On the Second Weight of Generalized Reed-Muller Codes[1]

Olav Geil
Department of Mathematical Sciences
Aalborg University
Email: olav@math.aau.dk

Abstract: Not much is known about the weight distribution of the generalized Reed-Muller code $\mathrm{RM}_q(s,m)$ when $q>2$, $s>2$ and $m\geq 2$. Even the second weight is only known for values of s being smaller than or equal to $q/2$. In this paper we establish the second weight for values of s being smaller than q. For s greater than $(m-1)(q-1)$ we then find the first $s+1-(m-1)(q-1)$ weights. For the case $m=2$ the second weight is now known for all values of s. The results are derived mainly by using Gröbner basis theoretical methods.

Keywords: Footprint, generalized Reed-Muller code, Gröbner basis, Hamming weight, weight distribution.

AMS classifications: 11G25 - 11T71 - 12.25

1 Introduction

Let $\mathbb{F}_q$ be any finite field and write $\mathbb{F}_q^m=\{P_1,\ldots,P_{q^m}\}$. In the present paper we consider the generalized Reed-Muller codes

$$\begin{aligned}\mathrm{RM}_q(s,m) &:= \{(F(P_1),\ldots,F(P_{q^m}))\mid F\in\mathbb{F}_q[X_1,\ldots,X_m],\deg(F)\leq s\}\\ &= \{(F(P_1),\ldots,F(P_{q^m}))\mid F\in\mathbb{F}_q[X_1,\ldots,X_m],\\ &\qquad \deg(F)\leq s,\deg_{X_i}(F)<q,\quad \text{for}\quad i=1,\ldots,m\}.\end{aligned}\tag{1}$$

Here, $\deg(F)$ denotes the total degree of F and $\deg_{X_i}(F)$ is the X_i-degree of F. The minimum distance d was established four decades ago in [6]. Soon after in [3] the polynomials producing codewords of weight d were shown all to be products of linear factors. Using this information it was possible to calculate the number of codewords with Hamming weight d. For $m=1$ generalized Reed-Muller codes are just extended Reed-Solomon codes which are known to be MDS. As there is a formula for the weight distribution of any MDS code (see [7, Th. 6, Chap. 11]) the weight distribution is known for $\mathrm{RM}_q(s,1)$. The problem of establishing the weight distribution of $\mathrm{RM}_q(s,m)$, $q\geq 2$, $m\geq 2$ and arbitrary s remains an unsolved problem even today. For $s\leq 2$ the entire weight distribution was described in [8]. For the special case of ordinary Reed-Muller codes, that is the case $q=2$, there are various results in the literature. However, for $q>2$, $s>2$ and $m\geq 2$ not much is known.

[1]This research is in part supported by the Danish National Science Research Council Grant FNV-21040368

For the case $q > 2$, $s > 2$ and $m \geq 2$ special attention has been given to calculate the second weight and to find the number of codewords having this weight. The first result in this direction was made in [1]. Recently, in [9] the results from [1] regarding the second weight were improved significantly so that we now have a complete picture for all generalized Reed-Muller codes $\mathrm{RM}_q(s, m)$ with $s \leq q/2$. The methods used in [9] were of a geometric nature. The main result was that if a polynomial $F(X_1, \ldots, X_m)$ of total degree s, $2 \leq s \leq q/2$ *is not* a product of linear factors then it has less than $sq^{m-1} - (s-1)q^{m-2}$ zeros. This was then combined with the result from [1] that if one consider instead the class of polynomials of total degree s, $2 \leq s < q$ that *are* products of linear factors then the second highest attainable number of zeros in this class is $sq^{m-1} - (s-1)q^{m-2}$. In the present paper we take on a completely different approach than the one used in [9], by using instead pure Gröbner basis theoretical methods. Doing this we are able to prove that the second weight equals $q^m - sq^{m-1} + (s-1)q^{m-2}$ for all s with $2 \leq s < q$. Using next some straightforward arguments we find the first $s + 1 - (m-1)(q-1)$ weights for all s with $(m-1)(q-1) < s \leq m(q-1)$. In particular for $m = 2$ the second weight is now known for every choice of s. For all the weights w that we discover there exist codewords of Hamming weight w which are made from products of linear factors. We should mention that our methods does not tell us if there are other polynomials from which codewords of Hamming weight w can be made.
The paper is organized as follows. In Section 2 we describe the Gröbner basis theoretical methods to be used. We illustrate the methods by applying them to the question of determining what is the minimum distance. Section 3 is concerned with the case $s < q$, and Section 4 deals with the case $(m-1)(q-1) < s \leq m(q-1)$.

2 Gröbner basis theoretical tools

Definition 1 *Let $\mathbb{F}$ be a field and let $\prec$ be a monomial ordering on*

$$\mathcal{M}(X_1, \ldots, X_m) := \{X_1^{i_1} \cdots X_m^{i_m} \mid i_1, \ldots, i_m \in \mathbb{N}_0\}.$$

Given an ideal $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ the footprint of I is

$$\Delta_\prec(I) := \{M \in \mathcal{M}(X_1, \ldots, X_m) \mid M \text{ is not the leading monomial of any polynomial in } I\}.$$

When only one monomial ordering is under consideration sometimes we write $\Delta(I)$ instead of $\Delta_\prec(I)$.

Our interest in the footprint arises from the following proposition. For any ideal $I \subseteq \mathbb{F}_q[X_1, \ldots, X_m]$ this proposition provides a method for estimating the size of the variety $\mathbb{V}_{\mathbb{F}_q}(I)$.

Proposition 1 *Let the notation be as in Definition 1 and consider the ideal*

$$\begin{aligned} I &= \langle F_1(X_1, \ldots, X_m), \ldots, F_s(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m \rangle \\ &\subseteq \mathbb{F}_q[X_1, \ldots, X_m]. \end{aligned}$$

The footprint $\Delta_\prec(I)$ is finite and $\#\Delta_\prec(I) = \#\mathbb{V}_{\mathbb{F}_q}(I)$ holds.

Proof: See [4, Cor. 1]. □

Every ideal I, $I \subseteq \mathbb{F}[X_1, \ldots, X_m]$ possesses a particular type of basis from which the footprint is easily obtained. These are the Gröbner bases.

Definition 2 *A finite subset $G = \{G_1, \ldots, G_v\} \subseteq I$ is called a Gröbner basis for I with respect to $\prec$ if for any non-zero polynomial $F \in I$ there exists a G_i, $i \in \{1, \ldots, v\}$ such that $lm(G_i) \mid lm(F)$.*

To decide if a set $\{G_1, \ldots, G_v\}$ is a Gröbner basis with respect to $\prec$ we can use Buchberger's S-pair criteria which we explain in the following. Given non-zero polynomials $A(X_1, \ldots, X_m)$ and $B(X_1, \ldots, X_m)$ let $X_1^{\gamma_1} \cdots X_m^{\gamma_m}$ be the least common multiple of the leading monomials $\mathrm{lm}(A)$ and $\mathrm{lm}(B)$. The S-polynomial defined from A and B is

$$\mathrm{S}(A, B) := \frac{X_1^{\gamma_1} \cdots X_m^{\gamma_m}}{\mathrm{lt}(A)} A - \frac{X_1^{\gamma_1} \cdots X_m^{\gamma_m}}{\mathrm{lt}(B)} B.$$

Here $\mathrm{lt}(A)$ means the leading term of $A(X_1, \ldots, X_m)$. We next need to apply the division algorithm for multivariate polynomials which is a generalization of the usual division algorithm from the univariate case. It takes as input a polynomial and an ordered list of polynomials called divisors. It returns an ordered list of polynomials called quotients and a single polynomial called the remainder. We refer to [2, Sec. 2.3] for the details. For $1 \leq i < j \leq v$ we define

$$R(G_i, G_j) := S(G_i, G_j) \ \text{ rem } \ (G_1, \ldots, G_v),$$

where $S \ \text{ rem } \ (G_1, \ldots, G_v)$ means the remainder of S after division with $(G_1, \ldots, G_v)$. We are now able to state Buchberger's S-pair criteria (for a proof see [2, Th.6 p. 82]).

Theorem 1 *A set $\{G_1, \ldots, G_v\} \subseteq \mathbb{F}[X_1, \ldots, X_m]$ is a Gröbner basis for $\langle G_1, \ldots, G_v \rangle$ with respect to $\prec$ if and only if $R(G_i, G_j) = 0$ for all i, j with $1 \leq i < j \leq v$.*

In our application we will make use of the following remarks.

Remark 1 *To speed up the test in Theorem 1 we may use the fact that if the leading monomials of $A(X_1, \ldots, X_m)$ and $B(X_1, \ldots, X_m)$ are relatively prime then $S(A, B) \ \text{ rem } \ (A, B) = 0$ holds. For a proof of this fact see [2, Pro. 4, p. 101].*

Remark 2 *By the definition of an S-polynomial and by the nature of the division algorithm we have $R(G_i, G_j) \in \langle G_1, \ldots, G_v \rangle$ and if $R(G_i, G_j) \neq 0$ then $lm(R(G_i, G_j)) \preceq lm(S(G_i, G_j))$ holds.*

We conclude this section by showing that the minimum distance of the generalized Reed-Muller codes can be deduced by applying Proposition 1. The same method was used in [5] to deduce the minimum distance of the improved generalized Reed-Muller codes known as hyperbolic codes or Massey-Costello-Justesen codes. The original method used to derive the minimum distance of the generalized Reed-Muller codes ([6, Th. 5]) differs very much from our approach as it relies on the BCH-bound. We will need the following lemma that we proof in Appendix A.

Lemma 1 *Let $q, m, s \in \mathbb{N}$ be fixed with $0 \leq s \leq m(q-1)$. Consider tuples $(i_1, \ldots, i_m) \in \mathbb{N}_0^m$ such that $i_1, \ldots, i_m < q$ and $i_1 + \cdots + i_m \leq s$. The minimum value of $\prod_{l=1}^{m}(q - i_l)$ is $(q-b)q^{m-a-1}$, where $a, b \in \mathbb{N}_0$ satisfy $s = a(q-1) + b$ with $0 \leq b < q-1$.*

Theorem 2 *Given $s \in \mathbb{N}_0$ with $0 \leq s \leq m(q-1)$ write $s = a(q-1) + b$ with $a, b \in \mathbb{N}_0$ and $0 \leq b < q-1$. The minimum distance of $RM_q(s, m)$ is $(q-b)q^{m-a-1}$.*

Proof: We will use the total degree lexicographic ordering $\prec_t$ given by $X_1^{a_1} \cdots X_m^{a_m} \prec_t X_1^{b_1} \cdots X_m^{b_m}$ if $(a_1, \ldots, a_m) \neq (b_1, \ldots, b_m)$ and either $a_1 + \cdots + a_m < b_1 + \cdots + b_m$ holds or $a_1 + \cdots + a_m = b_1 + \cdots + b_m$ with the first non-zero entry of $(b_1 - a_1, \ldots, b_m - a_m)$ being positive holds. According to (1), the polynomials $F(X_1, \ldots, X_m)$ used in the construction of $\mathrm{RM}_q(s, m)$ satisfy $\deg(F) \leq s$ and $\deg_{X_i}(F) < q$ for $i = 1, \ldots, m$. Let $F(X_1, \ldots, X_m)$ be any fixed polynomial as above, and write $\mathrm{lm}(F) = X_1^{i_1} \cdots X_m^{i_m}$. By assumption we have $i_1, \ldots, i_m < q$. We observe that

$$\Delta(\langle F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m \rangle) \subseteq \Delta(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q \rangle)$$

holds, and therefore from Proposition 1 it follows that $F(X_1, \ldots, X_m)$ can have at most

$$\#\Delta(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q \rangle) = q^m - \prod_{l=1}^{m}(q - i_l)$$

zeros. Considering now all possible choices of polynomials $F(X_1, \ldots, X_m)$ we see that the minimum distance of $\mathrm{RM}_q(s, m)$ is at least

$$\min\{\prod_{l=1}^{m}(q - i_l) \mid 0 \leq i_1 < q, \ldots, 0 \leq i_m < q, i_1 + \cdots + i_m \leq s\}. \tag{2}$$

Having established a lower bound on the minimum distance we next want to establish an upper bound. To this end write $\mathbb{F}_q = \{a_1, \ldots, a_q\}$. For any $X_1^{i_1} \cdots X_m^{i_m}$ with $i_1, \ldots, i_m < q$ the polynomial $\prod_{l=1}^{m} \prod_{n=1}^{i_l}(X_l - a_n)$ has leading monomial $X_1^{i_1} \cdots X_m^{i_m}$, and has exactly $q^m - \prod_{l=1}^{m}(q - i_l)$ zeros. Considering all possible choices of $X_1^{i_1} \cdots X_m^{i_m}$ with $i_1 + \cdots + i_m \leq s$ we see that (2) is also an upper bound on the minimum distance. The theorem now follows by applying Lemma 1. □

In the next section we will see that Proposition 1 is not only useful when dealing with the minimum distance but is also useful when we want to determine the second weight.

3 The case $s < q$

The results in this section holds for $m \geq 2$. The case $m = 1$ is covered by the theory in the next section as for $m = 1$ the condition $2 \leq s < q$ is the same as the condition $(m-1)(q-1) < s \leq m(q-1)$ which is treated there.
To estimate the second highest possible number of zeros of the polynomials under consideration we will need two lemmas. The proofs of the lemmas can be found in Appendix A.

Lemma 2 *Let $q, m, s \in \mathbb{N}$ be fixed with $2 \leq m$ and $2 \leq s < q$. Consider tuples $(i_1, \ldots, i_m) \in \mathbb{N}_0^m$ such that $i_1, \ldots, i_m < s$ and $i_1 + \cdots + i_m = s$. The minimum value of $\prod_{l=1}^{m}(q - i_l)$ is $q^m - sq^{m-1} + (s-1)q^{m-2}$.*

Lemma 3 *Let $q, m, s \in \mathbb{N}$ be fixed with $2 \leq m$ and $2 \leq s < q$. Consider tuples $(i_1, \ldots, i_m) \in \mathbb{N}_0^m$ such that $i_1 < s$, $i_2, \ldots, i_m < q$ and $i_1 + \cdots + i_m = q$. The minimum value of $(s - i_1)\prod_{l=2}^{m}(q - i_l)$ is $(s-1)q^{m-2}$.*

Proposition 2 *Let $F(X_1, \ldots, X_m) \in \mathbb{F}_q[X_1, \ldots, X_m]$ be of total degree s where $2 \leq s < q$ and $2 \leq m$. Then either $F(X_1, \ldots, X_m)$ has sq^{m-1} zeros or it has at most $sq^{m-1} - (s-1)q^{m-2}$ zeros.*

Proof: Throughout the proof we will use the total degree lexicographic ordering which we described in the proof of Theorem 2. Let $X_1^{i_1} \cdots X_m^{i_m}$ be the leading monomial of $F(X_1, \ldots, X_m)$ with respect to this ordering. We have $i_1 + \cdots + i_m = s$.
Assume first that $0 \leq i_1 < s, \ldots, 0 \leq i_m < s$ holds. We get

$$\begin{aligned} & \#\Delta(\langle F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m\rangle) \\ \leq\ & \#\Delta(\langle X_1^{i_1} \cdots X_m^{i_m}, X_1^q, \ldots, X_m^q\rangle) \qquad (3) \\ =\ & q^m - \prod_{l=1}^{m}(q - i_l). \qquad (4) \end{aligned}$$

Applying Lemma 2 we see that (4) does not exceed $sq^{m-1} - (s-1)q^{m-2}$. By Proposition 1 this means that $F(X_1, \ldots, X_m)$ has at most $sq^{m-1} - (s-1)q^{m-2}$ zeros.
Assume finally without loss of generality that $i_1 = s$, $i_2 = \cdots = i_m = 0$ hold and that the leading coefficient of $F(X_1, \ldots, X_m)$ is 1. Consider the S-polynomial

$$\begin{aligned} H(X_1, \ldots, X_m) &:= S(X_1^q - X_1, F(X_1, \ldots, X_m)) \\ &= X_1^q - X_1 - X_1^{q-s}F(X_1, \ldots, X_m). \end{aligned}$$

We observe that the total degree of $H(X_1, \ldots, X_m)$ does not exceed q. We reduce $H(X_1, \ldots, X_m)$ modulo $(F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m)$ to get a polynomial $R(X_1, \ldots, X_m)$. If $R(X_1, \ldots, X_m) = 0$ then by Theorem 1 and Remark 1 $\mathcal{B} = \{F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m\}$ is a Gröbner basis. But then equality holds in (3) and by Proposition 1 $F(X_1, \ldots, X_m)$ has precisely sq^{m-1} zeros. If $R(X_1, \ldots, X_m)$ is non-zero then we consider its leading monomial, say $X_1^{v_1} \cdots X_m^{v_m}$. Clearly, $0 \leq v_1 < s, 0 \leq v_2 < q, \ldots, 0 \leq v_m < q$ and by

the last part of Remark 2 $\mathrm{lm}(R) \preceq \mathrm{lm}(H)$ holds and therefore $v_1 + \cdots + v_m \leq q$. By the first part of Remark 2 we have

$$\begin{aligned} & \#\Delta(\langle F(X_1, \ldots, X_m), X_1^q - X_1, \ldots, X_m^q - X_m \rangle) \\ \leq & \#\Delta(\langle X_1^s, X_2^q, \ldots, X_m^q, X_1^{v_1} \cdots X_m^{v_m} \rangle) \\ = & sq^{m-1} - (s - v_1) \prod_{i=2}^{m} (q - v_i). \end{aligned} \tag{5}$$

Applying Lemma 3 we see that (5) does not exceed $sq^{m-1} - (s-1)q^{m-2}$. By Proposition 1 this means that $F(X_1, \ldots, X_m)$ has at most $sq^{m-1} - (s-1)q^{m-2}$ zeros. □

Theorem 3 *Let s, m be integers with $2 \leq s < q$ and $2 \leq m$. The second weight of $RM_q(s, m)$ is equal to $sq^{m-1} - (s-1)q^{m-2}$. There exist codewords with Hamming weight equal to the second weight that are defined from products of linear factors.*

Proof: By Theorem 2 the minimum distance is $q^m - sq^{m-1}$. Therefore, by Proposition 2 the second weight is at least equal to the minimal value of $q^m - sq^{m-1} + (s-1)q^{m-2}$ and $q^m - (s-1)q^{m-1}$ which is $q^m - sq^{m-1} + (s-1)q^{m-2}$. Here, the expression $q^m - (s-1)q^{m-1}$ comes from applying the first part of Proposition 2 to a polynomial of total degree $s-1$. The polynomial $\left(\prod_{i=1}^{s-1}(X_1 - a_i)\right)(X_2 - a_1)$ has precisely $sq^{m-1} - (s-1)q^{m-2}$ zeros and the proof is complete. □

The proof of Proposition 2 does not reveal how many codewords that are of Hamming weight equal to the second weight $sq^{m-1} - (s-1)q^{m-2}$. Restricting however to codewords coming from products of linear factors [1, Th. 2.2] characterizes the ones that are of Hamming weight $sq^{m-1} - (s-1)q^{m-2}$ and [1, Cor. 2.1] counts them for all choices of s with $2 \leq s < q-1$. We conclude that [1, Cor. 2.1] can serve as a lower bound on the number of codewords of Hamming weight equal to the second weight.

4 The case $(m-1)(q-1) < s$

In this section we consider generalized Reed-Muller codes with $(m-1)(q-1) < s$. We derive the first $s + 1 - (m-1)(q-1)$ weights.

Theorem 4 *Let s, m be integers with $1 \leq m$ and $(m-1)(q-1) \leq s \leq m(q-1)$. Write $s = (m-1)(q-1) + b$. For $t = 1, \ldots, b+1$ the t-th weight of $RM_q(s, m)$ is $(q-b) + (t-1)$. In particular for $(m-1)(q-1) < s \leq m(q-1)$ the second weight is $q-b+1$. There exist codewords of weight equal to the t-th weight which are defined from products of linear factors.*

Proof: For $t = 1$ the first result is just an incidence of Theorem 2. For arbitrary t, $t \geq 1$ we have $\mathrm{RM}_q(s-t+1, m) \subseteq \mathrm{RM}_q(s, m)$. Therefore, $\mathrm{RM}_q(s, m)$ contains

codewords of Hamming weight

$$\begin{aligned} d(\mathrm{RM}_q(s-1,m)) &= q-(b-1) = d(\mathrm{RM}_q(s,m))+1 \\ d(\mathrm{RM}_q(s-2,m)) &= q-(b-2) = d(\mathrm{RM}_q(s,m))+2 \\ &\vdots \\ d(\mathrm{RM}_q(s-b,m)) &= d(\mathrm{RM}_q(s,m))+b. \end{aligned}$$

Here, $d(C)$ denotes the minimum distance of C. The first result now follows from the very definition of the t-th weight. A generalized Reed-Muller code contains codewords of weight equal to the minimum distance which are made from products of linear factors (see [3, Th. 2.6.3]). The last result now follows by applying this observation to the code $\mathrm{RM}_q(s-t+1,m)$. □

Observe that for $m = 2$ Theorem 3 and Theorem 4 together give a complete description of the second weights for all possible choices of s, $2 \leq s$.

5 Acknowledgments

The author would like to thank the anonymous referees for their helpful comments.

A Proofs of the lemmas

Proof of Lemma 1:
For $\prod_{l=1}^{m}(q-i_l)$ to be smallest possible under the conditions $i_1,\ldots,i_m \in \mathbb{N}_0$, $i_1,\ldots,i_m < q$, $i_1+\cdots+i_m \leq s$, clearly $i_1+\cdots+i_m = s$ must hold. Among the tuples $(i_1,\ldots,i_m)$ such that $\prod_{l=1}^{m}(q-i_l)$ is equal to the minimum value we pick one such that $i_1 \geq \cdots \geq i_m$ holds. This is possible due to symmetry. Having chosen $(i_1,\ldots,i_m)$ as above we observe that there does not exist a $t \in \{1,\ldots,m-1\}$ such that $0 < i_t < q-1$, $0 < i_{t+1} < q-1$ holds. The presence of such a t would namely lead to

$$(q-i_1)\cdots(q-i_{t-1})(q-(i_t+1))(q-(i_{t+1}-1))(q-i_{t+2})\cdots(q-i_m) < \prod_{l=1}^{m}(q-i_l)$$

which is in contradiction with the assumption that $\prod_{l=1}^{m}(q-i_l)$ is equal to the minimum value. Hence, if $i_t < q-1$ we must have $i_{t+1} = 0$. Defining a and b as in the lemma we get for $s < m(q-1)$, $i_1 = \cdots = i_a = q-1$, $i_{a+1} = b$ and $i_s = 0$ for all $a+1 < s \leq m$. If $s = m(q-1)$ then $a = m$ and $b = 0$ and $i_1 = \cdots = i_m = (q-1)$ hold. The lemma follows by plugging the values into $\prod_{l=1}^{m}(q-i_l)$ □

Proof of Lemma 2: For $\prod_{l=1}^{m}(q-i_l)$ to be smallest possible under the conditions $i_1,\ldots,i_m \in \mathbb{N}_0$, $i_1,\ldots,i_m < s$ and $i_1+\cdots+i_m \leq s$ clearly $i_1+\cdots+i_m = s$

must hold. Among the tuples $(i_1, \ldots, i_m)$ such that $\prod_{l=1}^{m}(q - i_l)$ is equal to the minimum value we pick one such that $i_1 \geq \cdots \geq i_m$ holds. This is possible due to symmetry. Having chosen $(i_1, \ldots, i_m)$ as above we observe that if $m \geq 3$ then there does not exists a $t \in \{2, \ldots, m-1\}$ such that $0 < i_t$ and $0 < i_{t+1}$. The presence of such a t would namely lead to a contradiction similar to the one explained in the proof of Lemma 1. Hence, whether $m > 2$ or $m = 2$, only i_1 and i_2 are non zero. To determine the minimum value we are therefore left with minimizing $(q - i_1)(q - i_2)q^{m-2}$ under the assumptions $i_1 < s$, $i_2 < s$ and $i_1 + i_2 = s$. The minimum value is attained for $i_1 = s - 1$ and $i_2 = 1$ and the lemma now follows by plugging into $\prod_{l}^{m}(q - i_l)$ □

Proof of Lemma 3: We start by replacing the assumption $i_1 + \cdots + i_m = q$ with the assumption $i_1 + \cdots + i_m \leq q$. This does not change the minimum of $(s - i_1)\prod_{l=2}^{m}(q - i_l)$, but it will allow us to apply Lemma 1. Considering for a moment i_1 to be a fixed value we apply Lemma 1 to the problem of minimizing $\prod_{l=2}^{m}(q - i_l)$ under the assumption $i_2, \ldots, i_m < q$, $i_2 + \cdots + i_m \leq q - i_1$. Then we get that the minimum of $\prod_{l=2}^{m}(q - i_l)$ is

$$\begin{cases} (q-1)q^{m-3} & \text{if } \ i_1 = 0 \\ i_1 q^{m-2} & \text{if } \ i_1 > 0. \end{cases}$$

If we no longer consider i_1 to be a fixed value, but assume only that $0 \leq i_1 < s$ then the minimum value of $(s - i_1)\prod_{l=2}^{m}(q - i_l)$ is the smallest of the values

$$s(q-1)q^{m-3} \tag{6}$$

and

$$\min\{(s - i_1)i_1 q^{m-2} \mid i_1 = 1, \ldots, s-1\}.$$

The last value equals $(s-1)q^{m-2}$ which is smaller than (6). □

References

[1] J. P. Cherdieu and R. Rolland, On the Number of Points of Some Hypersurfaces in $\mathbb{F}_q^n$, *Finite Fields and their Applications*, **2**, (1996), 214-224.

[2] D. Cox, J. Little and D. O'Shea, *Ideals, Varieties, and Algorithms, Sec. Ed.*, Springer, 1997.

[3] P. Delsarte, J. M. Goethals, F. J. Mac Williams, On generalized Reed-Muller codes and their relatives, *Information and Control*, **16**, (1970), 403-442.

[4] O. Geil, On Codes From Norm-Trace Curves, *Finite Fields and their Applications*, **9**, (2003), 351-371.

[5] O. Geil and T. Høholdt, On Hyperbolic Codes, Proc. AAECC-14, *Lecture Notes in Computer Science* **2227**, (S. Bozta, I. Shparlinski, Eds.), Springer, (2001), 159-171.

[6] T. Kasami, S. Lin, W. Peterson, New generalizations of the Reed-Muller codes. I. Primitive codes, *IEEE Transactions on Information Theory*, **14**, (1968), 189-199.

[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes, First Ed., Eight Impression,* North-Holland, 1993.

[8] R. J. McEliece, Quadratic forms over finite fields and second-order Reed-Muller codes, *JPL Space Programs Summary*, **III**, (1969), 37-58.

[9] A. Sboui, Second highest number of points of hypersurfaces in $\mathbb{F}_q^n$, *Finite Fields and their Applications*, **13**, (2007), 444-449.