

The density of weights of Generalized Reed–Muller codes

Shachar Lovett *

Weizmann Institute of Science
shachar.lovett@weizmann.ac.il

April 5, 2009

Abstract

We study the density of the weights of Generalized Reed–Muller codes. Let $RM_p(r, m)$ denote the code of multivariate polynomials over \mathbb{F}_p in m variables of total degree at most r . We consider the case of fixed degree r , when we let the number of variables m tend to infinity. We prove that the set of relative weights of codewords is quite sparse: for every $\alpha \in [0, 1]$ which is not rational of the form $\frac{\ell}{p^k}$, there exists an interval around α in which no relative weight exists, for any value of m . This line of research is to the best of our knowledge new, and complements the traditional lines of research, which focus on the weight distribution and the divisibility properties of the weights.

Equivalently, we study distributions taking values in a finite field, which can be approximated by distributions coming from constant degree polynomials, where we do not bound the number of variables. We give a complete characterization of all such distributions.

1 Introduction

We study the weights of Generalized Reed–Muller codes.

Definition 1 (Generalized Reed–Muller codes). Let \mathbb{F}_p be a prime finite field. We denote by $RM_p(r, m)$ the r^{th} -order Generalized Reed–Muller code with m variables. This is a linear code over \mathbb{F}_p , whose codewords $f \in RM_p(r, m) : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ are evaluations of polynomials over \mathbb{F}_p in m variables of total degree at most r .

Definition 2 (Weights). Let \mathcal{C} be a code. The weight of a codeword $f \in \mathcal{C}$ is the number of non-zero elements in it. For $\mathcal{C} = RM_p(r, m)$, this is

$$\text{wt}(f) = |\{\mathbf{x} \in \mathbb{F}_p^m : f(\mathbf{x}) \neq 0\}|$$

*Research supported by the Israel Science Foundation (grant 1300/05).

One of the main problems in coding theory is understanding the possible weights and the distribution of the weights for various families of codes. Generalized Reed–Muller codes are one of the more basic family of codes, and has been researched extensively. To quote [15]:

Reed–Muller (or RM) codes are one of the oldest and best understood families of codes

Understanding the weights of codewords of Generalized Reed–Muller codes is considered to be one of the important questions in coding theory, however our current understanding of it is quite limited. There are two traditional lines of research regarding the weights of Generalized Reed–Muller codes: their distribution, and their divisibility properties. We introduce in this work a third line of research, studying the density of the weights.

We study the weights of codewords of $RM_p(r, m)$ when we fix the order r and let the number of variables m tend to infinity. This can be better described in terms of the relative weights of the codewords.

Definition 3 (Relative weights). Let \mathcal{C} be a code. The relative weight of a codeword $f \in \mathcal{C}$ is the *fraction* of non-zero elements in it. For $\mathcal{C} = RM_p(r, m)$, this is

$$\mathbf{rel-wt}(f) = \frac{1}{p^m} |\{\mathbf{x} \in \mathbb{F}_p^m : f(\mathbf{x}) \neq 0\}| = \Pr_{x \in \mathbb{F}_p^m} [f(x) \neq 0]$$

Let $W_p(r, m)$ be the set of relative weights of codewords of $RM_p(r, m)$:

$$W_p(r, m) = \{\mathbf{rel-wt}(f) : f \in RM_p(r, m)\}$$

Since $RM_p(r, m)$ can be embedded in $RM_p(r, m+1)$, we have $W_p(r, m) \subseteq W_p(r, m+1)$. Thus it makes sense to consider the limit of the weights when $m \rightarrow \infty$. We define $W_p(r)$ to be the set of weights of codewords of $RM_p(r, m)$ where we do not restrict m , i.e.

$$W_p(r) = \bigcup_{m \in \mathbb{N}} W_p(r, m)$$

The set $W_p(r)$ is contained in the interval $[0, 1]$, and in fact can be further restricted based on the minimal relative weight of $RM_p(r, m)$, which is well known (see for example [4]). We are interested however in the density of the weight set. Our a-priory intuition was that the set $W_p(r)$ should be relatively dense, since we allow the number of variables to grow indefinitely. However, our main theorem shows that the truth is quite far from it. In order to state it, we first define the notion of p -rational numbers.

Definition 4 (p -rational numbers). We say a number $\alpha \in [0, 1]$ is p -rational if it is rational of the form $\alpha = \frac{\ell}{p^k}$ for some integers ℓ, k .

Theorem 1 (Main theorem). *Let $\alpha \in [0, 1]$ be a number which is not p -rational. Then there exists $\epsilon > 0$ such that $W_p(r)$ contains no value in the interval $(\alpha - \epsilon, \alpha + \epsilon)$. Equivalently, there is no sequence of multivariate polynomials f_1, f_2, \dots over \mathbb{F}_p of degree at most r , each possibly on a different number of variables, such that $\lim_{k \rightarrow \infty} \mathbf{rel-wt}(f_k) = \alpha$.*

Thus, around every $\alpha \in [0, 1]$ which is not p -rational, there is a "hole", in which there are no relative weights of $RM_p(r, m)$.

Another way to view Theorem 1 is as a theorem about the approximation of random variables over finite fields by low-degree polynomials.

Definition 5 (Distribution of a polynomial). The distribution of a polynomial $f(x_1, \dots, x_m)$ over \mathbb{F}_p is defined to be the distribution of f applied to a uniform input in \mathbb{F}_p^m .

Let X be a random variable taking values in \mathbb{F}_p . We say X can be approximated by degree- r polynomials, if its distribution can be arbitrarily approximated by the distribution of degree- r polynomials. That is to say, for every $\epsilon > 0$, there exists a multi-variate polynomial $f(x_1, \dots, x_m)$ over \mathbb{F}_p of total degree at most r , whose distribution is ϵ -close to the distribution of X (for example in statistical distance). The following is an immediate corollary of Theorem 1.

Corollary 2. *Let X be a random variable taking values in \mathbb{F}_p , which can be approximated by degree- r polynomials, for some constant r . Then all the probabilities $\Pr[X = a]$ are p -rational. In particular, X can be realized as the distribution of a single polynomial over \mathbb{F}_p .*

So for example, we cannot have an arbitrary good approximation of perfect random bits by constant degree polynomials over \mathbb{F}_3 , for any constant degree, since $1/2$ is not 3-rational.

Returning to the framework of weights of Generalized Reed–Muller codes, we note that although the set $W_p(r)$ is sparse, it is not finite. For example, consider the set $W_2(2)$, the set of relative weights of quadratics over \mathbb{F}_2 . The relative weight of $f(x_1, \dots, x_{2k}) = x_1x_2 + x_3x_4 + \dots + x_{2k-1}x_{2k}$ is $\frac{2^k+1}{2^{k+1}}$, and the set of these weights is infinite.

1.1 Related work

As we mentioned before, the two traditional lines of research regarding the weights of Generalized Reed–Muller codes are studying their weight distribution and their divisibility properties. We now describe them in more details.

The weight distribution of $RM_p(r, m)$ is the number of codewords below a certain weight. The case of $r = 1$, i.e. of linear functions, is trivial, since all non-constant codewords have the same weight. The case of $r = 2$, i.e. of quadratic functions, is also fully understood. A theorem of Dixon [15] gives a canonical characterization of quadratic functions, and in particular gives the possible weights and the weight distribution of quadratic functions. By the McWilliams identity, this characterizes the weight distribution of their dual codes, which are $RM_p(m - 2, m)$ and $RM_p(m - 3, m)$. These are, to the best of our knowledge, the only (non-trivial) orders for which complete characterization of the weights of Generalized Reed–Muller codes is known. For other orders, complete characterization is known only for specific values of m . For example, for cubics the record is the work of Sugita, Kasami and Fujiwara [17], characterizing the weight distribution for $RM_2(3, 9)$.

Considering general orders, several characteristics of the weights are known. The minimal weight of non-zero codewords in $RM_p(r, m)$ is known, as are as are the codewords achieving

this minimal distance [4]. In the case of Reed–Muller codes, corresponding to $p = 2$, Kasami and Tokura [11] give a complete characterization of codewords of weight at most *twice* the minimal weight of the code, and Azumi, Kasami and Tokura [1] gave a characterization of codewords of weight at most 2.5 the minimal weight of the code. Recently, Kaufman and the author [10] gave a relatively tight estimate on the number of codewords in Reed–Muller codes, holding for all weights.

The second line of research is divisibility of the weights of codewords. Ax [2] proved that all weights of codewords $f \in RM_p(r, m)$ are divisible by $p^{\lceil m/r \rceil - 1}$. This was later generalized to general codes [13, 5]. For a survey on divisible codes see [18] or [12].

1.2 Organization

The paper is organized as follows. Theorem 1 is proved in Section 2. The proof is based on a technical lemma which is proved in Section 3.

2 Proof of Theorem 1

We study codewords $f \in RM_p(r, m)$. Equivalently, we study polynomials: f is a polynomial over \mathbb{F}_p in m variables of total degree at most r . First, we fix some notations. We denote probabilities according to a distribution D by $\Pr_{z \sim D}$. For a set S we denote by U_S the uniform distribution over S , and we shorthand $\Pr_{z \in S}$ for $\Pr_{z \sim U_S}$. We let $\mathbb{N} = \{1, 2, \dots\}$ denote the set of natural numbers. We will denote elements of \mathbb{F}_p^m by $\mathbf{x} = (x_1, \dots, x_m)$, and polynomials or functions by $f(\mathbf{x}) = f(x_1, \dots, x_m)$. When we refer to the degree of a polynomial, we will always mean its total degree. The relative weight of a polynomial/function $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ is the fraction of non-zero elements in it,

$$\mathbf{rel-wt}(f) = \Pr_{\mathbf{x} \in \mathbb{F}_p^m} [f(\mathbf{x}) \neq 0]$$

In order to prove Theorem 1 we will show that for any degree- r polynomial $f(x_1, \dots, x_m)$, there exists a function $g(x_1, \dots, x_c)$ on a constant number of inputs (i.e. independent of m), such that $\mathbf{rel-wt}(f) \approx \mathbf{rel-wt}(g)$. This is straight-forward if the required approximation is fixed a-priori; we show this can be achieved even if the error is allowed to depend arbitrarily on the number of inputs c .

Lemma 3. *Let $\mathcal{E} : \mathbb{N} \rightarrow (0, 1)$ be an arbitrary mapping from the naturals to $(0, 1)$. For any constant degree r there exists a constant $C = C(\mathbb{F}_p, r, \mathcal{E}(\cdot))$ such that the following holds: for any degree- r polynomial $f(\mathbf{x}) = f(x_1, \dots, x_m)$, there exists $c \leq C$ and a function $g(x_1, \dots, x_c)$, such that*

$$|\mathbf{rel-wt}(f) - \mathbf{rel-wt}(g)| < \mathcal{E}(c)$$

Remark. In fact, a somewhat stronger version of the lemma also holds. Not only $|\mathbf{rel-wt}(f) - \mathbf{rel-wt}(g)| < \mathcal{E}(c)$. but the statistical distance between the distributions of f and g is bounded by $\mathcal{E}(c)$. However, we will not need this stronger version in the proof of Theorem 1.

We now prove Theorem 1 using Lemma 3.

Proof of Theorem 1. Let $\alpha \in (0, 1)$ be a number which is not p -rational, and assume by contradiction there exists a sequence of polynomials f_1, f_2, \dots of degree at most r , where $f_k = f_k(x_1, \dots, x_{m_k})$, whose relative weights converge to α ,

$$\lim_{k \rightarrow \infty} \text{rel-wt}(f_k) = \alpha.$$

We now define a mapping δ from the naturals to $(0, 1)$. For every $c \in \mathbb{N}$, define $\delta(c)$ to be the distance of α from the set of rational numbers of the form $\frac{\ell}{p^c}$. Explicitly, $\delta(c)$ is given by

$$\delta(c) = \min \left\{ \alpha - \frac{\lfloor \alpha p^c \rfloor}{p^c}, \frac{\lceil \alpha p^c \rceil}{p^c} - \alpha \right\}$$

Notice that $\delta(\cdot)$ is non-increasing, and by our assumption that α is not p -rational, $\delta(c) > 0$ for all $c \in \mathbb{N}$.

Set $\mathcal{E}(c) = \frac{\delta(c)}{4}$. Once we fix the mapping $\mathcal{E}(\cdot)$, we can use Lemma 3: there exists a constant $C = C(\mathbb{F}_p, r, \mathcal{E}(\cdot))$, such that for any polynomial f_k there exists $c_k \leq C$, and a function $g_k(x_1, \dots, x_{c_k})$, such that

$$|\text{rel-wt}(f_k) - \text{rel-wt}(g_k)| < \mathcal{E}(c_k) = \frac{\delta(c_k)}{4} \quad (1)$$

Since $\lim_{k \rightarrow \infty} \text{rel-wt}(f_k) = \alpha$, and $\mathcal{E}(\cdot)$ is positive, there exists some k such that

$$|\text{rel-wt}(f_k) - \alpha| < \mathcal{E}(C) = \frac{\delta(C)}{4} \quad (2)$$

Combining (1) and (2), and since $\delta(\cdot)$ is non-increasing, we get that

$$|\text{rel-wt}(g_k) - \alpha| < \frac{\delta(c_k)}{4} + \frac{\delta(C)}{4} \leq \frac{\delta(c_k)}{2} \quad (3)$$

We now show this cannot hold. g_k is a function on c_k inputs; thus, its relative weight is rational of the form $\frac{\ell}{p^{c_k}}$. By definition of $\delta(\cdot)$:

$$|\text{rel-wt}(g_k) - \alpha| = \left| \frac{\ell}{p^{c_k}} - \alpha \right| \geq \delta(c_k) \quad (4)$$

Combining (3) and (4) yields a contradiction. Thus, α must be p -rational. □

3 Proof of Lemma 3

The proof of Lemma 3 is based on regularity results for constant degree polynomials by Green and Tao [8] and by Kaufman and Lovett [9]. We first make some definitions. In this section, all polynomials will be polynomials over \mathbb{F}_p in m variables.

Definition 6 (rank of polynomials). Let $f(\mathbf{x})$ be a degree- r polynomial. The $(r-1)$ -rank of f , denoted by $\text{rank}_{r-1}(f)$, is the minimal number of degree- $(r-1)$ polynomials required to compute f . This means, $\text{rank}_{r-1}(f)$ is the minimal c such that there exists polynomials $g_1(\mathbf{x}), \dots, g_c(\mathbf{x})$ of degree at most $r-1$ and a function $F : \mathbb{F}_p^c \rightarrow \mathbb{F}_p$ such that

$$f(\mathbf{x}) = F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x}))$$

Definition 7 (regularity of polynomials). A degree- r polynomial $f(\mathbf{x})$ is T -regular if $\text{rank}_{r-1}(f) > T$. A set of polynomials $\{f_1(\mathbf{x}), \dots, f_c(\mathbf{x})\}$ is T -regular if all non-zero linear combinations of them are T -regular. This means, for every $a_1, \dots, a_c \in \mathbb{F}_p$ not all zero, let $f'(\mathbf{x}) = a_1 f_1(\mathbf{x}) + \dots + a_c f_c(\mathbf{x})$. We require that f' is not identically zero, and that if $\text{degree}(f') = k$, then $\text{rank}_{k-1}(f') > T$.

We will need the following result from [8]: any degree- r polynomial f is a function of a constant number of regular polynomials g_1, \dots, g_c , even if the regularity requirements on g_1, \dots, g_c depend on the number of polynomials c :

Lemma 4 (Lemma 2.3 in [8]). *Let $\mathcal{T} : \mathbb{N} \rightarrow \mathbb{N}$ by an arbitrary mapping. There exists a constant $C_1 = C_1(\mathbb{F}_p, r, \mathcal{T}(\cdot))$ such that the following holds. For any degree- r polynomial $f(\mathbf{x})$ there exists some $c \leq C_1$, a set of polynomials $g_1(\mathbf{x}), \dots, g_c(\mathbf{x})$ of degree at most r and a function $F : \mathbb{F}_p^c \rightarrow \mathbb{F}_p$, such that:*

1. $f(\mathbf{x}) = F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x}))$,
2. The set of polynomials $\{g_1(\mathbf{x}), \dots, g_c(\mathbf{x})\}$ is $\mathcal{T}(c)$ -regular.

We also need a result relating regularity of polynomials to their joint distribution.

Definition 8 (distribution of polynomials). Let $f : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$ be a polynomial. Its distribution $\mathcal{D}(f)$ is the distribution (taking values in \mathbb{F}_p) of applying f on a random input $\mathbf{x} \in \mathbb{F}_p^m$,

$$\mathcal{D}(f) = f(\mathbf{x})_{\mathbf{x} \sim U_{\mathbb{F}_p^m}}.$$

For a set of polynomials $f_1, \dots, f_c : \mathbb{F}_p^m \rightarrow \mathbb{F}_p$, their joint distribution $\mathcal{D}(f_1, \dots, f_c)$ (taking values in \mathbb{F}_p^c) is the distribution of applying f_1, \dots, f_c on a common random input $\mathbf{x} \in \mathbb{F}_p^m$,

$$\mathcal{D}(f_1, \dots, f_c) = (f_1(\mathbf{x}), \dots, f_c(\mathbf{x}))_{\mathbf{x} \sim U_{\mathbb{F}_p^m}}.$$

Definition 9 (statistical distance). Let D', D'' be two distributions taking values in the same set S . Their statistical distance is

$$\text{dist}(D', D'') = \frac{1}{2} \sum_{s \in S} |\Pr[D' = s] - \Pr[D'' = s]|.$$

The following result from [9] shows that polynomials whose distribution is not close to uniform must have low rank:

Lemma 5 (Theorem 4 in [9]). *Let $f(\mathbf{x})$ be a degree- r polynomial such that $\text{dist}(\mathcal{D}(f), U_{\mathbb{F}_p}) \geq \epsilon$. Then $\text{rank}_{r-1}(f) \leq C_2(\mathbb{F}_p, r, \epsilon)$.*

We combine Lemma 4 and Lemma 5 to prove the following lemma, showing that any degree- r polynomial is a function of a constant number of polynomials which are uncorrelated.

Lemma 6. *Let $\mathcal{E} : \mathbb{N} \rightarrow (0, 1)$ be an arbitrary mapping from the naturals to $(0, 1)$. For any constant degree r there exists a constant $C = C(\mathbb{F}_p, r, \mathcal{E}(\cdot))$ such that the following holds: For any degree- r polynomial $f(\mathbf{x})$ there exists some $c \leq C$, a set of polynomials $g_1(\mathbf{x}), \dots, g_c(\mathbf{x})$ of degree at most r and a function $F : \mathbb{F}_p^c \rightarrow \mathbb{F}_p$, such that:*

1. $f(\mathbf{x}) = F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x}))$,
2. $\text{dist}(\mathcal{D}(g_1, \dots, g_c), U_{\mathbb{F}_p^c}) < \mathcal{E}(c)$.

Proof. We will choose $\mathcal{T} : \mathbb{N} \rightarrow \mathbb{N}$ large enough, to be specified later, and apply Lemma 4. Let g_1, \dots, g_c be the polynomials given by the lemma such that $f(\mathbf{x}) = F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x}))$, and the set $\{g_1, \dots, g_c\}$ is $\mathcal{T}(c)$ -regular. We will show that if we choose $\mathcal{T}(\cdot)$ large enough, we can guarantee that $\mathcal{D}(g_1, \dots, g_c)$ is close to uniform.

We first reduce the task to guaranteeing that all the non-zero linear combinations of g_1, \dots, g_c are close to uniform. We claim that in order to guarantee that $\text{dist}(\mathcal{D}(g_1, \dots, g_c), U_{\mathbb{F}_p^c}) < \mathcal{E}(c)$, it is enough to guarantee for every non-zero linear combination $g'(\mathbf{x}) = a_1 g_1(\mathbf{x}) + \dots + a_c g_c(\mathbf{x})$ that $\text{dist}(\mathcal{D}(g'), U_{\mathbb{F}_p}) < p^{-c} \mathcal{E}(c)$. The proof is by simple Fourier analysis: see for example Claim 33 in [3].

Given this reduction, we show it is enough to require that g' is regular. Assume $\text{dist}(\mathcal{D}(g'), U_{\mathbb{F}_p}) \geq p^{-c} \mathcal{E}(c)$. Either $g' \equiv 0$, or, by Lemma 5, if $\text{degree}(g') = k$ then

$$\text{rank}_{k-1}(g') \leq C_2(\mathbb{F}_p, k, p^{-c} \mathcal{E}(c)) \tag{5}$$

In any case, if we set $\mathcal{T}(c) = \max_{1 \leq k \leq r} C_2(\mathbb{F}_p, k, p^{-c} \mathcal{E}(c))$, we get that the set $\{g_1, \dots, g_c\}$ is not $\mathcal{T}(c)$ -regular, since g' is not $\mathcal{T}(c)$ -regular. This is a contradiction to the promise of Lemma 4.

Hence we conclude that the joint distribution $\mathcal{D}(g_1, \dots, g_c)$ has statistical distance of at most $\mathcal{E}(c)$ to the uniform distribution \mathbb{F}_p^c , where $c \leq C$ and

$$C = C_1(\mathbb{F}_p, d, \mathcal{T}(\cdot))$$

□

Before proving Lemma 3, we will also need the following simple claim: the statistical distance between distributions bounds the probability that a function will be able to distinguish between them:

Claim 7. *Let D', D'' be two distributions taking values in the same set S . Then for any subset $S' \subseteq S$:*

$$\left| \Pr_{z \sim D'}[z \in S'] - \Pr_{z \sim D''}[z \in S'] \right| \leq \text{dist}(D', D'')$$

We are now ready to prove Lemma 3.

Proof of Lemma 3. Let $f(\mathbf{x})$ be a degree- r polynomial. Apply Lemma 6. There exists some $C = C(\mathbb{F}_p, r, \mathcal{E}(\cdot))$ such that there is $c \leq C$, a set of polynomials $g_1(\mathbf{x}), \dots, g_c(\mathbf{x})$ and a function $F : \mathbb{F}_p^c \rightarrow \mathbb{F}_p$ such that

1. $f(\mathbf{x}) = F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x}))$,
2. $\text{dist}(\mathcal{D}(g_1, \dots, g_c), U_{\mathbb{F}_p^c}) < \mathcal{E}(c)$.

We claim that the function $F(y_1, \dots, y_c)$, where $y_1, \dots, y_c \in \mathbb{F}_p$ are independent variables, have approximately the same relative weight as that of $f(\mathbf{x}) = F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x}))$. We bound:

$$\begin{aligned} & |\text{rel-wt}(f) - \text{rel-wt}(F)| = \\ & \left| \Pr_{\mathbf{x} \in \mathbb{F}_p^m} [F(g_1(\mathbf{x}), \dots, g_c(\mathbf{x})) \neq 0] - \Pr_{y_1, \dots, y_c \in \mathbb{F}_p} [F(y_1, \dots, y_c) \neq 0] \right| = \\ & \left| \Pr_{\mathbf{x} \in \mathbb{F}_p^m} [(g_1(\mathbf{x}), \dots, g_c(\mathbf{x})) \in F^{-1}(\mathbb{F}_p \setminus \{0\})] - \Pr_{y_1, \dots, y_c \in \mathbb{F}_p} [(y_1, \dots, y_c) \in F^{-1}(\mathbb{F}_p \setminus \{0\})] \right| \leq \\ & \text{dist}(\mathcal{D}(g_1, \dots, g_c), \mathcal{D}(y_1, \dots, y_c)) = \\ & \text{dist}(\mathcal{D}(g_1, \dots, g_c), U_{\mathbb{F}_p^c}) < \mathcal{E}(c). \end{aligned}$$

□

4 Open problems

We studied in this work the density of the weights of $RM_p(r, m)$ where we keep r constant. We proved that any $\alpha \in [0, 1]$ which is not p -rational, cannot be the limit of relative weights of constant degree polynomials. However, we can ask what is the asymptotics of the degrees of polynomials that are required to approximate α , i.e, for every $\epsilon > 0$, what should be the the degree of $f(\mathbf{x})$ such that $|\text{rel-wt}(f) - \alpha| < \epsilon$, and how do this degree depend on ϵ ?

Another open problem is giving good bounds on the constant C in Lemma 3. We note that the current proof depends on Lemma 4 and Lemma 5, for which no good bounds are currently known.

Acknowledgements I thank Amir Shpilka for raising the problem studied in this paper, in the context of pseudorandom generators for polynomials. I thank my instructor, Omer Reingold, for his constant support and encouragement. I thank Alex Samorodnitsky, Tali Kaufman and Simon Litsyn on helpful discussions.

References

- [1] S. Azumi, T. Kasami and N. Tokura. *On the weight enumeration of weights less than 2.5d of Reed-Muller codes*. In Information and Control, 30(4):380–395, 1976.

- [2] J. Ax. *Zeros of polynomials over finite fields*. In the Amer. J. Math., vol. 86, pp. 255–261, 1964.
- [3] A. Bogdanov and E. Viola. *Pseudorandom Bits for Polynomials*. In the 48th Annual Symposium on Foundations of Computer Science (FOCS), pp. 41–51, 2007.
- [4] P. Delsarte, J. M. Goethals, and F. J. MacWilliams. *On generalized Reed-Muller codes and their relatives*. In Information and Control, 16:403-442, 1970.
- [5] P. Delsarte and R.J.McEliece. *Zeros of functions in finite abelian group algebras*. In Amer. J. Math. 98:197–224, 1976.
- [6] P. Gopalan, A. Klivans and D. Zuckerman. *List-Decoding Reed Muller Codes over Small Fields*. In the Proceedings of the 40th ACM Symposium on Theory of Computing (STOC), pp. 265–274, 2008.
- [7] O. Goldreich. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*. Springer-Verlag, Algorithms and Combinations, 1998.
- [8] B. Green and T.Tao. *The distribution of polynomials over finite fields, with applications to the Gowers norms*. submitted, 2007.
- [9] T. Kaufman and S. Lovett. *Worst case to Average Case Reductions for Polynomials*. In the Proceedings of the 49th Annual Symposium on Foundations of Computer Science (FOCS), pp. 166–175, 2008.
- [10] T. Kaufman and S. Lovett. *List Size vs. Decoding Radius for Reed–Muller Codes*. submitted, 2008.
- [11] T. Kasami and N. Tokura. *On the weight structure of Reed–Muller codes*. In the IEEE transactions on Information Theory, 16(6), pp. 752–759, 1970.
- [12] X. Liu. *On Divisible Codes over Finite Fields*. Ph.D. Thesis, 2006.
- [13] R. J. McEliece. *Weight congruences for p -ary cyclic codes*. In Discrete Math. 3:177–192, 1972.
- [14] R. Motwani and R. Raghavan. *Randomized Algorithms*. Cambridge University press, 1995.
- [15] F. MacWilliams and N. Sloane. *The theory of Error-Correcting Codes*. North-Holland, 1977.
- [16] R. Shaltiel. *Recent developments in explicit constructions of extractors*. In the Bulletin of the European Association for Theoretical Computer Science, 77:67–95, 2002.

- [17] T. Sugita, T. Kasami and Toru Fujiwara. *The weight distribution of the third-order Reed-Muller code of length 512*. In IEEE Transactions on Information Theory 42(5): 1622-1625 (1996).
- [18] H. Ward. *Divisible codes - a survey*. In Serdica Math. J. 27:263–278, 2004.