Optimal Bounds for Testing Sparse Polynomials over $\mathbb{F}_3$

Kai Werther*

August 9, 1994

Abstract

We show that the size of a minimal zero test set for t-sparse n-variate polynomials over $\mathbb{F}_3$ is of order $(2n)^{\lfloor \log t \rfloor}(1 + \Theta(1/n))$, thereby significantly improving the best previously known lower bound ([5]).

1 Introduction

The classical problem of interpolation reaches far back into the history of mathematics. Among the first to consider this problem were Newton and Lagrange who gave interpolation formulas for polynomials in one variable.

For multivariate polynomials the number of terms of a degree bounded polynomial increases exponentially with the number of variables. Recently, the design of so called *sparse interpolation algorithms* [1, 2, 3, 5, 6, 7] has attracted a lot of attention, which in contrast to classical interpolation methods, take as an additional parameter an upper bound on the number of terms of the polynomial. This number of terms, say t, is often denoted as the *sparsity* of f and f is said to be t-sparse. If the sparsity is small compared to $(d+1)^n$, the complexity of the interpolation problem may decrease significantly.

In the following we adopt the black box model, i.e., the polynomial f to be reconstructed is hidden in a "black box" that given an input x computes in one step the output $f(x)$. The zero test problem, i.e., the problem of deciding whether a polynomial given by a black box is the zero polynomial, is related to the interpolation problem. A set of query points that establishes such a test is called a *test set*. For a more detailed introduction we refer to [1, 2, 3, 5, 6, 7].

In this paper we study the minimal size of test sets for t-sparse n-variate polynomials over the field $\mathbb{F}_3$.

The main results of this paper is an almost optimal improvement of the previously known lower bounds [1, 5] (Section 3), implying, that the test set constructed in [1] is asymptotically optimal.

2 Preliminaries

Let us first introduce some notation. For an integer s let $[s]$ denote the set of integers $\{1, \ldots, s\}$. We use the notation $\mathbf{0}$ and $\mathbf{1}$ for the all-zero and all-one vector, respectivly.

Definition 2.1 Let K be a field and $0 \not\equiv f \in K[x_1, \ldots, x_n]$. A point $a \in K^n$ is called a *witness* for f if $f(a) \neq 0$. A set $A \subseteq K^n$ is called a *test-set* for a family $\mathcal{F} \subseteq K[x_1, \ldots, x_n]$ if there is a witness $a \in A$ for each $0 \not\equiv f \in \mathcal{F}$. A set $A^* \in (K^*)^n$ is called a *$*$-test-set* for a family $\mathcal{F} \subseteq K[x_1, \ldots, x_n]$ if there is a witness $a \in A^*$ for all polynomials $f \in \mathcal{F}$ not vanishing on $(K^*)^n$.

*Institut für Informatik V, Römerstr. 164, Universität Bonn, 53117 Bonn, Germany

Given a family $\mathcal{F}$ of polynomials let $\mathcal{F}^* \subseteq \mathcal{F}$ denote the set of polynomials f from $\mathcal{F}$ not vanishing on $(K^*)^n$.

Let $C(\mathcal{F})$ denote a test-set of minimum size (or minimal test-set) and $c(\mathcal{F})$ denote the size of $C(\mathcal{F})$. Similarly, let $C^*(\mathcal{F})$ denote a $*$-test-set of minimum size and $c^*(\mathcal{F})$ denote the size of $C^*(\mathcal{F})$.

In the following we consider the family of t-sparse n-variate polynomials over $\mathbb{F}_q$, denoted by $\mathcal{F}_q(n,t)$ and let $c_q(n,t) = c(\mathcal{F}_q(n,t))$ and $c_q^*(n,t) = c^*(\mathcal{F}_q(n,t))$. Let $\mathcal{A}_q(n,t)$ denote the set of all test-sets for $\mathcal{F}_q(n,t)$ and $\mathcal{A}_q^*(n,t)$ denote the set of all $*$-test-sets.

The following lemma reveals the structure of test-sets.

Lemma 2.2 *Let $A \in \mathcal{A}_q(n,t)$ be a test-set. Then for all $T \subseteq [n]$ of size at most $\lfloor \log t \rfloor$ there are $*$-test-sets $A_T \in \mathcal{A}_q^*(n-|T|, t/2^{|T|})$ such that*

$$A = \bigcup_{T, |T| \leq \lfloor \log t \rfloor} \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \mid a_i = 0 \Leftrightarrow i \in T, (a_i)_{i \notin T} \in A_T\}$$

Proof. It is not hard to see that a polynomial f evaluates to zero for all $a \in (\mathbb{F}_q^*)^n$ if and only if for some $\emptyset \neq I \subseteq [n]$, f is divisible by $(\prod_{i \in I} x_i^{q-1} - 1)$. Thus $0 \not\equiv f \in \mathcal{F}_q(n,t)$ is either contained in $\mathcal{F}_q^*(n,t)$ or for some $\emptyset \neq I \subseteq [n]$,

$$f = (\prod_{i \in I} x_i^{q-1} - 1) g(x_1, \ldots, x_n).$$

Since $f \not\equiv 0$, we have $g' := g|_{x_i = 0} \not\equiv 0$ for some x_i, $i \in I$. Therefore $g' \in \mathcal{F}_q(n-1, t/2)$. Thus a test-set $A \in \mathcal{A}_q(n,t)$ can be written as

$$A = A^* \cup \bigcup_{i=1}^{n} \{(a_1, \ldots, a_n) \mid a_i = 0, (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n) \in A_i\}$$

where $A^* \in \mathcal{A}_q^*(n,t)$ and $A_i \in \mathcal{A}_q(n-1, t/2)$. Now the assertion is clear by an induction on t. □

In particular, a minimal test-set is constructed by minimal $*$-test-sets.

Corollary 2.3

$$c_q(n,t) = \sum_{i=0}^{\lfloor \log t \rfloor} c_q^*(n-i, t/2^i) \binom{n}{i}. \tag{1}$$

Corollary 2.3 allows us to concentrate on determining the value $c_q^*(n,t)$.

The multiplicative group $(\mathbb{F}_q^*, \cdot)$ of a finite field is a cyclic group of order $q-1$ and therefore isomorphic to the additive group $(\mathbb{Z}_{q-1}, +)$: fixing a primitive element (or generator) ω of $\mathbb{F}_q^*$ the index of $a \in \mathbb{F}_q^*$ with respect to ω is defined to be the smallest integer $\hat{a} \geq 0$ such that $a = \omega^{\hat{a}}$. This isomorphism transforms multiplication into addition and powering into multiplication, i.e., the index of a^n equals n times the index of a. Thus monomials $c x_1^{\beta_1} \cdots x_n^{\beta_n}$ over $\mathbb{F}_q$ transform to linear forms $\beta_0 + \beta_1 y_1 + \ldots + \beta_n y_n$ over $\mathbb{Z}_{q-1}$ where β_0 is the index of c. Applying this transformation to all monomials of a t-sparse polynomial

$$f = \sum_{i=1}^{t} c_i x_1^{\beta_{i,1}} \cdots x_n^{\beta_{i,n}}, \tag{2}$$

with pairwise distinct monomials, coefficients $0 \neq c_i = \omega^{\beta_{i,0}}$ and $\beta_{i,j}$ satisfying $0 \leq \beta_{i,j} \leq q-2$, transforms f into a set of t linear forms. These can be arranged in a $t \times (n+1)$ matrix over $\mathbb{Z}_{q-1}$:

$$\hat{f} = \begin{pmatrix} \beta_{1,0} \ldots \beta_{1,n} \\ \vdots \ddots \vdots \\ \beta_{t,0} \ldots \beta_{t,n} \end{pmatrix}. \tag{3}$$

In the sequel we let $q = 3$. In particular, $\mathbb{Z}_{q-1} = \mathbb{F}_2$ is a field and the generator $\omega = 2$ is unique. For notational reasons we identify a subset S of $[n]$ with its characteristic vector $\chi(S) \in \mathbb{F}_2^n$ and the expression $M \cdot S$, where M is a matrix with n columns over $\mathbb{F}_2$ and S is a subset of $[n]$ becomes a well defined expression.

The test-set

$$A(n,t) := \{(a_1,\ldots,a_n) \in (\mathbb{F}_3^*)^n \mid \#\{i \mid a_i = 2\} \le \lfloor \log t \rfloor\} \tag{4}$$

constructed in [1] yields the upper bound

$$c_3^*(n,t) \le \sum_{i=0}^{\lfloor \log t \rfloor} \binom{n}{i} \tag{5}$$

In the next section we derive the following (almost optimal) lower bound. The best previously known lower bounds ([5]) are only linear in n:

$$c_3^*(n,t) \ge \binom{n}{\lfloor \log t \rfloor} - \sum_{i=1}^{\lfloor \log t \rfloor - 1} \binom{n}{i} \tag{6}$$

3 The lower bound

The following lemma correlates the values of $f(a)$ and of $\hat{f}(\hat{a}) = \hat{f} \cdot (1, \hat{a}_1, \ldots, \hat{a}_n)$, where $\hat{a}_i$ is the index of a_i. In the following $\hat{a}$ denotes the index of a, and for a set of query points $A = \{(a_1,\ldots,a_n),\ldots,\} \subset (\mathbb{F}_3^*)^n$, the set $\{(\hat{a}_1,\ldots,\hat{a}_n),\ldots\} \subset \mathbb{F}_2^n$ is denoted by $\hat{A}$.

Lemma 3.1 *Let $f \in \mathbb{F}_3[x_1,\ldots,x_n]$ as given in (2) consist of exactly t terms, $\hat{f}$ as definied by (3), $a \in (\mathbb{F}_3^*)^n$, and $\hat{a} \in \mathbb{F}_2^n$. Then*

$$f(a) = (t - 2\#(\hat{f}(\hat{a})) \bmod 3.$$

Proof. $\#(\hat{f}(\hat{a}))$ is the number t_2 of terms in f that evaluate to 2 at the point a and $t_1 = t - t_2$ is the number of terms that evaluate to 1. Since the sum of 3 terms with the same value is zero and the sum of two terms with differnent value is also zero, the value of f depends only on $(t_1 - t_2) \bmod 3$. Now the assertion follows from a quick inspection for the possible values of $t_1 \bmod 3$ and $t_2 \bmod 3$. □

Let $V_{t,c} := \{\gamma \in \mathbb{F}_2^t \mid t - 2\#(\gamma) \equiv c \pmod 3\}$. Then $\hat{f}(\hat{a}) \in V_{t,c}$ is equivalent with $f(a) = c$. We are mostly interested in $V_t := V_{t,0}$.

The first nontrivial case is $t = 2$. Although the following result is known (c.f. [5, Lemma 6]) we will reprove it.

Lemma 3.2

$$c_3^*(n,2) \ge n + 1.$$

Proof. Let f be a 2-sparse polynomial, $A = \{a^{(1)},\ldots,a^{(n)}\} \subset (\mathbb{F}_3^*)^n$ be any set of size n, and $\hat{A} = \{\hat{a}^{(1)},\ldots,\hat{a}^{(n)}\} \subset \mathbb{F}_2^n$. By Lemma 3.1, $f(a) = 0$ if and only if $\hat{f}(\hat{a}) \in \{(0,1)^T,(1,0)^T\}$. Let $\mathbf{0} \ne C = \hat{f}_1 + \hat{f}_2$ the sum of the rows of the matrix $\hat{f}$ and $c = \hat{f}_1 + \hat{f}_2$. Now $f(a) = 0$ iff $C\hat{a} + c = 1$. Thus A fails to be a $*$-test-set since if the matrix

$$M := \begin{pmatrix} \hat{a}_1^{(1)} & \ldots & \hat{a}_n^{(1)} \\ \ldots & \ddots & \vdots \\ \hat{a}_1^{(n)} & \ldots & \hat{a}_n^{n)} \end{pmatrix}$$

is singular then there exists $\mathbf{0} \ne C$ with $M \cdot C = \mathbf{0}$ and if M is regular then there exists $\mathbf{0} \ne C$ with $M \cdot C = \mathbf{1}$. Choosing $c = 1$ in the first case and $c = 0$ in the second case makes $C\hat{a}^{(i)} + c = 1$ for all i. Hence any $*$-test-set must have size at least $n + 1$. □

Observe, that as a consequence of the proof, for any $*$-test-set $A \subset (\mathbb{F}_3^*)^n$ for 2-sparse polynomials, the set $\hat{A} = \{\hat{a}^{(1)}, \ldots, \hat{a}^{(|A|)}\} \subset \mathbb{F}_2^n$ must contain a basis for $\mathbb{F}_2^n$. Clearly, if $t > 2$, the same holds for $*$-test-sets for t-sparse polynmials.

The idea behind the improved lower bound for $t > 2$ is as follows. Let f be a t-sparse polynomial and $\hat{f}$ be the affine map specified by (3). The image W of $\hat{f}$ is an affine subspace of $\mathbb{F}_2^t$. If we choose $\hat{f}$ in such away that W is almost entirely contained in V_t, then $\hat{f}$ maps many vectors into V_t, i.e., $f(a)$ is zero for many $a \in (\mathbb{F}_3^*)^n$.

More precisely, let $t = 2^k$ be a power of two, $C := \{c^{(0)}, c^{(1)}, \ldots, c^{(k)}\} \subset \mathbb{F}_2^{2^k}$, and $B = \{\hat{a}^{(1)}, \ldots, \hat{a}^{(n)}\}$ be a basis of $\mathbb{F}_2^n$. For each $\pi : [n] \to \{0, 1 \ldots, k\}$ there is an affine linear map $\hat{g}$ mapping $\hat{a}^{(i)}$ to $c^{(\pi(i))}$ and $\mathbf{0}$ to $c^{(0)}$. The image of $\hat{g}$ is the affine linear space $W = \langle c^{(1)} - c^{(0)}, \ldots, c^{(k)} - c^{(0)} \rangle + c^{(0)}$ defined by C. For each set $I \subseteq [n]$ let $J(I) := \{j \mid |I \cap \pi^{-1}(j)| \text{ is odd}\}$. Now for any $I \subseteq [n]$,

$$\begin{aligned} \hat{g}(\sum_{i \in I} \hat{a}^{(i)}) &= \sum_{i \in I} c^{(\pi(i))}) + (|I| - 1)c^{(0)} \\ &= \sum_{j \in J(I)} c^{(j)} + (|J(I)| - 1)c^{(0)}, \end{aligned} \tag{7}$$

since $|I| \equiv |J(I)| \pmod 2$ and computation is performed in $\mathbb{F}_2$. We will construct C such that (7) lies in V_t for all J except for $J = \{1, \ldots, k\}$. This in turn means that the vectors $c^{(1)}, \ldots, c^{(k)}$ are pairwise distinct, hence the constructed $\hat{g}$ corresponds to a nonzero 2^k-sparse polynomnial g.

Lemma 3.3 *Let $k \geq 1$. The vectors $c^{(0,k)}, \ldots, c^{(k-1,k)} \in \mathbb{F}_2^{2^k}$ defined by*

$$c_j^{(i,k)} = 1 \iff (j-1) \bmod 2^{i+1} \in \{0, \ldots, 2^i - 1\}, \quad 0 \leq i \leq k-1, 1 \leq j \leq 2^k$$

have the following property:

$$\forall\, \emptyset \neq I \subseteq \{0, \ldots, k-1\} : \quad \#(\sum_{i \in I} c^{(i,k)}) = 2^{k-1}$$

Proof. We prove the assertion by induction on k. For $k = 1$ the assertion is clear, so assume $k > 1$. As can be seen from the definition, $c^{(i,k)}$, $i < k-1$, consists of a concatenation of two copies of $c^{(i,k-1)}$. By the induction hypothesis the weight of $\sum_{i \in I} c^{(i,k-1)}$ is 2^{k-2} for all $\emptyset \neq I \subseteq \{0, \ldots, k-2\}$. Therefore the assertion follows for all $I \not\ni k-1$. Now $c^{(k-1,k)} = (\underbrace{1, \ldots, 1}_{2^{k-1}} \underbrace{0, \ldots, 0}_{2^{k-1}})$ and therefore adding $c^{(k-1,k)}$ to $\sum_{i \in I} c^{(i,k)}$ does not change the weight, since $2^{k-1} - 2^{k-2} = 2^{k-2}$. The assertion follows. □

Lemma 3.4 *Let $k \geq 1$ and let $c^{(0,k)}, \ldots, c^{(k-1,k)}$ be specified as in Lemma 3.3 and let $c^{(k,k)} = \mathbf{1} + \sum_{i=r}^{k-1} c^{(i,k)}$ where $r = k \bmod 2$. Then*

$$\#(\sum_{j \in J} c^{(j,k)} + (|J| - 1)c^{(0,k)}) = \begin{cases} 2^k & \text{if } J = [k] \\ 2^{k-1} & \text{otherwise} \end{cases}.$$

Proof. For $k \notin J$ the assertion of the lemma follows directly from Lemma 3.3. For $k \in J$,

$$\sum_{j \in J} c^{(j,k)} + (|J| - 1)c^{(0,k)} = \mathbf{1} + \sum_{j \notin J} c^{(j,k)} + (|J| - r)c^{(0,k)}.$$

Since the complement of a vector of weight 2^{k-1} is also of weight 2^{k-1} the assertion follows in the case $J \neq [k]$. The assertion for $J = [k]$ is also obvious. □

The vectors of weight 2^{k-1} lie in V_{2^k}, but the vector of weight 2^k does not. Therefore $C = \{c^{(0,k)}, \ldots, c^{(k,k)}\}$ has the desired property.

Now we can give a necessary property of $*$-test-sets.

Lemma 3.5 *Let $A \subset (\mathbb{F}_3^*)^n$ be a $*$-test-set for 2^k-sparse polynomials. Then for all bases $B = \{\hat{a}^{(1)}, \ldots, \hat{a}^{(n)}\}$ of $\hat{A}$ and all mappings $\pi : [n] \to \{0, \ldots, k\}$, $\hat{A}$ contains a linear combination $\sum_{i \in I} \hat{a}^{(i)}$, such that for all $1 \leq l \leq k$, $|I \cap \pi^{-1}(l)|$ is either zero or odd.*

Proof. For purpose of contradiction suppose that for some mapping π and all $\sum_{i \in I} \hat{a}^{(i)} \in \hat{A}$ there exists l such that $|I \cap \pi^{-1}(l)|$ is nonzero and even. Let k' be the number of indices $1 \leq l \leq k$ such that $\pi^{-1}(l)$ is nonempty and assume w.l.o.g. that these indices are $1, \ldots, k'$ and let $\hat{g} = \hat{g}_\pi$ be the affine linear map mapping $\hat{a}^{(i)}$ to $c^{(\pi(i),k')}$ and $\mathbf{0}$ to $c^{(0,k')}$. If $|I \cap \pi^{-1}(l)|$ is even for some $1 \leq l \leq k'$, the set $J(I)$ is a proper subset of $[k']$. By (7) and Lemma 3.4, for all $I \subseteq [n]$ the image of $\sum_{i \in I} \hat{a}^{(i)}$ under $\hat{g}$ has weight $2^{k'-1}$ and is therefore included in $V_{2^{k'}}$. We reached a contradiction since $\hat{g}$ does not correspond to the zero polynomial. The assertion follows. □

The advantage of this new formulation becomes clear if we use the language of multilinear algebra. Let us begin with some facts.

Let W be an n-dimensional vector space over some field K. A mapping $h : W^k \to K$ that is linear in every coordinate is called a *k-linear map*. If additionally $h(x) = (-1)^\sigma h(\sigma(x))$ for any permutation $\sigma \in S_n$, h is called *alternating*. Given a basis $B = \{e_1, \ldots, e_n\}$ of W, an alternating k-linear map h is uniquely determined by the image of the (ordered) k-sets of B. Therefore the dimension of the vector space $AL_{n,k}$ of alternating k-linear maps is $\binom{n}{k}$. This readily defines an equivalence relation on W^k, namely, by the orbits of $AL_{n,k}$:

$$(x_1, \ldots, x_k) \cong (y_1, \ldots, y_k) \iff \forall\, h \in AL_{n,k} : \quad h(x_1, \ldots, x_k) = h(y_1, \ldots, y_k). \tag{8}$$

Another important property is that the value of an alternating k-linear map does not change when an argument is altered by adding some multiple of another argument to it, e.g., for any $\beta \in K$, $h(x_1, x_2) = h(x_1 + \beta x_2, x_2)$. This directly gives us a method to check whether two elements of W^k are equivalent in the sense of (8).

The most famous example of an alternating multilinear form ist the determinant where the above property is extensively used in the Gaussian elimation method for computing the value of the determinant of a given matrix. Here our equivalence relation is the notion of similarity of two matrices.

Let $\tilde{\det} : W^k \to K$ denote the alternating k-linear form, that maps a k-tuple of linear independent vectors to 1 and a k-tuple of linear dependent vectors to 0.

For each $\hat{a} \in \mathbb{F}_2^n$ and all $k \leq n$ we will define the alternating k-linear form $h_{\hat{a}}$ over $(F_2^n)^k$ as follows:

$$h_{\hat{a}}(x_1, \ldots, x_k) := \langle \hat{a}, x_1 \rangle_B \langle \hat{a}, x_2 \rangle_B \cdots \langle \hat{a}, x_k \rangle_B \cdot \tilde{\det}(x_1, \ldots, x_k),$$

where the inner product $\langle ., . \rangle_B$ is with respect to the basis B.

Now Lemma 3.5 has the nice formulation we sought for:

$$\begin{gathered} A \text{ is a } * \text{-test-set for } 2^k \text{-sparse polynomials} \iff \\ \forall\, \pi : [n] \to \{0, 1, \ldots, k\},\ \exists \hat{a} \in \hat{A} : \quad h_{\hat{a}}(\textstyle\sum_{j \in \pi^{-1}(i_1)} \hat{a}^{(j)}, \ldots, \sum_{j \in \pi^{-1}(i_l)} \hat{a}^{(j)}) = 1, \end{gathered} \tag{9}$$

where $1 \leq i_1, \ldots, i_l \leq n$ are the indices with nonempty preimage. Observe that the sets $\pi^{-1}(i_j)$ are pairwise disjoint. Note that (9) also holds if we restrict π to be surjective on $[k]$.

The following lemma gives a characterization of $(\mathbb{F}_2^n)^k$ with respect to alternating k-linear forms.

Lemma 3.6 *Let $\xi_1, \ldots, \xi_k \in \mathbb{F}_2^n$ be linear independent and let $X = (\xi_1, \ldots, \xi_k)^T \in \mathbb{F}_2^{n \times k}$. Then the following holds*
a) $(\xi_1, \ldots, \xi_k) \cong (\beta_1, \ldots, \beta_k)$ where the β seen as subsets of $[n]$ are pairwise disjoint, or
b) there is a regular submatrix $Y \in \mathbb{F}_2^{k \times k}$ of X such that $Y \mathbf{1}_k \neq \mathbf{1}_k$. In particular, for some $b \notin \{\mathbf{0}_k, \mathbf{1}_k\}$ we have $Y \cdot b = \mathbf{1}_k$

Proof. Since $\xi_1, \ldots, \xi_k$ are linear independent there is regular submatrix $Y \in \mathbb{F}_2^{k \times k}$ of X. Suppose $Y \mathbf{1}_k = \mathbf{1}_k$. If the columns of X not contained in Y are all zero or each of these columns is identical to one

of Y, then using the Gaussian elimination we can transform X to some matrix Z, such that the submatrix Y transforms to the unity matrix. Thus the columns of Z are the unity vectors. It follows that the rows of Z seen as sets are pairwise disjoint. In the other case there is a column, neither zero nor identical to one column of Y. This column together with any $k-1$ columns of Y gives a regular matrix Y' with $Y' \cdot \mathbf{1}_k \neq \mathbf{1}_k$. As Y' is regular for some $b \notin \{\mathbf{0}_k, \mathbf{1}_k\}$ we have $Y' \cdot b = \mathbf{1}_k$. The assertion follows. □

Now we can prove the main theorem.

Theorem 3.7

$$c_3^*(n, 2^k) \geq \binom{n}{k} - \sum_{i=1}^{k-1} \binom{n}{i}$$

Proof. Let $\hat{A} \subset \mathbb{F}_2^n$ and $B = \{\hat{a}^{(1)}, \ldots, \hat{a}^{(n)}\} \subset \hat{A}$ be a basis for $\mathbb{F}_2^n$. We represent all elements of $\mathbb{F}_2^n$ as coordinate vectors over this basis. Consider the set $\{h_{\hat{a}} \in AL_{n,k} \mid \hat{a} \in \hat{A}\}$. If this set does not span $AL_{n,k}$ then there are linear independent vectors $\xi_1, \ldots, \xi_k \in \mathbb{F}_2^n$ such that for all $\hat{a} \in \hat{A}$, $h_{\hat{a}}(\xi_1, \ldots, \xi_k) = 0$. In order to separate any k-tupel of vectors from zero, $\hat{A}$ has to contain at least $\dim(AL_{n,k}) = \binom{n}{k}$ elements. We must exclude some k-tupels of vectors, namely those, which are inequivalent in the sense of (8) with any k-tupel $\xi_1, \ldots, \xi_k$ of vectors with pairwise disjoint ξ_i (seen as subsets of $[n]$), since such vectors can not be induced by the mapping π in (9). By Lemma 3.6, these vectors can be separated by $\sum_{i=1}^{k-1} \binom{n}{i}$ elements $\hat{a} \in \mathbb{F}_2^n$, namely, those with less than k ones in their representation with respect to B. The assertion follows. □

The lower bound on $c_3^*(n,t)$, Corollary 2.3 together with the upper bound (5) imply:

Corollary 3.8 *For all t,*

$$c_3(n,t) = \frac{2^{\lfloor \log t \rfloor}}{(\lfloor \log t \rfloor)!} n^{\lfloor \log t \rfloor} \left(1 + \Theta(\frac{1}{n})\right)$$

For small values of k we can give a better lower bound.

Lemma 3.9

$$c_3^*(n, 2^k) \geq kn + 1.$$

Proof. Let $A \subset (\mathbb{F}_3^*)^n$ be a set of size kn. By Lemma 3.2, for each set $C \subset (\mathbb{F}_3^*)^n$ of size n there is a polynomial $f_C \in \mathcal{F}^*(n,2)$ vanishing on C. Thus f_{C_1} vanishes on $C_1 = \{a_1, \ldots, a_n\}$, f_{C_2} vanishes on $C_2 = \{a_{n+1}, \ldots, a_{2n}\}$ and so on. Therefore, $f = \prod_{i=1}^{k} f_{C_i}$ is a 2^k-sparse polynomial that vanishes on A. The assertion follows. □

To conclude this section, let us remark that the lower bound obtained for $\mathbb{F}_3$ is valid for all fields of odd characteristic. This can be seen in the same way as in [4, 5]: the $\frac{q-1}{2}$-th power can be interpreted as a mapping $\tau : \mathbb{F}_q \to \mathbb{F}_3 = \{0, 1, -1\}$ by observing that for all $a \in \mathbb{F}_q$, $a^{(q-1)/2} \in \{0, 1, -1\} \subset \mathbb{F}_q$. More precisely $a^{(q-1)/2}$ is 0 if $a = 0$, 1 if a is a square, and -1 if a is a nonsquare. Thus we obtain the same lower bound for the subset of polynomials in $\mathcal{F}_q(n,t)$ that can be written as

$$f(x_1, \ldots, x_n) = \tilde{f}(x_1^{(q-1)/2}, \ldots, x_n^{(q-1)/2})$$

for some polynomial $\tilde{f}$.

Table 1 gives some numeric examples of the improvements achieved in this paper.

n	3	4	5	6	8	11	11
$\lfloor \log t \rfloor$	2	2	2	2	2	2	3
lower bound [1]	7	11	16	22	37	67	232
lower bound [5]	16	27	41	58	101	188	848
new lower bound	19	31	46	64	112	220	1199
upper bound [1]	19	33	51	73	129	243	1563

Figure 1: Lower and upper bounds for small values

References

[1] Clausen, M., Dress, A., Grabmeier, J., Karpinski, M., *On Zero-Testing and Interpolation of k-sparse Multivariate Polynomials over Finite Fields*, TCS **84**, pp. 151–164, 1991.

[2] Dür, A., Grabmeier, J., *Applying Coding Theory to Sparse Interpolation*, SIAM J. Comput. **22**, 695–704, 1993.

[3] Grigoriev, D. Y., Karpinski, M., Singer, M. F. *Fast Parallel Algorithms for Sparse Multivariate Polynomial Interpolation over Finite Fields*, SIAM J. Comput. **19**, pp. 1059–1063, 1990.

[4] Werther, K., *Interpolation und Approximation Boolescher Formeln*, Masters Thesis, University of Bonn, October 1991.

[5] Werther, K., *The Computational Complexity of Interpolating Sparse Multivariate Polynomials over Finite Fields*, Research Report. No 8577-CS, University of Bonn, 1992, to appear in AAECC.

[6] Zippel, R., *Probabilistic Algorithms for Sparse Polynomials*, LNCS 72, pp. 216–226, 1979.

[7] Zippel, R., *Interpolating Polynomials from their Values*, J. Symb. Comp. **9**, 375–403, 1990.