/\epsilon)$ factor of the optimal size.

For $\nu^{\mathcal{HP}}_{\mathbb{F}_q}$ (and therefore for $\nu_{\mathbb{F}_q}$) slightly better results can be obtained.

Theorem 23. *For any $q \ge d+1$, any t, any constant integer c and any $\epsilon > d/(q+1)+d/(q^2+1)+d/(q^{2^2}+1)+\cdots+d/(q^{2^c}+1)+8d/(q^{2^{c+1}}-1)$, we have*

$$\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le poly\left(\frac{d}{\epsilon}\right)\cdot t.$$

In particular, the bound holds for $\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon})$.

Theorem 24. *For any $10\cdot d \ge q = d+\delta-1$ where $\delta \ge 1$ and any constant $c<1$ we have the following results*

t	ϵ	$\nu^{\mathcal{HP}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\epsilon)=O(\cdot)$
I.S.	$\epsilon\ge 1-\frac{c\delta}{q+1}=\frac{d}{q+1}+(1-c)\frac{\delta}{q+1}$	$d^3\cdot t$
$-$	$\epsilon\ge 1-\frac{c\delta}{q+1}=\frac{d}{q+1}+(1-c)\frac{\delta}{q+1}$	$d^4\cdot t$
I.S.	$\epsilon\ge 1-\frac{\delta}{q+1}+o\left(\frac{\delta}{q+1}\right)=\frac{d+o(\delta)}{q+1}$	$d^{3+o(1)}\cdot t$
$-$	$\epsilon\ge 1-\frac{\delta}{q+1}+o\left(\frac{\delta}{q+1}\right)=\frac{d+o(\delta)}{q+1}$	$d^{4+o(1)}\cdot t$

Now notice that $d/(q+1)=d/q+\theta(d/q^2)$ and therefore the bounds for ϵ in Theorem 21 (except the last row in the table that is included in Theorem 24) are the same for $\nu^{\mathcal{HP}}_{\mathbb{F}_q}$.

We also show

Theorem 25. *All the above bounds are true for componentwise, linear reducible and symmetric $\bar{\epsilon}$-testers.*

We note here that there are many other results that are not included in the above theorems. For example, for infinite sequence of integers t, any constant $c>1$ and $\epsilon\ge\epsilon_{min}=cd/q$ we have $\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\epsilon)\le(d/\epsilon)^3t$. We simply avoided results that immediately follows from the above results and their proof techniques.

For notations used in this section we refer the reader to Sections 1.1 – 1.4 in [16].

We first prove

Lemma 26. *Let $F/\mathbb{F}_q$ be a function field, $P_1,\ldots,P_s$ be distinct places of $F/\mathbb{F}_q$ of degree 1 and $D=P_1+P_2+\cdots+P_s$. Let G be a divisor of $F/\mathbb{F}_q$ such that $(\text{supp } D)\cap(\text{supp } G)=\emptyset$. Let $L=\{l_{P_1},\ldots,l_{P_s}\}$ be a set of maps $l_{P_i}:\mathscr{L}(G)\to\mathbb{F}_q\cup\{\infty\}$ where $l_{P_i}(x):=x(P_i)$. If $s>d\deg(G)$ then L is a componentwise, linear, reducible and symmetric $(\mathcal{P}(\mathbb{F}_q,n,d),\mathscr{L}(G),\mathbb{F}_q)$-$(1-d\deg G/s)$-tester of size s. Therefore*

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathscr{L}(G),1-d\deg G/s)\le s.$$

Proof. We have shown in Lemma 12.1 in [3] that any $L'\subseteq L$ where $|L'|=d\deg(G)+1$ is a symmetric and reducible $(\mathcal{P}(\mathbb{F}_q,n,d),\mathscr{L}(G),\mathbb{F}_q)$-tester. This implies the result. □

In Lemma 13 in [3] we have proved

Lemma 27. *Let $F/\mathbb{F}_q$ be a function field. Let G be a divisor of $F/\mathbb{F}_q$ and Q a prime divisor of degree $\deg Q=\ell(G)=t$ such that $v_Q(G)=0$. If $\ell(G-Q)=0$ then we have*

1. *The map*

$$\begin{array}{rcl} E:\mathscr{L}(G) & \to & F_Q\cong\mathbb{F}_{q^t} \\ f & \mapsto & f(Q) \end{array}$$

   is an isomorphism of linear spaces over $\mathbb{F}_q$

2. *$L=\{E^{-1}\}$ is a linear, reducible and symmetric $(\mathbb{F}_q[\boldsymbol{x}],\mathbb{F}_{q^t},\mathscr{L}(G))$-1-tester where $\boldsymbol{x}=(x_1,\ldots,x_n)$. Therefore*
$$\nu^{\circ}_{\mathscr{L}(G)}(\mathbb{F}_q[\boldsymbol{x}],\mathbb{F}_{q^t},1)=1.$$

We now use the above two lemmas to prove

Lemma 28. *Let d and t be two integers. Let $F/\mathbb{F}_q$ be a function field of genus g that has $N>d(t+g-1)$ places of degree 1. If $t\ge 3+2\log_q(2g+1)$ then for any $N\ge s>d(t+g-1)$ and $\epsilon=d(t+g-1)/s$ we have*
$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon})\le\frac{d(t+g-1)}{\epsilon}.$$

Proof. First, by Corollary 5.2.10 (c) in [16], if $2g+1\le q^{(t-1)/2}(q^{1/2}-1)$ then there is a prime divisor of degree t. Since $t\ge 3+2\log_q(2g+1)$ the inequality holds and there is at least one prime divisor of degree t. Let Q be such divisor. Let $P_1,\ldots,P_s$, $s>d(t+g-1)$, be distinct places of $F/\mathbb{F}_q$ of degree 1 and $D=P_1+P_2+\cdots+P_s$. By Lemma 14 in [3] and Lemma 2.1 and 2.2 in [2], there is a divisor G of $F/\mathbb{F}_q$ such that $(\mathrm{supp}\ D)\cap(\mathrm{supp}\ G)=\emptyset$, $\deg Q=t=\ell(G)$, $v_Q(G)=0$, $\ell(G-Q)=0$ and $\deg G=t+g-1$.

By Lemmas 5, 26 and 27 we have
$$\begin{aligned}\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},1-d(t+g-1)/s) &\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathscr{L}(G),1-d(t+g-1)/s)\cdot\nu^{\mathcal{P}}_{\mathscr{L}(G)}(d,\mathbb{F}_{q^t},1)\\ &\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathscr{L}(G),1-d(t+g-1)/s)\le s.\end{aligned}$$

□

We are now ready to give the construction.

A *tower* of function fields over $\mathbb{F}_q$ is a sequence $\mathcal{F}=(F^{(0)},F^{(1)},F^{(2)},\cdots)$ of function fields $F^{(i)}/\mathbb{F}_q$ with $F^{(0)}\subseteq F^{(1)}\subseteq F^{(2)}\subseteq\cdots$ where each extension $F^{(k+1)}/F^{(k)}$ is finite and separable.

There are many explicit towers known from the literature. We will use the following $\mathcal{W}_1$ tower defined in [6]. See also [7] Chapter 1 and [15] Chapter I. To avoid confusion we must note here that $F^{(k)}$ here is the function field F_{k-1} in [7, 15].

Lemma 29. *Let x_1 be indeterminate over $\mathbb{F}_{q^2}$ and $F^{(1)}=\mathbb{F}_{q^2}(x_1)$. For $k\ge 2$ let $F^{(k)}=F^{(k-1)}(x_k)$ where*
$$x_k^q+x_k=\frac{x_{k-1}^q}{x_{k-1}^{q-1}+1}.$$

Let g_k be the genus of $F^{(k)}/\mathbb{F}_{q^2}$ and N_k the number of places in $F^{(k)}/\mathbb{F}_{q^2}$ of degree 1. Then
$$g_k=\left\{\begin{array}{ll} q^k-2q^{k/2}+1 & \text{if } k=0 \mod 2\\ q^k-q^{(k+1)/2}-q^{(k-1)/2}+1 & \text{if } k=1 \mod 2\end{array}\right., \tag{8}$$

$$N_k = \left\{ \begin{array}{ll} (q^2-q)q^{k-1}+2q & \text{if } k \geq 3, q=1 \mod 2 \\ (q^2-q)q^{k-1}+2q^2 & \text{if } k \geq 3, q=0 \mod 2 \end{array} \right. \tag{9}$$

and $N_k \geq (q^2-q)q^{k-1}$ for $k = 1, 2$.

We are now ready to prove Theorem 20, 21 and 22. We start with Theorem 21. The proof will be consequence of the following lemmas. See the table in Theorem 21.

Lemmas 30–34 below prove Theorem 21.

Lemma 30. *Let k be any integer, $Q = q^2$ and $c \geq (k+4)/q^k$ be any constant such that $t := cq^k$ is an integer. For every ϵ such that*

$$1 > \epsilon \geq \epsilon_{min} := (c+1)\frac{d}{\sqrt{Q}-1}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_Q}(d, \mathbb{F}_{Q^t}, \bar{\epsilon}) \leq \left(1+\frac{1}{c}\right)\frac{dt}{\epsilon}.$$

Proof. Consider the tower defined in Lemma 29 and the function field $F^{(k)}/\mathbb{F}_{q^2}$. The number of places of degree 1 is at least $N = q^{k+1} - q^k$ and the genus is $g_k \leq q^k - 2q^{k/2} + 1 = t/c - 2\sqrt{t/c} + 1$. We now use Lemma 28. Since $t = cq^k \geq k+4$ and $3 + 2\log_{q^2}(2g_k+1) \leq 4+k$ the first condition in Lemma 28 holds. Therefore, for any $N \geq s > d(t+g_k-1)$ and $\epsilon = d(t+g_k-1)/s$ we have

$$\begin{aligned} \nu^{\mathcal{P}}_{\mathbb{F}_{q^2}}(d, \mathbb{F}_{(q^2)^t}, \bar{\epsilon}) &\leq \frac{d(t+g_k-1)}{\epsilon} \\ &\leq \frac{d(t+t/c) - 2d\sqrt{t/c}}{\epsilon} \\ &\leq \left(1+\frac{1}{c}\right)\frac{dt}{\epsilon}. \end{aligned}$$

The minimal possible ϵ is

$$\begin{aligned} \frac{d(t+g_k-1)}{N} &\leq \frac{d(cq^k + q^k - 2q^{k/2})}{q^{k+1}-q^k} \\ &\leq \frac{d(c+1-2\sqrt{c/t})}{q-1} \\ &\leq (c+1)\frac{d}{q-1} = \epsilon_{min}. \end{aligned}$$

□

Although the result in Lemma 30 seems to be true for any perfect square Q, the condition $1 > \epsilon \geq (c+1)d/(\sqrt{Q}-1)$ makes sense only when $(c+1)d/(\sqrt{Q}-1) < 1$ and therefore $Q > ((c+1)d+1)^2$. Therefore we will ignore the condition on q in the subsequent results with the understanding that for some q the results are true as the statement is void.

We note here that many other results can be obtained using different other towers. This will not be discussed in this paper.

We now prove

Lemma 31. *Let $q \geq d+1$. Let k be any integer and $c \geq (k+4)/q^k$ be any constant such that $t := cq^k$ is an integer. Then for any ϵ such that*

$$1 > \epsilon \geq \epsilon_{min} := 2(c+1)\frac{d}{q-1}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon}) \leq 5\left(1+\frac{1}{c}\right)\left(\frac{d}{\epsilon}\right)^2 t.$$

Proof. By Lemma 4, (5), Corollary 13 and Lemma 30 we have

$$\begin{aligned}
\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon}) &\leq \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^{2t}}, \overline{\epsilon}) \\
&\leq \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^2}, \overline{\epsilon/2}) \cdot \nu^{\mathcal{P}}_{\mathbb{F}_{q^2}}(d, \mathbb{F}_{q^{2t}}, \overline{\epsilon/2}) \\
&\leq \left(\frac{2d}{\epsilon}+1\right)\left(1+\frac{1}{c}\right)\frac{2dt}{\epsilon} \\
&\leq 5\left(1+\frac{1}{c}\right)\left(\frac{d}{\epsilon}\right)^2 t.
\end{aligned}$$

□

Lemma 32. *Let $q \geq d+1$ and $t \geq 8$. Then for any ϵ such that*

$$1 > \epsilon \geq \epsilon_{min} := 8\frac{d}{q-1}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon}) \leq 120\left(\frac{d}{\epsilon}\right)^3 t.$$

Proof. Let k be an integer such that $q^k \leq t < q^{k+1}$ and $r = q^k$. Let $\epsilon \geq \epsilon_{min} = 8d/(q-1)$. Then, since by (7)

$$r \cdot N_q(r) \geq q^{q^k-1} \geq q^{k+2} \geq qt \geq \frac{dt-d+1}{\epsilon/2}$$

by Lemma 14 and 31 we have

$$\begin{aligned}\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon}) &\leq \left\lceil\frac{dt-d+1}{(\epsilon/2)r}\right\rceil\cdot\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^r},\overline{\epsilon/2})\\ &\leq \left(\frac{3dt}{\epsilon r}\right)\left(5\cdot 2\cdot\left(\frac{d}{\epsilon/2}\right)^2 r\right)\\ &\leq 120\left(\frac{d}{\epsilon}\right)^3 t.\end{aligned}$$

□

Lemma 33. *Let $q\geq d+1$, $8>c>1+8q/(q^2-1)$ and $t\geq 8$. Then for any ϵ such that*

$$8\frac{d}{q}>\epsilon=c\frac{d}{q}>\frac{d}{q}+\frac{8d}{q^2-1}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon})\leq O\left(\frac{1}{(c-1)^3}\left(\frac{d}{\epsilon}\right)^4\right)\cdot t.$$

Proof. Let $\epsilon_1=d/q$ and $\epsilon_2=(c-1)d/q$. By Lemma 4, (5), Corollary 13 and Lemma 32 we have

$$\begin{aligned}\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon}) &\leq \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^{2t}},\overline{\epsilon_1+\epsilon_2})\\ &\leq \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^2},\overline{\epsilon_1})\cdot\nu^{\mathcal{P}}_{\mathbb{F}_{q^2}}(d,\mathbb{F}_{q^{2t}},\overline{\epsilon_2})\\ &\leq q\cdot 120\cdot\left(\frac{d}{\epsilon_2}\right)^3 t\\ &\leq 120\frac{q^4}{(c-1)^3}t=O\left(\frac{1}{(c-1)^3}\left(\frac{d}{\epsilon}\right)^4\right)\cdot t.\end{aligned}$$

□

Lemma 34. *Let $q\geq d+1$, $8>c>8q^2/(q^4-1)$ and $t\geq 8$. Then for any ϵ such that*

$$\frac{d}{q}+\frac{9d}{q^2}>\epsilon=\frac{d}{q}+\frac{d}{q^2}+c\frac{d}{q^2}>\frac{d}{q}+\frac{d}{q^2}+\frac{8d}{q^4-1}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon})\leq O\left(\frac{1}{c^3}\left(\frac{d}{\epsilon}\right)^9\right)\cdot t.$$

Proof. Let $\epsilon_1 = d/q$, $\epsilon_2 = d/q^2$ and $\epsilon_3 = cd/q^2$. By Lemma 4, (5), Corollary 13 and Lemma 32 we have

$$\begin{array}{rcl}
\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon}) & \le & \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^{4t}}, \overline{\epsilon_1 + \epsilon_2 + \epsilon_3}) \\
& \le & \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^2}, \overline{\epsilon_1}) \cdot \nu^{\mathcal{P}}_{\mathbb{F}_{q^2}}(d, \mathbb{F}_{q^4}, \overline{\epsilon_2}) \cdot \nu^{\mathcal{P}}_{\mathbb{F}_{q^4}}(d, \mathbb{F}_{q^{4t}}, \overline{\epsilon_3}) \\
& \le & q \cdot q^2 \cdot 120 \left(\dfrac{d}{\epsilon_3}\right)^3 t \\
& \le & 120 \dfrac{q^9}{c^3} t = O\left(\dfrac{1}{c^3}\left(\dfrac{d}{\epsilon}\right)^9\right) \cdot t.
\end{array}$$

□

Lemmas 30–34 prove Theorem 21. We now prove Theorem 20. We show

Lemma 35. *Let $q \ge d+1$, m is any integer, $8 > c > 8q^{2^m}/(q^{2^{m+1}} - 1)$ and $t \ge 8$. Then for any constant m and ϵ such that*

$$\frac{d}{q} + \frac{d}{q^2} + \cdots + \frac{d}{q^{2^{m-1}}} + \frac{9d}{q^{2^m}} > \epsilon = \frac{d}{q} + \frac{d}{q^2} + \cdots + \frac{d}{q^{2^m}} + c\frac{d}{q^{2^m}} > \frac{d}{q} + \frac{d}{q^2} + \cdots + \frac{d}{q^{2^m}} + \frac{8d}{q^{2^{m+1}} - 1}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon}) \le O\left(\frac{1}{c^3}\left(\frac{d}{\epsilon}\right)^{5\cdot 2^m - 1}\right) \cdot t.$$

Proof. Let $\epsilon_i = d/q^{2^i}$, $i = 0, 1, 2, \ldots, m$ and $\epsilon_{m+1} = cd/q^{2^m}$. By Lemma 4, (5), *1* in Corollary 13 and Lemma 32 we have

$$\begin{array}{rcl}
\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon}) & \le & \nu^{\mathcal{P}}_{\mathbb{F}_q}\left(d, \mathbb{F}_{q^{2^{m+1}t}}, \overline{\displaystyle\sum_{i=0}^{m+1} \epsilon_i}\right) \\
& \le & \left(\displaystyle\prod_{i=0}^{m} \nu^{\mathcal{P}}_{\mathbb{F}_{q^{2^i}}}(d, \mathbb{F}_{q^{2^{i+1}}}, \overline{\epsilon_i})\right) \cdot \nu^{\mathcal{P}}_{\mathbb{F}_{q^{m+1}}}(d, \mathbb{F}_{q^{2^{m+1}t}}, \overline{\epsilon_{m+1}}) \\
& \le & q \cdot q^2 \cdots q^{2^m} \cdot 120 \left(\dfrac{d}{\epsilon_{m+1}}\right)^3 t \\
& \le & 120 \dfrac{q^{5\cdot 2^m - 1}}{c^3} t = O\left(\dfrac{1}{c^3}\left(\dfrac{d}{\epsilon}\right)^{5\cdot 2^m - 1}\right) \cdot t.
\end{array}$$

□

The same proof but using *2* in Corollary 13 instead of *1* gives

Lemma 36. *Let $q \ge d$, m is any integer, $8 > c > 8q^{2^m}/(q^{2^{m+1}}-1)$ and $t \ge 8$. Then for any constant m and ϵ such that*

$$\epsilon = \frac{d}{q+1} + \frac{d}{q^2+1} + \cdots + \frac{d}{q^{2^m}+1} + c\frac{d}{q^{2^m}}$$

we have

$$\nu_{\mathbb{F}_q}^{\mathcal{HP}}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \le O\left(\frac{1}{c^3}\left(\frac{d}{\epsilon}\right)^{5\cdot 2^m - 1}\right) \cdot t.$$

We now prove Theorem 22.

Lemma 37. *Let $q = d + \delta$ where $1 \le \delta \le 9d$. Then for any $c < 1$ and every ϵ such that*

$$1 > \epsilon = \frac{d}{q} + (1-c)\frac{\delta}{q} = 1 - \frac{c\cdot\delta}{q} \ge \epsilon_{min}$$

where

$$\epsilon_{min} := \frac{d}{q} + \frac{12\delta}{q^2} - \frac{12\delta^2}{q^3} = 1 - \frac{\delta}{q} + O\left(\frac{\delta}{q^2}\right)$$

we have

$$\nu_{\mathbb{F}_q}^{\mathcal{P}}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \le O\left(\frac{d^{\tau+1}}{(1-c)^\tau}\right) \cdot t$$

where $\tau = 2$ for infinite number of integers t and $\tau = 3$ for all integers t.

Proof. Let $\epsilon_1 = d/q$ and

$$\epsilon_2 := \frac{q\epsilon - d}{q-d} = 1 - c.$$

Then it is easy to see that $\bar{\epsilon} = \bar{\epsilon}_1\bar{\epsilon}_2$ and

$$\epsilon_2 = \frac{q\epsilon - d}{q-d} \ge \frac{q\epsilon_{min} - d}{q-d} = \frac{12d}{q^2}.$$

By Lemma 4, Corollary 6 and 13 and Lemma 31 and 32 we have

$$\begin{aligned}
\nu_{\mathbb{F}_q}^{\mathcal{P}}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) &\le \nu_{\mathbb{F}_q}^{\mathcal{P}}(d, \mathbb{F}_{q^{2t}}, \bar{\epsilon}_1\bar{\epsilon}_2) \\
&\le \nu_{\mathbb{F}_q}^{\mathcal{P}}(d, \mathbb{F}_{q^2}, \bar{\epsilon}_1) \cdot \nu_{\mathbb{F}_{q^2}}^{\mathcal{P}}(d, \mathbb{F}_{q^{2t}}, \bar{\epsilon}_2) \\
&= q \cdot \nu_{\mathbb{F}_{q^2}}^{\mathcal{P}}(d, \mathbb{F}_{q^{2t}}, \bar{\epsilon}_2) \\
&\le O\left(q\left(\frac{d}{\epsilon_2}\right)^\tau\right) \cdot t \\
&\le O\left(\frac{d^{\tau+1}}{(1-c)^\tau}\right) \cdot t
\end{aligned}$$

□

The same proof as above (replace each occurrence of q to $q+1$) gives Theorem 24.

Since all the above bounds use the componentwise, linear, reducible and symmetric testers that are constructed in Lemma 26, 27 and Corollary 13, by Lemma 7 and 5, Theorem 25 follows.

5.2 Testers for Small Fields

In this section we use our results from the previous sections to construct testers for small fields. We give constructions for testers for $\mathcal{HLF}(\mathbb{F}_q,n,d)$ from $\mathbb{F}_{q^t}$ to $\mathbb{F}_q$ for any q. Theorem 16 and Theorem 19 show that the size of such tester is at least $(1+1/(q-1))^d t$ and its density is at most $\overline{\epsilon} \le (1-1/q)^d$. One of the testers we give in this subsection is a tester of size $(1+(\log q)/q)^d t$ and density $\overline{\epsilon} \le (1-(\log q)/q)^d$.

We first prove

Theorem 38. *Let $q<d+1$ be a power of prime and t be any integer. Let r be an integer such that $q^{2^{r-1}} < 9d \le q^{2^r}$. Let $\boldsymbol{\epsilon} = (\epsilon_0,\ldots,\epsilon_{r-1},\epsilon_r)$ where $\epsilon_i(q^{2^i}+1) \le q^{2^i}$ is an integer for $i=0,1,\ldots,r-1$ and $2/3 \ge \epsilon_r \ge 1/3$. Let*

$$c_{q,\boldsymbol{\epsilon}} := \sum_{i=0}^{r-1} \frac{\log(q^{2^i}+1)}{\epsilon_i(q^{2^i}+1)}$$

and

$$\pi_{q,\boldsymbol{\epsilon}} := \sum_{i=0}^{r-1} \frac{-\log(1-\epsilon_i)}{\epsilon_i(q^{2^i}+1)}.$$

Then

$$\overline{\epsilon^\star} := \overline{\epsilon}_r \prod_{i=0}^{r-1} \overline{\epsilon}_i^{\lceil d/(\epsilon_i(q^{2^i}+1))\rceil} \ge \frac{2^{-\pi_{q,\boldsymbol{\epsilon}}\cdot d}}{\Theta(d^2)},$$

and

$$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star}) \le \Theta(d^5)\cdot 2^{c_{q,\boldsymbol{\epsilon}}\cdot d}\cdot t.$$

Proof. By Lemma 4, Corollary 6, Lemma 11 and 12 we have

1. $\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^{t_1}},\overline{\epsilon}) \le \nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^{t_1t_2}},\overline{\epsilon})$.
2. $\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^{t_1t_2}},\overline{\epsilon}_1\overline{\epsilon}_2) \le \nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^{t_1}},\overline{\epsilon}_1)\cdot \nu_{\mathbb{F}_{q^{t_1}}}(d,\mathbb{F}_{q^{t_1t_2}},\overline{\epsilon}_2)$.
3. $\nu_{\mathbb{F}_q}(d_1+d_2,\mathbb{F}_{q^t},\overline{\epsilon}_1\overline{\epsilon}_2) \le \nu_{\mathbb{F}_q}(d_1,\mathbb{F}_{q^t},\overline{\epsilon}_1)\cdot \nu_{\mathbb{F}_q}(d_2,\mathbb{F}_{q^t},\overline{\epsilon}_2)$.
4. $\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^2},\overline{\epsilon}) \le q+1$ for any $\epsilon<1$ such that $\epsilon(q+1)$ is an integer and $d \le \epsilon(q+1)$.

Let $\eta_i = \epsilon_i(q^{2^i}+1)$. Then

$$\begin{aligned}
\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star}) &\le \nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^{t\cdot 2^r}},\overline{\epsilon^\star}) \quad \text{By (1.)}\\
&\le \left(\prod_{i=0}^{r-1}\nu_{\mathbb{F}_{q^{2^i}}}\left(d,\mathbb{F}_{q^{2^{i+1}}},\bar{\epsilon}_i^{\lceil d/\eta_i\rceil}\right)\right)\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r) \quad \text{By (2.)}\\
&\le \left(\prod_{i=0}^{r-1}\nu_{\mathbb{F}_{q^{2^i}}}(\eta_i,\mathbb{F}_{q^{2^{i+1}}},\bar{\epsilon}_i)^{\lfloor d/\eta_i\rfloor}\cdot\nu_{\mathbb{F}_{q^{2^i}}}(d-\eta_i\lfloor d/\eta_i\rfloor,\mathbb{F}_{q^{2^{i+1}}},\bar{\epsilon}_i)\right)\\
&\qquad \cdot\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r) \quad \text{By (3.)}\\
&\le \left(\prod_{i=0}^{r-1}\left(q^{2^i}+1\right)^{\lceil d/\eta_i\rceil}\right)\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r) \;\; \text{By (4.)}\\
&\le \left(\left(\prod_{i=0}^{r-1}\left(q^{2^i}+1\right)\right)2^{c_{q,\epsilon}\cdot d}\right)\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r)\\
&\le \frac{q^{2^r}-1}{q-1}\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r)\cdot 2^{c_{q,\epsilon}\cdot d}\\
&\le \Theta(d^5)\cdot 2^{c_{q,\epsilon}\cdot d}\cdot t \;\; \text{By Lemma 32}
\end{aligned}$$

Now

$$\begin{aligned}
\overline{\epsilon^\star} &= \bar{\epsilon}_r\prod_{i=0}^{r-1}\bar{\epsilon}_i^{\lceil d/(\epsilon_i(q^{2^i}+1))\rceil}\\
&\ge \bar{\epsilon}_r\left(\prod_{i=0}^{r-1}\bar{\epsilon}_i\right)\prod_{i=0}^{r-1}\bar{\epsilon}_i^{d/(\epsilon_i(q^{2^i}+1))}\\
&\ge \frac{1}{3}\left(\prod_{i=0}^{r-1}\frac{1}{q^{2^i}+1}\right)\left(\prod_{i=0}^{r-1}(\bar{\epsilon}_i)^{1/(\epsilon_i(q^{2^i}+1))}\right)^d\\
&= \frac{1}{3}\frac{q-1}{q^{2^r}-1}2^{-\pi_{q,\epsilon}\cdot d} \ge \frac{2^{-\pi_{q,\epsilon}\cdot d}}{\Theta(d^2)}.
\end{aligned}$$

□

Proposition 52 in Appendix B will help us choose ϵ_i in Theorem 38 to obtain different results. We first prove

Corollary 39. *Let $q < d+1$ be a power of prime. For any integer m such that $1 \le m \le q$ we have:*

For

$$\overline{\epsilon^\star} \;=\; \left(1-\frac{m}{q+1}\right)^{\frac{1}{m}\left(1+\frac{1}{\Theta(q)}\right)d}$$

we have

$$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star}) \le (q+1)^{\frac{d}{m}\left(1+\frac{1}{\Theta(q)}\right)}\cdot t.$$

The following Table shows the results for different choices of m (ignoring the small terms)

m	$\overline{\epsilon^\star}$	$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star})/t$
$m=1$	$\left(1-\frac{1}{q+1}\right)^d$	$(q+1)^d$
$m=\log(q+1)/c$, $c=o(\log(q+1))$	$\left(1-\frac{1}{q+1}\right)^d$	2^{cd}
$m=o(q)$, $\omega(\log(q+1))$	$\left(1-\frac{1}{q+1}\right)^d$	$\left(1+\frac{\ln(q+1)}{m}\right)^d$
$m=c(q+1)$, $c<1$, $c=\Theta(1)$	$\left(1-\frac{\ln(1/(1-c))}{c(q+1)}\right)^d$	$\left(1+\frac{\ln(q+1)}{c(q+1)}\right)^d$
$m=(q+1)-(q+1)/c$, $c=\omega(1)$	$\left(1-\frac{\ln c}{q+1}\right)^d$	$\left(1+\frac{\ln(q+1)}{q+1}\right)^d$
$m=(q+1)-c$, $c=\Theta(1)$	$\left(1-\frac{\ln(q+1)}{q+1}\right)^d$	$\left(1+\frac{\ln(q+1)}{q+1}\right)^d$

Proof. We use Theorem 38 and Proposition 52 in Appendix B. We choose $\epsilon_i(q+1)=m$, for $i=0,1,2,\ldots,r-1$ and $\epsilon_r=1/3$. □

The reason for the choice of such ϵ_i in Theorem 39 is explained in Appendix C.

The following corollary gives the minimal possible size of a tester that can be obtained from Theorem 38

Corollary 40. *Let $q<d+1$. Let*

$$c_q=\sum_{i=0}^{\infty}\frac{\log(q^{2^i}+1)}{q^{2^i}}=\Theta\left(\frac{\log q}{q}\right).$$

For

$$\overline{\epsilon^\star}=2^{-c_q d}/\Theta(d^2)$$

we have

$$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star})\le\Theta(d^5)\cdot 2^{c_q d}\cdot t$$

In particular we have following values of c_q

q	c_q
2	1.659945821
3	1.116191294
4	0.867464571
5	0.719921672
7	0.548433289

Proof. We use Theorem 38. We choose $\epsilon_i(q^{2^i}+1) = q^{2^i}$ for $i = 0, 1, \ldots, r-1$ and $\epsilon_r = 1/3$. □

In Theorem 19 we have shown that there is no $(\mathcal{HLF}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\overline{\epsilon}$-tester of density greater than $\overline{\epsilon}_{min} = (1-1/q)^d$. We now use Theorem 38 to show that one can get a tester with density $\overline{\epsilon} = (1 - 1/q - 1/poly(q))^d$ and size $q^{O(d)} \cdot t$.

Corollary 41. *Let $q < d+1$. For every $(\log d)/d \le \delta \le 1/q^2$ we have: For*

$$\overline{\epsilon^\star} = \left(1 - \frac{1}{q} - c_1\delta\right)^d,$$

$$\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon^\star}) \le \left(\frac{c_2 \log_q(1/\delta)}{\delta}\right)^d \cdot t$$

for some constants c_1 and c_2.

In particular, for

$$\overline{\epsilon^\star} = \left(1 - \frac{1}{q} - \frac{1}{poly(q)}\right)^d,$$

$$\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon^\star}) \le q^{O(d)} \cdot t.$$

Proof. Consider the integer r in Theorem 38. Let $k < r$ be constant that will be determined later such that $(\log d)/d < 2^k/q^{2^{k+1}}$. Apply Theorem 38 and consider the case where $\epsilon_i(q^{2^i}+1) = 1$ for $i = 0, \ldots, k-1$, $m_k = \epsilon_k(q^{2^k}+1) = 2^k = \lfloor \log(q^{2^k}+1)/\log q \rfloor$, $\epsilon_i = 1/2$ for $i \ge k+1$ and $\epsilon_r = 2/3$.

Then by Theorem 38 and Proposition 52 in Appendix B,

$$
\begin{aligned}
\overline{\epsilon^\star}^{1/d} &\geq \left(\frac{1}{\Theta(d^2)}\right)^{1/d} \cdot \left(\prod_{i=0}^{k-1}\left(1-\frac{1}{q^{2^i}+1}\right)\right) \cdot \left(1-\frac{m_k}{q^{2^k}+1}\right)^{\frac{1}{m_k}} \cdot \prod_{i=k+1}^{r}\left(\frac{1}{2}\right)^{\frac{2}{q^{2^i}+1}} \\
&= \left(\frac{1}{\Theta(d^2)}\right)^{1/d} \cdot \left(1-\frac{1}{q}\right)\left(1-\frac{1}{q^{2^k}}\right)^{-1} \cdot \left(1-\frac{1}{q^{2^k}+1}-\Theta\left(\frac{2^k}{q^{2^{k+1}}}\right)\right) \cdot \left(1-\Theta\left(\frac{1}{q^{2^{k+1}}}\right)\right) \\
&= \left(\frac{1}{\Theta(d^2)}\right)^{1/d} \left(1-\frac{1}{q}\right)\left(1+\frac{1}{q^{2^k}}+\Theta\left(\frac{1}{q^{2^{k+1}}}\right)\right)\left(1-\frac{1}{q^{2^k}+1}-\Theta\left(\frac{2^k}{q^{2^{k+1}}}\right)\right) \\
&= \left(1-\Theta\left(\frac{\log d}{d}\right)\right)\left(1-\frac{1}{q}\right)\left(1-\Theta\left(\frac{2^k}{q^{2^{k+1}}}\right)\right) \\
&= 1-\frac{1}{q}-\Theta\left(\frac{2^k}{q^{2^{k+1}}}\right)
\end{aligned}
$$

Denote the small term $W_k = 2^k/q^{2^{k+1}}$ and choose k such that $W_k \leq \delta$ and $W_{k-1} > \delta$. Then by Theorem 38 and Proposition 52 in Appendix B,

$$
\begin{aligned}
\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon^\star})^{1/d} &\leq (\Theta(d^5))^{1/d}\left(\prod_{i=0}^{k-1}(q^{2^i}+1)\right)(q^{2^k}+1)^{\frac{1}{m_k}} \prod_{i=k+1}^{r}(q^{2^i}+1)^{\frac{2}{q^{2^i}+1}} \\
&\leq \frac{q^{2^k}-1}{q-1}\Theta(q) = \Theta(q^{2^k}) = \Theta\left(\frac{2^{k-1}}{W_{k-1}}\right) \\
&= \Theta\left(\frac{\log_q(1/W_{k-1})}{W_{k-1}}\right) = O\left(\frac{\log_q(1/\delta)}{\delta}\right).
\end{aligned}
$$

□

The last result in this subsection is

Theorem 42. *All the above testers are componentwise and linear but not reducible and not symmetric.*

Proof. All the testers built in the previous sections and subsections are componentwise and linear and since all the constructions used in Theorem 38 preserve those two properties, the testers in this subsection are componentwise and linear.

The construction in Theorem 38 uses the tester constructed in *3* of Lemma 12 which is not reducible ($l_\infty(1) = 0$). It also uses construction *4* of Lemma 11 that, by Lemma 9, does not preserve the symmetric property. □

6 Almost Linear Time Constructions and Locally Explicit

In this section we show that a dense tester $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_q,\mathbb{F})$-$\bar{\epsilon}$-tester of size $s = poly(d/\epsilon)\cdot t$ can be constructed in almost linear time in s and p and is locally explicit. Here p is the characteristic of the field which is $O(1)$ for all the applications we have in [3].

6.1 Dense Testers for Very Small t and Large q

In this section give linear time constructions for small t.

In Theorem 16 we showed that the size of any $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}$-tester is at least $\Omega((d/\epsilon)\cdot t)$. In Theorem 19 we showed that the best possible density one can get for $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}$-tester is $\epsilon \ge d/q$. In this section we show that for small $t = o(q)$ one can in almost linear time build testers of size poly$(d/\epsilon)\cdot t$ of density $d/q + o(d/q)$.

We will abuse the notations $\nu_R^{\mathcal{P}}, \nu_R^{\mathcal{HP}}$ or ν_R and identify every inequality in $\nu_R^{\mathcal{P}}, \nu_R^{\mathcal{HP}}$ or ν_R with its corresponding construction. For example, by the first inequality in (10) below we mean the following statement: From a $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^2},\mathbb{F})$-$\bar{\epsilon}_2$-tester of size s_1 a $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F})$-$\bar{\epsilon}_1\bar{\epsilon}_2$-tester of size $s_2 := s_1\lfloor (dt-d+1)/(2\epsilon_1)\rfloor$ can constructed in almost linear time. See Important Note 1 in Subsection 3.3.

Note that just reading the elements of the field $\mathbb{F}_{q^t}$ takes time $t\log q$. Therefore one cannot expect any time complexity that is better than $\tilde{O}(t)$.

Theorem 43. *The following $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}$-tester can be constructed in deterministic time $T\cdot poly(\log(qtd/\epsilon)) = \tilde{O}(T)$ and any entry of any map in the tester can be constructed and computed in time $T'\cdot poly(\log(qtd/\epsilon)) = \tilde{O}(T')$.*

	Size$= O(\cdot)$	ϵ	t	T	T'
1)	$\frac{d}{\epsilon}\cdot t$	$\epsilon \ge \frac{d(t-1)}{q}$	ANY	$Size$	t
2)	$\frac{d^2}{\epsilon(\epsilon-d/q)}\cdot t$	$\epsilon \ge \frac{d}{q}+\frac{dt-d+1}{q^2-q}$	$< q-1$	$Size + p^{1/2}$	$t+p^{1/2}$
3)	$\frac{1}{c}\left(\frac{d}{\epsilon}\right)^2\cdot t$	$\epsilon \ge (1+c)\frac{d}{q}$	$< c(q-1)$	$Size + p^{1/2}$	$t+p^{1/2}$
4)	$\left(\frac{d}{\epsilon}\right)^3$	$\epsilon = \frac{d}{q}+o\left(\frac{d}{q}\right)$	$= o(q)$	$Size$	$t+p^{1/2}$
5)	$\frac{1}{c^2}\left(\frac{d}{\epsilon}\right)^3\cdot t$	$O\left(\frac{d}{q}\right) = \epsilon \ge (1+c)\frac{d}{q}$	$\frac{q}{\log q} < t < \frac{c}{2}q^{\frac{c}{2}(q-1)-3}$	$Size$	t
6)	$\left(\frac{d}{\epsilon}\right)^4\left(\log^3\frac{d}{\epsilon}\right)\cdot t$	$O\left(\frac{d}{q}\right) = \epsilon \ge \frac{d}{q}+o\left(\frac{d}{q}\right)$	$q^{4c'q/\log q} < t < q^{q^{c'q/\log q}}$	$Size$	t

for any $1 \ge c \ge 0$ and any constant $c' > 1$.

Proof. By Corollary 13 we have for $\epsilon \ge d(t-1)/q$, a tester of size $O((d/\epsilon)\cdot t)$ can be constructed in linear time in dt/ϵ and any entry of any map in the tester can be constructed and computed in time $\tilde{O}(t)$. This implies result 1.

We now prove result 2. Consider the field $\mathbb{F}_{q^2}$. Then by (6), $2N_q(2) = q^2 - q$. By Lemma 14 and Corollary 13, for any

$$\epsilon_1 \geq \frac{dt-d+1}{q^2-q} \text{ and } \epsilon_2 \geq \frac{d}{q}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}_1\bar{\epsilon}_2) \leq \left\lceil \frac{dt-d+1}{2\epsilon_1} \right\rceil \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^2}, \bar{\epsilon}_2) \leq \left\lceil \frac{dt-d+1}{2\epsilon_1} \right\rceil \left\lceil \frac{d}{\epsilon_2} \right\rceil. \tag{10}$$

Notice that for $t < q-1$,

$$\frac{dt-d+1}{q^2-q} < \frac{d}{q}.$$

We now distinguish between two cases. When $2d/q \leq \epsilon$ we substitute $\epsilon_1 = \epsilon_2 = \epsilon/2$ and get

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \leq O\left(\left(\frac{d}{\epsilon}\right)^2 \cdot t\right) = O\left(\left(\frac{d^2}{\epsilon(\epsilon - d/q)}\right) \cdot t\right).$$

When

$$\frac{d}{q} + \frac{dt-d+1}{q^2-q} \leq \epsilon < \frac{2d}{q}$$

we substitute $\epsilon_2 = d/q$ and $\epsilon_1 = \epsilon - \epsilon_2$ and get

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \leq O\left(\left(\frac{d^2}{\epsilon(\epsilon - d/q)}\right) \cdot t\right).$$

The time complexity follows from Lemma 14 and Lemma 1 (for constructing $\mathbb{F}_{q^2}$).

We now prove result 3. For $\epsilon \geq (1+c)d/q$ and $t < c(q-1)$ where $1 \geq c \geq 0$ is any constant we have $\epsilon \geq d/q + (dt-d+1)/(q^2-q)$ and therefore by (2),

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \leq O\left(\frac{1}{c}\left(\frac{d}{\epsilon}\right)^2 \cdot t\right).$$

To prove result 4, we use (10) for $\epsilon_2 = d/q$ and $\epsilon_1 = O(dt/q^2)$. Notice here that $Size = O(q^3)$ which is much larger than the extra term $\tilde{O}(p^{1/2})$.

To prove result 5, we use Lemma 14 with $k = (c/2)(q-1) - 1$, $\epsilon_1 = (c/2)(d/q)$ and $\epsilon_2 = \epsilon - \epsilon_1 \geq (1 + c/2)(d/q)$. Now since

$$\epsilon_1 = \frac{c}{2}\frac{d}{q} \geq \frac{dt}{q^{k-1}} \geq \frac{dt-d+1}{q^{k-1}} \geq \frac{dt-d+1}{k \cdot N_q(k)}$$

we get

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon_1\bar\epsilon_2)\le \left\lceil \frac{dt-d+1}{\epsilon_1 k}\right\rceil \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^k},\bar\epsilon_2).$$

By result 3 we have $\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^k},\bar\epsilon_2)=O((1/c)(d/\epsilon_2)^2k)$ and therefore

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon)=O\left(\frac{1}{c^2}\left(\frac{d}{\epsilon}\right)^3\cdot t\right).$$

The time complexity is $O((1/c^2)(d/\epsilon)^3t+q^3p^{1/2}+q^4\log^2 q)=\tilde O(Size)$.

To prove result 6, take $c=\Theta(1/\log q)$ such that $k:=q^{c'q/\log q}+3<(c/2)q^{(c/2)(q-1)-3}$, $\epsilon_1=d/(q\log q)$ and $\epsilon_2=(1+c)(d/q)$. Since

$$kN_q(k)\ge q^{k-1}\ge(\log q)qt\ge\frac{dt-d+1}{\epsilon_1}$$

by Lemma 14 and (5), for $\epsilon=d/q+\Theta(d/(q\log q))$,

$$\begin{aligned}\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon) &\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar\epsilon_1\bar\epsilon_2)\le \left\lceil \frac{dt-d+1}{\epsilon_1 k}\right\rceil \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^k},\bar\epsilon_2)\le O(q(\log q)t\cdot(\log q)^2q^3)\\ &= O\left(\left(\frac{d}{\epsilon}\right)^4\log^3\left(\frac{d}{\epsilon}\right)\cdot t\right).\end{aligned}$$

□

The above Theorem give dense testers for $\epsilon=O(d/q)$. For $\epsilon=\omega(d/q)$ we have

Theorem 44. *The following $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar\epsilon$-tester can be constructed in deterministic time $T\cdot poly(\log(qtd/\epsilon))=\tilde O(T)$ and any entry in any map in the tester can be constructed and computed in time $T'\cdot poly(\log(qtd/\epsilon))=\tilde O(T')$*

	Size$=O(\cdot)$	ϵ	t	T	T'
1)	$\frac{d}{\epsilon}\cdot t$	$\epsilon\ge(t-1)\frac{d}{q}$	ANY	*Size*	t
2)	$\left(\frac{d}{\epsilon}\right)^2\cdot t$	$\epsilon\ge 2\eta\frac{d}{q}$	$\le\eta q^{\eta-1}$	$Size+\eta^3p^{1/2}+\eta^4$	$t+\eta^3p^{1/2}+\eta^4$
3)	$\left(\frac{d}{\epsilon}\right)^3\cdot t$	$\epsilon\ge 3\eta\frac{d}{q}$	$q^{4\eta}\le t\le q^{\eta q^{\eta-1}-2}$	*Size*	t
4)	$\left(\frac{d}{\epsilon}\right)^4\cdot t$	$\epsilon\ge 4\eta\frac{d}{q}$	$q^{4\eta q^{\eta-1}}\le t\le q^{q^{\eta q^{\eta-1}-2}-2}$	*Size*	t

where $\eta\le q/d$ is any integer. In particular for $\epsilon\ge 34\cdot d/q$ and any $t\le q^{q^q}$ a $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar\epsilon$-tester of size

$$S=O\left(\left(\frac{d}{q}\right)^4\cdot t\right)$$

can be constructed in deterministic time $\tilde{O}(S+p^{1/2})$ and any entry of any map in the tester can be constructed and computed in time $\tilde{O}(t+p^{1/2})$.

Proof. Result 1 is the same as result 1 in Theorem 43.

We now prove result 2. Consider the field $\mathbb{F}_{q^{\eta+1}}$. Then by (7), $(\eta+1)N_q(\eta+1)\ge q^\eta$. By Lemma 14 and Corollary 13, for any

$$\epsilon_1 \ge \frac{dt-d+1}{q^\eta} \text{ and } \epsilon_2 \ge \eta\frac{d}{q}$$

we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1\bar{\epsilon}_2) \le \left\lceil \frac{dt-d+1}{(\eta+1)\epsilon_1}\right\rceil \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^{\eta+1}},\bar{\epsilon}_2) \le \left\lceil \frac{dt-d+1}{(\eta+1)\epsilon_1}\right\rceil \left\lceil \frac{d}{\epsilon_2}\eta\right\rceil. \tag{11}$$

Notice that for $t\le \eta q^{\eta-1}$,

$$\frac{dt-d+1}{q^\eta} < \eta\frac{d}{q}.$$

When $2\eta d/q\le\epsilon$ we substitute $\epsilon_1=\epsilon_2=\epsilon/2$ and get

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le O\left(\left(\frac{d}{\epsilon}\right)^2\cdot t\right).$$

We now prove result 3. Consider the field $\mathbb{F}_{q^k}$ where $k=\eta q^{\eta-1}$. Then by (7), $kN_q(k)\ge q^{k-1}\ge (dt-d+1)/\epsilon_1$ where $\epsilon_1\ge\eta(d/q)$. Let $\epsilon_2\ge 2\eta(d/q)$. By Lemma 14 and result 2 we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1\bar{\epsilon}_2) \le \left\lceil \frac{dt-d+1}{k\epsilon_1}\right\rceil \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^k},\bar{\epsilon}_2) \le \left\lceil \frac{dt-d+1}{k\epsilon_1}\right\rceil \cdot O\left(\left(\frac{d}{\epsilon_2}\right)^2 k\right). \tag{12}$$

When $3\eta d/q\le\epsilon$ we substitute $\epsilon_1=\epsilon/3$ and $\epsilon_2=2\epsilon/3$ and get

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) \le O\left(\left(\frac{d}{\epsilon}\right)^3\cdot t\right).$$

We now prove result 4. Consider the field $\mathbb{F}_{q^k}$ where $k=q^{\eta q^{\eta-1}-2}$. Then by (7), $kN_q(k)\ge q^{k-1}\ge (dt-d+1)/\epsilon_1$ where $\epsilon_1\ge\eta(d/q)$. Let $\epsilon_2\ge 3\eta(d/q)$. By Lemma 14 and result 3 we have

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}_1\bar{\epsilon}_2) \le \left\lceil \frac{dt-d+1}{k\epsilon_1}\right\rceil \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^k},\bar{\epsilon}_2) \le \left\lceil \frac{dt-d+1}{k\epsilon_1}\right\rceil \cdot O\left(\left(\frac{d}{\epsilon_2}\right)^3 k\right). \tag{13}$$

When $4\eta d/q \le \epsilon$ we substitute $\epsilon_1 = \epsilon/4$ and $\epsilon_2 = 3\epsilon/4$ and get

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \le O\left(\left(\frac{d}{\epsilon}\right)^4 \cdot t\right).$$

The final result in the Theorem follows from results 2, 3 and 4 with $\eta = 17, 4, 2$ respectively. □

6.2 Dense Testers for any t and Large q

In this section we first prove

Theorem 45. *Let $q \ge d + 1$, $c > 0$ be a constant and*

$$\epsilon \ge 34 \cdot \frac{d}{q}.$$

A $(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\bar{\epsilon}$-tester of size

$$s = \left(\frac{d}{\epsilon}\right)^4 \cdot t$$

can be constructed in time $T = \tilde{O}(s + p^{1/2})$ and any entry of any map in the tester can be constructed and computed in time $\tilde{O}(t + p^{1/2})$.

Proof. By Theorem 44 we may assume that $t \ge w := q^{q^q}$. Let $t_1 = \lceil \log_q t \rceil + 2$ and $t_2 = c_1 q^k$ where $c_1 < 1$ is any small constant such that $c_1 q^{k-1}$ is an integer and $c_1 q^k \ge \lceil \log_q t_1 \rceil + 2 \ge c_1 q^{k-1}$. Since for $\epsilon_1 = \epsilon/4$

$$t_1 N_q(t_1) \ge q^{t_1 - 1} \ge qt \ge \frac{dt - d + 1}{\epsilon_1}$$

and

$$t_2 N_q(t_2) \ge q^{t_2 - 1} \ge qt_1 \ge \frac{dt_1 - d + 1}{\epsilon_1}$$

by Lemma 14 and Lemma 31

$$\nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \bar{\epsilon}) \le \left\lceil \frac{dt}{\epsilon_1 t_1} \right\rceil \cdot \left\lceil \frac{dt_1}{\epsilon_1 t_2} \right\rceil \cdot \nu^{\mathcal{P}}_{\mathbb{F}_q}(d, \mathbb{F}_{q^{t_2}}, \overline{\epsilon - 2\epsilon_1}) = O\left(\left(\frac{d}{\epsilon}\right)^4 \cdot t\right).$$

Now we prove that the above can be constructed in time T. If $t \le w$ then the time complexity follows from Theorem 44. Now suppose $t \ge w$. By Lemma 14 the reduction to $\mathbb{F}_{q^{t_2}}$ can be done in time $\tilde{O}(s + t_1^3 p^{1/2} + t_1^4) = \tilde{O}(s)$. By Lemma 31 a symmetric $(\mathcal{P}(\mathbb{F}_q, n, d), \mathbb{F}_{q^{t_2}}, \mathbb{F}_q)$-$(\bar{\epsilon} - 2\epsilon_1)$-tester of size $s = 15(d/(\bar{\epsilon} - 2\epsilon_1))^2 t$ exists. We will construct it by exhaustive search. We exhaustively search for linear maps $L=\{l_1,\ldots,l_s\}$ where $s=15(d/(\epsilon-2\epsilon_1))^2t_2\le q^3\log_q\log_q t\le(\log_q\log_q t)^4$ in $\mathbb{F}^*_{q^{t_2}}$, and check if every $\lfloor(\epsilon-2\epsilon_1)|L|\rfloor+1$ elements in L is a tester. Verifying whether a set of maps is a tester can be done in polynomial time in s [4]. The number of all possible sets L and subsets of L is at most

$$\binom{|\mathbb{F}^*_{q^{t_2}}|}{s}2^s\le q^{st_2}\le q^{2(\log_q\log_q t)^6}.$$

Now notice that $q\ge 34d/\epsilon\ge 68$ and since $2(\log_q\log_q t)^6<\log_q t$ for $t\ge q^{q^q}$ and $q\ge 68$ we have $q^{2(\log_q\log_q t)^6}<t$. Therefore the time complexity of the exhaustive search is less than s. This finishes the proof that the above can be constructed in time T.

Now we show that any entry of any map in the tester can be constructed and computed in time $\tilde{O}(t+p^{1/2})$. If $t\le w$ then the result follows from Theorem 44. Now suppose $t\ge w$. Notice that $d/\epsilon\le q=\tilde{O}(1)$ with respect to t and therefore $O(s+p^{1/2})=\tilde{O}(t)$. This completes the proof. □

We now prove

Theorem 46. *Let $q\ge d+1$, $34\ge c\ge 1+34/q$ and $\epsilon>0$ such that*

$$34\frac{d}{q}\ge\epsilon=c\frac{d}{q}\ge\frac{d}{q}+\frac{34d}{q^2}.$$

A $(\mathcal{P}(\mathbb{F}_q,n,d),\mathbb{F}_{q^t},\mathbb{F}_q)$-$\bar{\epsilon}$-tester of size

$$s=\frac{1}{(1-c)^4}\left(\frac{d}{\epsilon}\right)^5\cdot t$$

can be constructed in deterministic polynomial time $\tilde{O}(s)$ and any entry of any map in the tester can be constructed and computed in time $\tilde{O}(t+p^{1/2})$..

Proof. Let $\epsilon_1=d/q$ and $\epsilon_2=(c-1)d/q$. By Lemma 4, (5), Corollary 13 and Theorem 45 we have

$$\begin{aligned}
\nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\bar{\epsilon}) &\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^{2t}},\overline{\epsilon_1+\epsilon_2})\\
&\le \nu^{\mathcal{P}}_{\mathbb{F}_q}(d,\mathbb{F}_{q^2},\overline{\epsilon_1})\cdot\nu^{\mathcal{P}}_{\mathbb{F}_{q^2}}(d,\mathbb{F}_{q^{2t}},\overline{\epsilon_2})\\
&\le q\cdot\left(\frac{d}{\epsilon_2}\right)^4 t\\
&\le q\cdot\left(\frac{d}{(c-1)(d/q)}\right)^4 t\\
&\le \frac{q^5}{(c-1)^4}t=O\left(\frac{1}{(c-1)^4}\left(\frac{d}{\epsilon}\right)^5\right)\cdot t.
\end{aligned}$$

Notice here that $s \geq d/\epsilon \geq q/34 \geq p/34$. This is why $p^{1/2}$ does not appear in the complexity.

The complexity of constructing and computing any entry of any map in the tester follows from Corollary 13 and Theorem 45. $\square$

6.3 Dense Testers for any t and Small q

The following is Theorem 38 with the time complexity of constructing such tester

Theorem 47. *Let $q < d^{1/2}$ be a power of prime and t be any integer. Let r be an integer such that $q^{2^{r-1}} < 9d \leq q^{2^r}$. Let $\boldsymbol{\epsilon} = (\epsilon_0, \ldots, \epsilon_{r-1}, \epsilon_r)$ where $\epsilon_i(q^{2^i}+1) \leq q^{2^i}$ is an integer for $i = 0, 1, \ldots, r-1$ and $2/3 \geq \epsilon_r \geq 1/3$. Let*

$$c_{q,\boldsymbol{\epsilon}} := \sum_{i=0}^{r-1} \frac{\log(q^{2^i}+1)}{\epsilon_i(q^{2^i}+1)}$$

and

$$\pi_{q,\boldsymbol{\epsilon}} := \sum_{i=0}^{r-1} \frac{-\log(1-\epsilon_i)}{\epsilon_i(q^{2^i}+1)}.$$

Then for

$$\overline{\epsilon^\star} := \bar{\epsilon}_r \prod_{i=0}^{r-1} \bar{\epsilon}_i^{\lceil d/(\epsilon_i(q^{2^i}+1))\rceil} \geq \frac{2^{-\pi_{q,\boldsymbol{\epsilon}}\cdot d}}{\Theta(d^2)},$$

a $(\mathcal{HLF}(\mathbb{F}_q, n, d), \mathbb{F}_{q^t}, \mathbb{F}_q)$-$\epsilon^\star$-tester of size

$$s := \Theta(d^6) \cdot 2^{c_{q,\boldsymbol{\epsilon}}\cdot d} \cdot t$$

can be constructed in time $\tilde{O}(s) = \tilde{O}(2^{c_{q,\boldsymbol{\epsilon}}\cdot d} \cdot t)$. The time complexity of constructing and computing any entry in any map in the tester is equal to $\tilde{O}(c_{q,\boldsymbol{\epsilon}} d + t)$.

Proof. We will go over the construction and compute the total time and the time for constructing and computing any entry of any map. We have used the following results that follows from Lemma 4, Corollary 6, Lemma 11 and 12.

1. $\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^{t_1}}, \bar{\epsilon}) \leq \nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^{t_1 t_2}}, \bar{\epsilon})$.
2. $\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^{t_1 t_2}}, \bar{\epsilon}_1\bar{\epsilon}_2) \leq \nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^{t_1}}, \bar{\epsilon}_1) \cdot \nu_{\mathbb{F}_{q^{t_1}}}(d, \mathbb{F}_{q^{t_1 t_2}}, \bar{\epsilon}_2)$.
3. $\nu_{\mathbb{F}_q}(d_1 + d_2, \mathbb{F}_{q^t}, \bar{\epsilon}_1\bar{\epsilon}_2) \leq \nu_{\mathbb{F}_q}(d_1, \mathbb{F}_{q^t}, \bar{\epsilon}_1) \cdot \nu_{\mathbb{F}_q}(d_2, \mathbb{F}_{q^t}, \bar{\epsilon}_2)$.
4. $\nu_{\mathbb{F}_q}(d, \mathbb{F}_{q^2}, \bar{\epsilon}) \leq q + 1$ for any $\epsilon < 1$ such that $\epsilon(q+1)$ is an integer and $d \leq \epsilon(q+1)$.

Let $\eta_i = \epsilon_i(q^{2^i}+1)$. Then the following (from the proof of Theorem 38) shows how to construct such tester

$$\begin{aligned}
\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star}) &\le \nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^{t\cdot 2^r}},\overline{\epsilon^\star}) \quad \text{By (1.)} && (14)\\
&\le \left(\prod_{i=0}^{r-1}\nu_{\mathbb{F}_{q^{2^i}}}\left(d,\mathbb{F}_{q^{2^{i+1}}},\bar{\epsilon}_i^{\lceil d/\eta_i\rceil}\right)\right)\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r) \quad \text{By (2.)} && (15)\\
&\le \left(\prod_{i=0}^{r-1}\nu_{\mathbb{F}_{q^{2^i}}}(\eta_i,\mathbb{F}_{q^{2^{i+1}}},\bar{\epsilon}_i)^{\lfloor d/\eta_i\rfloor}\cdot\nu_{\mathbb{F}_{q^{2^i}}}(d-\eta_i\lfloor d/\eta_i\rfloor,\mathbb{F}_{q^{2^{i+1}}},\bar{\epsilon}_i)\right)\\
&\qquad \cdot\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r) \quad \text{By (3.)} && (16)\\
&\le \left(\prod_{i=0}^{r-1}\left(q^{2^i}+1\right)^{\lceil d/\eta_i\rceil}\right)\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r) \quad \text{By (4.)} && (17)\\
&\le \left(\left(\prod_{i=0}^{r-1}\left(q^{2^i}+1\right)\right)2^{c_{q,\epsilon}\cdot d}\right)\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r)\\
&\le \frac{q^{2^r}-1}{q-1}\nu_{\mathbb{F}_{q^{2^r}}}(d,\mathbb{F}_{(q^{2^r})^t},\bar{\epsilon}_r)\cdot 2^{c_{q,\epsilon}\cdot d}\\
&\le \Theta(d^6)\cdot 2^{c_{q,\epsilon}\cdot d}\cdot t \quad \text{By Theorem 45} && (18)
\end{aligned}$$

In (14) and (15) we need to construct $\mathbb{F}_{q^{2^r t}},\mathbb{F}_{q^{2^{r-1}t}},\ldots,\mathbb{F}_{q^{2t}}$ from $\mathbb{F}_{q^t}$ which by Lemma 1 takes time $\tilde{O}(r(p^{1/2}2^{3r}+2^{4r}))$. Since $p<q<d^{1/2}$, $2^r\le 2\log_q(9d)$ and $c_{q\boldsymbol{\epsilon}}\ge 1/q$ (see Corollary 39) the time complexity of (14) is $\tilde{O}(p^{1/2})=\tilde{O}(c_{q,\boldsymbol{\epsilon}}d)$. In (15), by Lemma 5, the time of the construction is linear in the sum of time of the construction of each tester $\mathbb{F}_{q^{2^{i+1}}}\to\mathbb{F}_{q^{2^i}}$ and in the size which is the product of the sizes. Constructing and computing any entry in any map is linear in the sum of constructing and computing any entry of any map in each tester. The same is true for (16). In (17), by Lemma 12, the testers that map $\mathbb{F}_{q^{2^{i+1}}}$ to $\mathbb{F}_{q^{2^i}}$, $i=1,\ldots,r-1$, are constructed in time $\tilde{O}(\eta_i/\epsilon_i)=\tilde{O}(d^2)$ and constructing and computing any entry of any map in the testers takes time $\tilde{O}(1)$. Computing each map in this tester involves substituting an element of $\mathbb{F}_{q^{2^i}}$ in a quadratic polynomial which takes time $poly(2^i,\log q)=\tilde{O}(1)$. In (18) we use Theorem 45 (rather than Lemma 32) that takes construction time $\tilde{O}(d^4t+p^{1/2})=\tilde{O}(d^4t)$. Constructing and computing any entry of any map in this tester takes time $\tilde{O}(t+p^{1/2})=\tilde{O}(t+c_{q,\boldsymbol{\epsilon}}d)$. Now the time for the construction is clearly equal to $O(poly(d)\times s)$ where s is the size of the tester and therefore is equal to $\tilde{O}(2^{c_{q,\boldsymbol{\epsilon}}\cdot d}\cdot t)$.

Using $T(\cdot)$ for the time of constructing and computing any entry in any map in the tester, by the above discussion, we have

$$\begin{aligned}
T_{\mathbb{F}_q}(d, \mathbb{F}_{q^t}, \overline{\epsilon^\star}) &= T_{\mathbb{F}_q}(d, \mathbb{F}_{q^{t\cdot 2^r}}, \overline{\epsilon^\star}) + \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) \\
&= \left(\sum_{i=0}^{r-1} T_{\mathbb{F}_{q^{2^i}}} \left(d, \mathbb{F}_{q^{2^{i+1}}}, \bar{\epsilon}_i^{\lceil d/\eta_i \rceil}\right)\right) + T_{\mathbb{F}_{q^{2^r}}}(d, \mathbb{F}_{(q^{2^r})^t}, \bar{\epsilon}_r) + O(r) + \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) \\
&= \left(\sum_{i=0}^{r-1} \lfloor d/\eta_i \rfloor \cdot T_{\mathbb{F}_{q^{2^i}}}(\eta_i, \mathbb{F}_{q^{2^{i+1}}}, \bar{\epsilon}_i) + T_{\mathbb{F}_{q^{2^i}}}(d - \eta_i \lfloor d/\eta_i \rfloor, \mathbb{F}_{q^{2^{i+1}}}, \bar{\epsilon}_i) \right) \\
&\qquad + T_{\mathbb{F}_{q^{2^r}}}(d, \mathbb{F}_{(q^{2^r})^t}, \bar{\epsilon}_r) + \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) \\
&= \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) + T_{\mathbb{F}_{q^{2^r}}}(d, \mathbb{F}_{(q^{2^r})^t}, \bar{\epsilon}_r) + \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) \\
&= \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) + \tilde{O}(t + c_{q,\boldsymbol{\epsilon}} d) + \tilde{O}(c_{q,\boldsymbol{\epsilon}} d) = \tilde{O}(c_{q,\boldsymbol{\epsilon}} d + t).
\end{aligned}$$

□

7 Appendices

7.1 Appendix A

We remind the reader that $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_t) \in \mathbb{F}_q^t$ is of period t if

$$\boldsymbol{\lambda}^0 := \boldsymbol{\lambda},\ \boldsymbol{\lambda}^1 := (\lambda_t, \lambda_1, \ldots, \lambda_{t-1}),\ \boldsymbol{\lambda}^2 := (\lambda_{t-1}, \lambda_t, \lambda_1, \ldots, \lambda_{t-2}), \cdots, \boldsymbol{\lambda}^{t-1} := (\lambda_2, \lambda_3, \ldots, \lambda_t, \lambda_1)$$

are distinct.

By the proof of Lemma 2 it is enough to find a total order on $r = q^{t-2}/2t$ vectors $\boldsymbol{\lambda} \in \mathbb{F}_q^t$ of period t and show how to access the mth vector in time $\tilde{O}(\log m + t^2)$.

Define $\mathcal{S}$ the set of vectors $(0, 0, \overset{k}{\ldots}, 0, \alpha_1, \ldots, \alpha_{t-k})$ where no k consecutive zeros occurs in $(\alpha_1, \ldots, \alpha_{t-k})$. The integer k will be determined later. The following result is trivial

Claim 48. *The vectors in $\mathcal{S}$ are of period t.*

Let $M(k, n)$ be the number vectors $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ where no k consecutive zeros occurs in $\boldsymbol{\alpha}$. We denote the set of all such vectors by $S(k, n)$. Notice that $\mathcal{S} = \{0\}^k \times S(k, t-k)$. Then

Claim 49. *We have: $M(k, n) = q^n$ for $n \le k-1$, $M(k, k) = q^k - 1$ and*

$$M(k, n) = q \cdot M(k, n-1) - (q-1) \cdot M(k, n-k-1). \tag{19}$$

Also

$$M(k, n) = (q-1) \cdot \sum_{i=1}^{k} M(k, n-i).$$

Proof. The number of vectors in $S(k, n-1)$ that ends with one of the vectors in $(\mathbb{F}_q \backslash \{0\}) \times \{0\}^{k-1}$ is $(q-1) \cdot M(k, n-k-1)$. Denote the set of such vectors by $S'(k, n-1)$. Notice that $S(k, n) = S'(k, n-1) \times (\mathbb{F}_q \backslash \{0\}) \cup (S(k, n-1) \backslash S'(k, n-1)) \times \mathbb{F}_q$. This implies the first result.

For the second result notice that

$$S(k, n) = \bigcup_{i=1}^{k} \{0\}^{i-1} \times (\mathbb{F}_q \backslash \{0\}) \times S(k, n-i). \tag{20}$$

□

We now give some lower bound for $M(k, n)$.

Claim 50. *We have*

$$M(k, n) \ge q^n - n \cdot q^{n-k}.$$

Proof. Follows from (19) and $M(k, n-k-1) \le q^{n-k-1}$ by induction. □

In particular,

Claim 51. *For $k = \lceil \log_q t \rceil + 1$ we have*

$$|\mathcal{S}| \ge \frac{q^{t-2}}{2t}.$$

Proof. We have

$$\begin{aligned} |\mathcal{S}| &= M(k, t-k) \ge q^{t-k} - (t-k)q^{t-2k} \\ &= q^{t-k}\left(1 - \frac{t-k}{q^k}\right) \ge \frac{q^t}{2q^k} \ge \frac{q^{t-2}}{2t}. \end{aligned}$$

□

Define any total order on $\mathbb{F}_q$ where accessing the ith element takes time $\log q$. Let $\alpha_1, \ldots, \alpha_{q-1}$ be the non-zero elements of $\mathbb{F}_q$ in that order. The following procedure defines a total order on $S(k, n)$ and therefore on $\mathcal{S}$ when $n = t - k$. We denote the procedure that returns the rth element in $S(k, n)$ by $\mathbf{Select}(n, r)$. We define the order recursively using (20). That is, we first compute $M(k, i)$ for all $i = 1, \ldots, n$ using (19). Find $j_1 \in \{1, 2, \ldots, k\}$ such that

$$(q-1) \cdot \sum_{i=1}^{j_1 - 1} M(k, n-i) < r \le (q-1) \cdot \sum_{i=1}^{j_1} M(k, n-i)$$

Then for

$$r' := r - (q-1) \cdot \sum_{i=1}^{j_1 - 1} M(k, n-i)$$

find $j_2 \in \{1, 2, \ldots, q-1\}$ such that

$$(j_2 - 1) \cdot M(k, n - j_1) < r' \le j_2 \cdot M(k, n - j_1).$$

Then for

$$r'' := r' - (j_2 - 1) \cdot M(k, n - j_1)$$

define the element

$$\{0\}^{j_1 - 1} \times \{\alpha_{j_2}\} \times \mathbf{Select}\left(n - j_1, r''\right).$$

Since $M(k, i) = q^{\Theta(i)}$, computing $M(k, i)$, $i = 1, \ldots, n$, takes time $\tilde{O}(n^2)$. Computing $(q-1)\sum_{i=1}^{j} M(k, n-i)$ at each stage to find j_1 takes time $\tilde{O}(kn) = \tilde{O}(n)$. To find j_2 at each stage we perform binary search for j_2. This takes time $\tilde{O}(n)$. Therefore, the total time complexity is $\tilde{O}(n^2) = \tilde{O}(t^2)$.

7.2 Appendix B

In this Appendix we prove

Proposition 52. *Consider*

$$\epsilon(m) = \left(1 - \frac{m}{q+1}\right)^{1/m},$$

and

$$\nu(m) = (q+1)^{1/m}.$$

Then

1. *For $m = 1$ we have*
$$\epsilon(m) = 1 - \frac{1}{q+1} \quad \textit{and} \quad \nu(m) = (q+1) = 2^{\log(q+1)}.$$
2. *For $m = (1/c)\log(q+1)$ where $c = o(\log(q+1))$ we have*
$$\epsilon(m) = 1 - \frac{1}{q+1} - \Theta\left(\frac{\log(q+1)}{c(q+1)^2}\right) \quad \textit{and} \quad \nu(m) = 2^c.$$
3. *For $m = o(q)$ and $m = \omega(\log(q+1))$ we have*
$$\epsilon(m) = 1 - \frac{1}{q+1} - \Theta\left(\frac{m}{(q+1)^2}\right)$$
and
$$\nu(m) = (q+1)^{\frac{1}{m}} = 1 + \frac{\ln(q+1)}{m} + \Theta\left(\frac{\log^2(q+1)}{m^2}\right).$$
4. *For $m = (q+1)/2$ we have*
$$\epsilon(m) = 1 - \frac{2\ln 2}{q+1} + \Theta\left(\frac{1}{(q+1)^2}\right)$$
and
$$\nu(m) = (q+1)^{\frac{2}{q+1}} = 1 + \frac{2\ln(q+1)}{q+1} + \Theta\left(\frac{\log^2(q+1)}{(q+1)^2}\right).$$
5. *For $m = c(q+1)$, c constant we have*
$$\epsilon(m) = 1 - \frac{\ln(1/(1-c))}{c(q+1)} + \Theta\left(\frac{1}{(q+1)^2}\right)$$
and
$$\nu(m) = (q+1)^{\frac{1}{c(q+1)}} = 1 + \frac{\ln(q+1)}{c(q+1)} + \Theta\left(\frac{\log^2(q+1)}{(q+1)^2}\right).$$

6. For $m = (q+1) - (q+1)/c$ where $c = \omega(1)$ we have

$$\epsilon(m) = 1 - \frac{\ln c}{q+1} + \Theta\left(\frac{\ln^2 c}{2(q+1)^2} - \frac{\ln c}{c(q+1)}\right) + \Theta\left(\frac{\ln^2 c}{c(q+1)^2}\right)$$

and

$$\nu(m) = (q+1)^{\frac{1}{(q+1)-(q+1)/c}} = 1 + \frac{\ln(q+1)}{(q+1)} + \Theta\left(\frac{\ln(q+1)}{c(q+1)} + \frac{\ln^2(q+1)}{(q+1)^2}\right).$$

7. For $m = (q+1) - c$, where $c = (q+1)^{o(1)}$, we have

$$\epsilon(m) = 1 - \frac{\ln(q+1)}{q+1} + \Theta\left(\frac{\log c}{q+1}\right)$$

and

$$\nu(m) = 1 + \frac{\ln(q+1)}{q+1} + \Theta\left(\frac{c\log(q+1)}{(q+1)^2} + \frac{\log^2(q+1)}{(q+1)^2}\right).$$

Proof. Sketch. For *2.* we use

$$(1+x)^\alpha = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n = 1 + \alpha x - \Theta(\alpha x^2) \quad \text{for } |x| < 1, \alpha < 1/2 \tag{21}$$

where

$$\binom{\alpha}{n} = \prod_{k=1}^{n} \frac{\alpha - k + 1}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-n+1)}{n!}.$$

For *3.* we use (21) and

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots = 1 + x + \Theta(x^2) \text{ for } |x| < 1. \tag{22}$$

For *4-7* we use (22) and

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = 1 + x + \Theta(x^2) \text{ for } |x| < 1.$$

□

The following table ignores the small terms

m	$\epsilon(m)$	$\nu(m)$
$m=1$	$1-\frac{1}{q+1}$	$q+1$
$m=\log(q+1)/c$, $c=o(\log(q+1))$	$1-\frac{1}{q+1}$	2^c
$m=o(q)$, $\omega(\log(q+1))$	$1-\frac{1}{q+1}$	$1+\frac{\ln(q+1)}{m}$
$m=c(q+1)$, $c<1$, $c=\Theta(1)$	$1-\frac{\ln(1/(1-c))}{c(q+1)}$	$1+\frac{\ln(q+1)}{c(q+1)}$
$m=(q+1)-(q+1)/c$, $c=\omega(1)$	$1-\frac{\ln c}{q+1}$	$1+\frac{\ln(q+1)}{q+1}$
$m=(q+1)-c$, $c=\Theta(1)$	$1-\frac{\ln(q+1)}{q+1}$	$1+\frac{\ln(q+1)}{q+1}$

7.3 Appendix C

In Theorem 38 we showed the following. Let $q<d+1$ and t be any integer. Let r be an integer such that $q^{2^{r-1}}<9d\le q^{2^r}$. Let $\boldsymbol{\epsilon}=(\epsilon_0,\ldots,\epsilon_{r-1},\epsilon_r)$ where $\epsilon_i(q^{2^i}+1)\le q^{2^i}$ is an integer for $i=0,1,\ldots,r-1$ and $2/3\ge\epsilon_r\ge 1/3$. Let

$$c_{q,\boldsymbol{\epsilon}}:=\sum_{i=0}^{r-1}c_{q,\boldsymbol{\epsilon},i}\quad\text{where}\quad c_{q,\boldsymbol{\epsilon},i}:=\frac{\log(q^{2^i}+1)}{\epsilon_i(q^{2^i}+1)}$$

and

$$\pi_{q,\boldsymbol{\epsilon}}:=\sum_{i=0}^{r-1}\pi_{q,\boldsymbol{\epsilon},i}\quad\text{where}\quad \pi_{q,\boldsymbol{\epsilon},i}:=\frac{-\log(1-\epsilon_i)}{\epsilon_i(q^{2^i}+1)}.$$

Then for

$$\overline{\epsilon^\star}:=\bar{\epsilon}_r\prod_{i=0}^{r-1}\bar{\epsilon}_i^{\lceil d/(\epsilon_i(q^{2^i}+1))\rceil}\ge\frac{2^{-\pi_{q,\boldsymbol{\epsilon}}\cdot d}}{\theta(d^2)},$$

we have

$$\nu_{\mathbb{F}_q}(d,\mathbb{F}_{q^t},\overline{\epsilon^\star})\le\theta(d^5)\cdot 2^{c_{q,\boldsymbol{\epsilon}}\cdot d}\cdot t.$$

Now our goal in this appendix is to fix $\pi_{q,\boldsymbol{\epsilon}}$ and minimize $c_{q,\boldsymbol{\epsilon}}$ or to fix $c_{q,\boldsymbol{\epsilon}}$ and minimize $\pi_{q,\boldsymbol{\epsilon}}$. Therefore we define

$$c_q(\pi)=\min_{\pi_{q,\boldsymbol{\epsilon}}=\pi}c_{q,\boldsymbol{\epsilon}}\ \text{ and }\ \pi_q(c)=\min_{c_{q,\boldsymbol{\epsilon}}=c}\pi_{q,\boldsymbol{\epsilon}}.$$

To find $c_q(\pi)$ we use the method of Lagrange multipliers. Consider

$$F_q(\boldsymbol{\epsilon},\lambda)=\pi_{q,\boldsymbol{\epsilon}}-\lambda(c_{q,\boldsymbol{\epsilon}}-c).$$

We have

$$\frac{\partial F_q}{\partial\epsilon_i}=0\Longrightarrow\lambda=-\frac{L(\epsilon_i)}{\ln(q^{2^i}+1)}\tag{23}$$

where

$$L(\epsilon) = \frac{\epsilon}{1-\epsilon} + \ln(1-\epsilon) = \sum_{j=2}^{\infty} \left(1 - \frac{1}{j}\right) \epsilon^j.$$

The function $L : [0,1] \to \mathbb{R}$ is monotonically increasing function, $L(0) = 0$ and $L(1) = +\infty$. Therefore the inverse function $L^{-1} : \mathbb{R}^+ \to [0,1]$ is well defined and monotonically increasing function. By (23) we have

$$\epsilon_i = L^{-1}\left(\alpha_i L(\epsilon_0)\right) \quad \text{where} \quad \alpha_i = \frac{\log(q^{2^i}+1)}{\log(q+1)}.$$

Since L and L^{-1} are monotonically increasing functions, we have

$$\epsilon_i = L^{-1}\left(\alpha_i L(\epsilon_0)\right) \geq L^{-1}\left(L(\epsilon_0)\right) = \epsilon_0.$$

For $\alpha > 1$ and $\epsilon\sqrt{\alpha} < 1$ we have

$$\begin{aligned} L^{-1}(\alpha L(\epsilon)) &= L^{-1}\left(\alpha \sum_{j=2}^{\infty}\left(1-\frac{1}{j}\right)\epsilon^i\right) \\ &\leq L^{-1}\left(\sum_{j=2}^{\infty}\left(1-\frac{1}{j}\right)(\sqrt{\alpha}\epsilon)^i\right) \\ &= L^{-1}(L(\sqrt{\alpha}\epsilon)) = \sqrt{\alpha}\epsilon \end{aligned}$$

and for $\epsilon\sqrt{\alpha} \geq 1$ we have

$$L^{-1}(\alpha L(\epsilon)) \leq 1 \leq \sqrt{\alpha}\epsilon.$$

Therefore for any ϵ_0 we have

$$1 \geq \frac{\epsilon_0}{\epsilon_i} \geq \frac{1}{\sqrt{\alpha_i}}. \tag{24}$$

Then, by (24),

$$c_{q,\boldsymbol{\epsilon},i} = \frac{\log(q^{2^i}+1)}{\epsilon_i(q^{2^i}+1)} = c_{q,\boldsymbol{\epsilon},0} \cdot \alpha_i \frac{\epsilon_0}{\epsilon_i}\frac{q+1}{q^{2^i}+1} \geq c_{q,\boldsymbol{\epsilon},0} \cdot \sqrt{\alpha_i}\frac{q+1}{q^{2^i}+1}$$

and

$$c_{q,\boldsymbol{\epsilon},i} = \frac{\log(q^{2^i}+1)}{\epsilon_i(q^{2^i}+1)} = c_{q,\boldsymbol{\epsilon},0} \cdot \alpha_i \frac{\epsilon_0}{\epsilon_i}\frac{q+1}{q^{2^i}+1} \leq c_{q,\boldsymbol{\epsilon},0} \cdot \alpha_i\frac{q+1}{q^{2^i}+1}.$$

Therefore,

$$c_{q,\epsilon} = c_{q,\boldsymbol{\epsilon},0}\left(1 + \frac{1}{\Theta(q)}\right). \tag{25}$$

We now give another bound that will be used in the sequel. Let $t \geq 1$ be a real number such that $\epsilon_0 = 1 - 1/t$. Since $L(1-1/t) = t - \ln t - 1$, for any t and $\alpha > 1$ we have

$$L^{-1}\left(\alpha L\left(1-\frac{1}{t}\right)\right) = L^{-1}(\alpha t - \alpha \ln t - \alpha) \leq L^{-1}(\alpha t - \ln(\alpha t) - 1) \leq 1 - \frac{1}{\alpha t}.$$

Therefore

$$1 - \frac{1}{t} = \epsilon_0 \leq \epsilon_i \leq 1 - \frac{1}{\alpha_i t}. \tag{26}$$

To bound $\pi_{q,\boldsymbol{\epsilon},i}$ we first consider the function

$$\sigma(\epsilon) = \frac{\epsilon}{-\ln(1-\epsilon)}$$

for $0 \leq \epsilon \leq 1$. This function is monotonically decreasing and for $0 \leq \epsilon \leq 0.5$, $1 \geq \sigma(\epsilon) > .5$.

Now by (24) and the properties of σ we have

$$\pi_{q,\boldsymbol{\epsilon},i} = \frac{-\log(1-\epsilon_i)}{\epsilon_i(q^{2^i}+1)} = \pi_{q,\boldsymbol{\epsilon},0}\frac{\sigma(\epsilon_0)}{\sigma(\epsilon_i)}\frac{q+1}{q^{2^i}+1} \geq \pi_{q,\boldsymbol{\epsilon},0}\frac{q+1}{q^{2^i}+1}.$$

For the upper bound, let $\epsilon_0 = 1 - 1/t$. We have two cases: The first case is when

$$t \geq 1 + \frac{1}{2\sqrt{\alpha_i} - 1}.$$

Then, by (26),

$$\frac{\sigma(\epsilon_0)}{\sigma(\epsilon_i)} \leq \frac{-\ln(1-\epsilon_i)}{-\ln(1-\epsilon_0)} \leq \frac{\ln(\alpha_i t)}{\ln t} \leq \frac{\ln \alpha_i}{\ln(1 + 1/(2\sqrt{\alpha_i}-1))} + 1 \leq 4\sqrt{\alpha_i}\ln \alpha_i.$$

and therefore

$$\pi_{q,\boldsymbol{\epsilon},i} = \pi_{q,\boldsymbol{\epsilon},0}\frac{\sigma(\epsilon_0)}{\sigma(\epsilon_i)}\frac{q+1}{q^{2^i}+1} \leq \pi_{q,\boldsymbol{\epsilon},0} \cdot (4\sqrt{\alpha_i}\ln \alpha_i)\frac{q+1}{q^{2^i}+1}.$$

The second case is when

$$t < 1 + \frac{1}{2\sqrt{\alpha_i} - 1}.$$

Then $\epsilon_0 < 1/(2\sqrt{\alpha_i}) < 1/2$ and by (24), $\epsilon_i \leq \sqrt{\alpha_i}\epsilon_0 \leq 1/2$. Then by the properties of σ we get

$$\pi_{q,\boldsymbol{\epsilon},i} = \pi_{q,\boldsymbol{\epsilon},0}\frac{\sigma(\epsilon_0)}{\sigma(\epsilon_i)}\frac{q+1}{q^{2^i}+1} \leq \pi_{q,\boldsymbol{\epsilon},0} \cdot 2\frac{q+1}{q^{2^i}+1}.$$

Therefore

$$\pi_{q,\epsilon} = \pi_{q,\boldsymbol{\epsilon},0}\left(1+\frac{1}{\Theta(q)}\right). \tag{27}$$

Now by (25) and (27) we get

$$c_{q,\boldsymbol{\epsilon}} = \frac{\log(q+1)}{\epsilon_0(q+1)}\left(1+\frac{1}{\Theta(q)}\right)$$

and

$$\pi_{q,\boldsymbol{\epsilon}} = \frac{-\log(1-\epsilon_0)}{\epsilon_0(q+1)}\left(1+\frac{1}{\Theta(q)}\right).$$

This shows that the optimal solution (for large q) is determined by the first term of $c_{q,\boldsymbol{\epsilon}}$ and $\pi_{q,\boldsymbol{\epsilon}}$. Therefore (ignoring small terms) we get

$$\epsilon_0 = \frac{\log(q+1)}{c(q+1)}$$

and

$$\pi_q(c) = \min_{c_{q,\boldsymbol{\epsilon}}=c} \pi_{q,\boldsymbol{\epsilon}} = \frac{-c\log\left(1-\frac{\log(q+1)}{c(q+1)}\right)}{\log(q+1)} = \begin{cases} \frac{c'\log(1-1/c')}{q+1} & c = c'\frac{\log(q+1)}{q+1} \\ \frac{\log e}{q+1} & c = \omega\left(\frac{\log(q+1)}{q+1}\right) \end{cases}.$$

To get a better bounds for small q one can use the following estimates

$$\begin{aligned} L^{-1}\left(\alpha L\left(1-\frac{1}{t}\right)\right) &= L^{-1}(\alpha t - \alpha\ln t - \alpha) \\ &\geq L^{-1}((\alpha t - \alpha\ln t - \alpha + 1) - \ln(\alpha t - \alpha\ln t - \alpha + 1) - 1) \\ &= 1 - \frac{1}{\alpha t - \alpha\ln t - \alpha + 1}. \end{aligned}$$

Therefore

$$\epsilon_i \geq 1 - \frac{1}{\alpha_i t - \alpha_i\ln t - \alpha_i + 1}.$$

References

[1] L. M. Adleman and H. W. Lenstra, Jr. Finding Irreducible Polynomial over Finite Field. In 18th Annual ACM Symposium on Theory of Computing, pp. 350–355, (1986).

[2] S. Ballet. Curves with many points and multiplication complexity in any extension of F_q. Finite Fields and Their Applications, 5(4) , pp. 364–377. (1999).

[3] N. H. Bshouty. Testers and their Applications. Electronic Colloquium on Computational Complexity (ECCC) 19: 11 (2012). and ITCS 2014. pp. 327–352. (2014).

[4] N. H. Bshouty. Multilinear Complexity is Equivalent to Optimal Tester Size. Electronic Colloquium on Computational Complexity (ECCC) 20: 11. (2013)

[5] S. A. Evdokimov. Factoring a Solvable Polynomial over Finite Fields and Generalized Riemann Hypothesis. *Zapiski Nauchn Semin. Leningr. Otdel Matem. Inst. Acad. Sci.*, USSR 176, pp. 104–117, (1989).

[6] A. Garcia and H. Stichtenoth. On the Asymptotic Behaviour of Some Towers of Function Fields over Finite Fields. *Journal of Number Theory*, **61**, pp. 248–273 (1996).

[7] A. Garcia and H. Stichtenoth. Topics in Geometry, Coding Theory and Cryptography. Algebra and applications. Springer. (2007).

[8] V. Guruswami, C. Xing. Hitting Sets for Low-Degree Polynomials with Optimal Density. IEEE Conference on Computational Complexity 2014. pp. 161–168. (2014).

[9] H. W. Lenstra. Finding isomorphisms between finite fields. *Mathematics of Computation*, 56, 193, pp. 329–347. (1991).

[10] R. Lidl and H. Niederreiter. Finite Fields. Encyclopedia of Mathematics and its Applications. Addison-Wesley Publishing Company. (1984).

[11] A. Poli. A deterministic construction of normal bases with complexity $O(n^3+n\log n\log\log n\log q)$. *J. Symb. Comp.*, **19**, pp. 305–319. (1995).

[12] R. M. Roth. Introduction to Coding Theory. Cambridge University Press, Cambridge, UK, (2006).

[13] V. Shoup. New Algorithms for Finding Irreducible Polynomial over Finite Field. *Mathematics of Computation*, V. 54, N. 189, pp. 435-447, (1990).

[14] I. Shparlinski. Finite fields: theory and computation. Mathematics and Its Applications, Vol. 477. (1999).

[15] K. W. Shum. A low-complexity algorithm for the construction of algebraic-geometric codes better than the Gilbert-Varshamov bound. A Dissertation. University of Southern California.

[16] H. Stichtenoth. Algebraic Function Fields and Codes. Second Edition. Springer. 2008.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de