ACTA ARITHMETICA
176.1 (2016)

Polynomials meeting Ax's bound

by

XIANG-DONG HOU (Tampa, FL)

1. Introduction. Let $\mathbb{F}_q$ be the finite field with $q = p^m$ elements, where $p = \operatorname{char}\mathbb{F}_q$. Let $f \in \mathbb{F}_q[X_1, \dots, X_n]$ with $\deg f = d > 0$ and let $Z(f) = \{(x_1, \dots, x_n) \in \mathbb{F}_q^n : f(x_1, \dots, x_n) = 0\}$. Ax's theorem [A] states that

$$\nu_p(|Z(f)|) \geq m\left(\left\lceil \frac{n}{d} \right\rceil - 1\right), \tag{1.1}$$

where ν_p denotes the p-adic valuation. Ax's theorem is a strengthening of a result by Warning [War]. Further back along this line were a conjecture by Artin on the existence of nonzero roots of a homogeneous polynomial $f \in \mathbb{F}_q[X_1, \dots, X_n]$ with $n > \deg f$ and Chevalley's proof of Artin's conjecture (see [Ch]).

The main ingredient of the original proof of Ax's theorem is the Stickelberger congruence of Gauss sums. A different proof based on the same idea but without using Gauss sums and the Stickelberger congruence was given by Ward [Wa].

Ax's theorem has been extended to several polynomials by N. Katz [Ka]. Assume that $f_i \in \mathbb{F}_q[X_1, \dots, X_n]$, $1 \leq i \leq r$, are such that $\deg f_i = d_i > 0$ and $d_1 = \max_{1 \leq i \leq r} d_i$. Then

$$\nu_p\bigl(|Z(f_1) \cap \dots \cap Z(f_r)|\bigr) \geq m\left\lceil \frac{n - d_1 - \dots - d_r}{d_1} \right\rceil. \tag{1.2}$$

The original proof of Katz's theorem relied on sophisticated tools. A simpler proof was given by Wan [W1, W2] using a method similar to Ax's. A more elementary proof of Katz's theorem for prime fields was found by Wilson [Wi]. Sun [S] further extended Katz's theorem to prime fields along the line of Wilson's approach.

2010 *Mathematics Subject Classification*: Primary 11L05, 11T06; Secondary 94B27.
Key words and phrases: Ax's theorem, Katz's theorem, Gauss sum, Stickelberger congruence.
Received 7 January 2016; revised 8 June 2016.
Published online 30 September 2016.

Delsarte and McEliece [DM] studied functions from a finite abelian group A to $\mathbb{F}_q$, where $\gcd(|A|, q) = 1$. Such functions were treated as elements of the group algebra $\mathbb{F}_q[A]$. Instead of polynomials in $\mathbb{F}_q[X_1, \ldots, X_n]$ with a given degree, functions $f : A \to \mathbb{F}_q$ that belong to an ideal of $\mathbb{F}_q[A]$ were considered. (In coding theory, an ideal of $\mathbb{F}_q[A]$ is called an *abelian code.*) A lower bound for $\nu_p(|Z(f)|)$, established in [DM], implies Ax's theorem when A is the cyclic group of order $q^n - 1$. In [K] D. Katz generalized the result of [DM] to a lower bound for $\nu_p(|Z(f_1) \cap \cdots \cap Z(f_r)|)$, $f_1, \ldots, f_r \in \mathbb{F}_q[A]$, and when A is the cyclic group of order $q^n - 1$, the generalized bound gives the theorem of N. Katz.

Although not obvious, (1.2) *actually follows from* (1.1), which was proved by the present author [H].

The bounds in (1.1) and (1.2) are both sharp (see [A, Ka]). Therefore, improvements of these bounds are possible only under additional assumptions. For such improvements, see Cao [C], Cao and Sun [CS], and O. Moreno and C. Moreno [MM].

Focusing on (1.1), we note that another way to "improve" the bound is to find the next term in the p-adic expansion of $|Z(f)|$. In this paper, we will find an expression $E(f) \in \mathbb{F}_p$ such that

$$|Z(f)| \equiv q^{\lceil n/d \rceil - 1} E(f) \pmod{p^{m(\lceil n/d \rceil - 1) + 1}}. \tag{1.3}$$

Therefore,

$$\nu_p(|Z(f)|) \geq m\left(\left\lceil \frac{n}{d} \right\rceil - 1\right) + 1$$

if and only if $E(f) = 0$. The expression $E(f)$ is a homogeneous polynomial over $\mathbb{F}_p$ in the coefficients of f; it is not explicit in general. However, in several special but nontrivial cases, $E(f)$ can be made explicit. By exploiting this fact, we obtain several explicit formulas for the number of codewords in a Reed–Muller code with weight divisible by a power of p. More precisely, let $R_q(d, n)$ denote the *q-ary Reed–Muller code* $\{f \in \mathbb{F}_q[X_1, \ldots, X_n] : \deg f \leq d$, $\deg_{X_j} f \leq q - 1,\ 1 \leq j \leq n\}$, where deg is the total degree and $\deg_{X_j}$ is the degree in X_j, and let $N_q(d, n; t)$ be the number of codewords of $R_q(d, n)$ with weight divisible by p^t, where $p = \operatorname{char} \mathbb{F}_q$. We find explicit formulas for $N_q(d, n; t)$ in the following cases: (i) $q = 2^m$, n even, $d = n/2$, $t = m + 1$; (ii) $q = 2$, $n/2 \leq d \leq n - 2$, $t = 2$; (iii) $q = 3^m$, $d = n$, $t = 1$; (iv) $q = 3$, $n \leq d \leq 2n$, $t = 1$.

In fact, for a finite abelian group A and $f \in \mathbb{F}_q[A]$, Delsarte and McEliece found a formula for the next term in the p-adic expansion of $|Z(f)|$ (see [DM, (4.29)]). From that formula with $A = \mathbb{Z}/(q^n - 1)\mathbb{Z}$, one can derive an expression for the "next term" in Ax's theorem. The formula for the "next term" in [DM], including the case $A = \mathbb{Z}/(q^n - 1)\mathbb{Z}$, involves the Fourier transform of f which takes values in an extension of $\mathbb{F}_q$. In comparison, the expression $E(f)$ determined in (2.22) of the present paper is considerably simpler.

In Section 2, we determine the expression $E(f)$ in (1.3). The method is a refinement of the original proof of Ax's theorem and relies on a careful analysis of the Stickelberger congruence of Gauss sums. Applications to Reed–Muller codes are discussed in Section 3.

Throughout the paper, for $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{Z}^n$, the relations $\boldsymbol{u} \equiv \boldsymbol{v} \pmod{k}$ and $\boldsymbol{u} \le \boldsymbol{v}$ are understood componentwise. We define

$$\Delta_n = \begin{bmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{bmatrix}_{n \times n}. \tag{1.4}$$

2. p-adic expansion of $|Z(f)|$

2.1. Gauss sum and Stickelberger congruence. Facts gathered in this subsection can be found in any textbook on algebraic number theory, e.g., Lang [L, Ch. IV, §3].

For an integer $k > 0$, let $\zeta_k = e^{2\pi i/k}$. The ring of integers of a number field F is denoted by $\mathfrak{o}_F$. Let p be a rational prime, $m > 0$ and $q = p^m$. Let $\mathfrak{p}$ be a prime of $\mathfrak{o}_{\mathbb{Q}(\zeta_{q-1})}$ lying above p. Then $\mathfrak{p}$ is unramified over p and $\mathfrak{o}_{\mathbb{Q}(\zeta_{q-1})}/\mathfrak{p} = \mathbb{F}_q$. The *Teichmüller set* $T = \{0\} \cup \langle \zeta_{q-1} \rangle = \{0, \zeta_{q-1}^0, \ldots, \zeta_{q-1}^{q-2}\}$ forms a system of coset representatives of $\mathfrak{p}$ in $\mathfrak{o}_{\mathbb{Q}(\zeta_{q-1})}$, that is, $\mathbb{F}_q = \mathfrak{o}_{\mathbb{Q}(\zeta_{q-1})}/\mathfrak{p} = \{t + \mathfrak{p} : t \in T\}$. The *Teichmüller character* $\chi_{\mathfrak{p}}$ is a multiplicative character of $\mathbb{F}_q$ of order $q-1$ defined by

$$\chi_{\mathfrak{p}} : \mathbb{F}_q = \mathfrak{o}_{\mathbb{Q}(\zeta_{q-1})}/\mathfrak{p} \to T, \qquad t + \mathfrak{p} \mapsto t, \qquad t \in T.$$

For each $a \in \mathbb{Z}$, the *Gauss sum* of $\chi_{\mathfrak{p}}^a$ is

$$g(\chi_{\mathfrak{p}}^a) = \sum_{t \in \langle \zeta_{q-1} \rangle} \chi_{\mathfrak{p}}^a(t) \zeta_p^{\mathrm{Tr}_{q/p}(t+\mathfrak{p})} \in \mathfrak{o}_{\mathbb{Q}(\zeta_{p(q-1)})}.$$

Let $\wp$ be the unique prime of $\mathfrak{o}_{\mathbb{Q}(\zeta_{p(q-1)})}$ lying above $\mathfrak{p}$. Then $\wp$ is totally ramified over $\mathfrak{p}$ with ramification index $e(\wp \mid \mathfrak{p}) = p - 1$.

For an integer $a \ge 0$ with base p expansion $a = a_0 + a_1 p + \cdots$, $0 \le a_i \le p-1$, define $s(a) = a_0 + a_1 + \cdots$ and $\gamma(a) = a_0! a_1! \cdots$. The *Stickelberger congruence* states that for $1 \le a \le q-2$,

$$\frac{g(\chi_{\mathfrak{p}}^{-a})}{(\zeta_p - 1)^{s(a)}} \equiv \frac{-1}{\gamma(a)} \pmod{\wp}. \tag{2.1}$$

2.2. p-adic expansion of $|Z(f)|$. For $\boldsymbol{u} = (u_1, \ldots, u_m) \in \mathbb{N}^n$, let $|\boldsymbol{u}| = u_1 + \cdots + u_n$. If $\boldsymbol{x} = (x_1, \ldots, x_n)$ is an n-tuple of elements from a commutative ring, we define $\boldsymbol{x}^{\boldsymbol{u}} = x_1^{u_1} \cdots x_n^{u_n}$. Let $U_d = \{\boldsymbol{u} \in \mathbb{N}^n : |\boldsymbol{u}| \le d\}$ and consider

$$f = \sum_{\boldsymbol{u} \in U_d} a_{\boldsymbol{u}} \boldsymbol{X}^{\boldsymbol{u}} \in \mathbb{F}_q[X_1, \ldots, X_n],$$

where $\boldsymbol{X} = (X_1, \ldots, X_n)$. We write $\sum_{\boldsymbol{u}}$ and $\prod_{\boldsymbol{u}}$ for $\sum_{\boldsymbol{u} \in U_d}$ and $\prod_{\boldsymbol{u} \in U_d}$, respectively. By [A, (5′)], we have

$$q|Z(f)| = \sum_{i: U_d \to \{0, \cdots, q-1\}} \Big(\prod_{\boldsymbol{u}} \alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}\Big)\Big(\prod_{\boldsymbol{u}} c_{i(\boldsymbol{u})}\Big) \sum_{\boldsymbol{t} \in T^{n+1}} \boldsymbol{t}^{\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u})}, \tag{2.2}$$

where $\alpha_{\boldsymbol{u}} \in T$ is such that

$$a_{\boldsymbol{u}} = \alpha_{\boldsymbol{u}} + \mathfrak{p}, \tag{2.3}$$

and

$$c_i = \begin{cases} 1 & \text{if } i = 0, \\ -\dfrac{q}{q-1} & \text{if } i = q-1, \\ \dfrac{1}{q-1} g(\chi_{\mathfrak{p}}^{-i}) & \text{if } 0 < i < q-1. \end{cases} \tag{2.4}$$

By (2.1), we have $\nu_{\wp}(c_i) = s(i)$ for all $0 \le i \le q-1$. From the proof in [A, §3], we know that

$$\nu_{\wp}\Big(\Big(\prod_{\boldsymbol{u}} c_{i(\boldsymbol{u})}\Big) \sum_{\boldsymbol{t} \in T^{n+1}} \boldsymbol{t}^{\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u})}\Big) \ge m(p-1)\left\lceil \frac{n}{d} \right\rceil \tag{2.5}$$

for all $i : U_d \to \{0, \ldots, q-1\}$, where $\nu_{\wp}$ is the $\wp$-adic valuation. In fact, (2.5) implies (1.1) immediately. In what follows, we will reprove (2.5), and we will focus on those i for which equality holds in (2.5).

When $\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u}) \not\equiv (0, \ldots, 0) \pmod{q-1}$,

$$\sum_{\boldsymbol{t} \in T^{n+1}} \boldsymbol{t}^{\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u})} = 0.$$

When $\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u}) = (0, \ldots, 0)$,

$$\text{LHS of (2.5)} \ge \nu_{\wp}(q^{n+1}) = m(p-1)(n+1) > m(p-1)\left\lceil \frac{n}{d} \right\rceil.$$

Therefore, we assume that $\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u}) \equiv (0, \ldots, 0) \pmod{q-1}$ but $i \ne 0$ ($i(\boldsymbol{u}) \ne 0$ for at least one $\boldsymbol{u} \in U_d$). Let k be the number of nonzero components of $\sum_{\boldsymbol{u}} i(\boldsymbol{u})\boldsymbol{u}$. Then

$$\sum_{\boldsymbol{t} \in T^{n+1}} \boldsymbol{t}^{\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1, \boldsymbol{u})} = (q-1)^{k+1} q^{n-k}, \tag{2.6}$$

and

$$\begin{aligned}\text{LHS of (2.5) } &= \nu_{\wp}\Big(\Big(\prod_{\boldsymbol{u}} c_{i(\boldsymbol{u})}\Big)(q-1)^{k+1}q^{n-k}\Big)\\ &= \sum_{\boldsymbol{u}} s(i(\boldsymbol{u})) + m(p-1)(n-k)\\ &\ge m(p-1)\left\lceil \frac{k}{d}\right\rceil + m(p-1)(n-k) \qquad (2.7)\\ &= m(p-1)\Big(\left\lceil \frac{k}{d}\right\rceil + n-k\Big)\\ &\ge m(p-1)\left\lceil \frac{n}{d}\right\rceil. \qquad (2.8)\end{aligned}$$

In the above, inequality (2.8) is straightforward; inequality (2.7) was proved in [A] and will be explained below. First, we have

FACT 2.1. *When $d \ge 2$, equality holds in* (2.8) *if and only if either* (i) $k = n$, *or* (ii) $k = n-1$ *and* $d \mid n-1$.

Next, we determine necessary and sufficient conditions for equality to hold in (2.7). We have

$$d\sum_{\boldsymbol{u}} i(\boldsymbol{u}) \ge \sum_{\boldsymbol{u}} i(\boldsymbol{u})|\boldsymbol{u}| \ge k(q-1).$$

Since $\sum_{\boldsymbol{u}} i(\boldsymbol{u}) \equiv 0 \pmod{q-1}$, we have

$$\sum_{\boldsymbol{u}} i(\boldsymbol{u}) \ge (q-1)\left\lceil \frac{k}{d}\right\rceil. \tag{2.9}$$

For $a \in \{0,1,\ldots,q-1\}$ with base p expansion $a = a_0+a_1p+\cdots+a_{m-1}p^{m-1}$, $0 \le a_j \le p-1$, define

$$\tau(a) = a_{m-1} + a_0p + \cdots + a_{m-2}p^{m-1}.$$

Then (2.9) remains true with $i(\boldsymbol{u})$ replaced by $\tau(i(\boldsymbol{u}))$. Therefore,

$$m(q-1)\left\lceil \frac{k}{d}\right\rceil \le \sum_{h=0}^{m-1}\sum_{\boldsymbol{u}} \tau^h(i(\boldsymbol{u})) = \frac{q-1}{p-1}\sum_{\boldsymbol{u}} s(i(\boldsymbol{u})), \tag{2.10}$$

i.e.,

$$\sum_{\boldsymbol{u}} s(i(\boldsymbol{u})) \ge m(p-1)\left\lceil \frac{k}{d}\right\rceil, \tag{2.5$'$}$$

which is the same as (2.7).

FACT 2.2. *Equality holds in* (2.5′) *if and only if*

$$\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(j)} = (p-1)\left\lceil \frac{k}{d}\right\rceil \quad \textit{for all } 0 \le j \le m-1, \tag{2.11}$$

where $(i(\boldsymbol{u})^{(0)},\ldots,i(\boldsymbol{u})^{(m-1)})$ *are the base p digits of* $i(\boldsymbol{u})$.

Proof. First note that equality holds in (2.5′) if and only if

$$\sum_{\boldsymbol{u}} \tau^h(i(\boldsymbol{u})) = (q-1)\left\lceil \frac{k}{d} \right\rceil \quad \text{for all } 0 \le h \le m-1. \tag{2.12}$$

We prove that (2.11) is equivalent to (2.12).

(⇒) Assume that (2.11) holds. Then for each $0 \le h \le m-1$ we have

$$\begin{aligned}\sum_{\boldsymbol{u}} \tau^h(i(\boldsymbol{u})) &= \sum_{\boldsymbol{u}} \tau^h\Big(\sum_{j=0}^{m-1} i(\boldsymbol{u})^{(j)} p^j\Big) = \sum_{\boldsymbol{u}} \sum_{j=0}^{m-1} i(\boldsymbol{u})^{(j)} \tau^h(p^j) \\ &= \sum_{j=0}^{m-1} \Big(\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(j)}\Big) \tau^h(p^j) = (p-1)\left\lceil \frac{k}{d} \right\rceil \sum_{j=0}^{m-1} \tau^h(p^j) \\ &= (p-1)\left\lceil \frac{k}{d} \right\rceil (1+p+\cdots+p^{m-1}) = (q-1)\left\lceil \frac{k}{d} \right\rceil.\end{aligned}$$

(⇐) Assume that (2.12) holds. Since

$$\begin{aligned}\tau^h(i(\boldsymbol{u})) &= \tau\big(\tau^{h-1}(i(\boldsymbol{u}))\big) = p\tau^{h-1}(i(\boldsymbol{u})) - \big(\tau^{h-1}(i(\boldsymbol{u}))\big)^{(m-1)}(q-1) \\ &= p\tau^{h-1}(i(\boldsymbol{u})) - i(\boldsymbol{u})^{(m-h)}(q-1),\end{aligned}$$

where $m-h$ is taken modulo m, we have

$$\begin{aligned}(q-1)\left\lceil \frac{k}{d} \right\rceil &= \sum_{\boldsymbol{u}} \tau^h(i(\boldsymbol{u})) = \sum_{\boldsymbol{u}} \big(p\tau^{h-1}(i(\boldsymbol{u})) - i(\boldsymbol{u})^{(m-h)}(q-1)\big) \\ &= p(q-1)\left\lceil \frac{k}{d} \right\rceil - (q-1)\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(m-h)},\end{aligned}$$

i.e.,

$$\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(m-h)} = (p-1)\left\lceil \frac{k}{d} \right\rceil. \ \blacksquare$$

We assume that $d \ge 2$ (to avoid trivial situations).

Definition 2.3. Let $\mathcal{I}$ be the set of functions $i : U_d \to \{0,\dots,q-1\}$ such that

- each component of $\sum_{\boldsymbol{u}} i(\boldsymbol{u})\boldsymbol{u}$ is a positive multiple of $q-1$;
- $\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(j)} = (p-1)\lceil n/d \rceil$ for all $0 \le j \le m-1$.

If $d \mid n-1$, let $\mathcal{I}'$ be the set of functions $i : U_d \to \{0,\dots,q-1\}$ such that

- one of the components of $\sum_{\boldsymbol{u}} i(\boldsymbol{u})\boldsymbol{u}$ is 0 and the other components are all positive multiples of $q-1$;
- $\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(j)} = (p-1)(n-1)/d$ for all $0 \le j \le m-1$.

If $d \nmid n-1$, define $\mathcal{I}' = \emptyset$.

By Facts 2.1 and 2.2, equality holds in (2.5) if and only if $i \in \mathcal{I} \cup \mathcal{I}'$. Therefore by (2.2) and (2.6),

$$
\begin{aligned}
(2.13)\qquad & q|Z(f)| \\
&\equiv \sum_{i\in\mathcal{I}\cup\mathcal{I}'} \Big(\prod_{\boldsymbol{u}} \alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}\Big)\Big(\prod_{\boldsymbol{u}} c_{i(\boldsymbol{u})}\Big) \sum_{\boldsymbol{t}\in T^{n+1}} \boldsymbol{t}^{\sum_{\boldsymbol{u}} i(\boldsymbol{u})(1,\boldsymbol{u})} \pmod{q^{\lceil n/d\rceil}\wp} \\
&= \sum_{i\in\mathcal{I}} \Big(\prod_{\boldsymbol{u}} \alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}\Big)\Big(\prod_{\boldsymbol{u}} c_{i(\boldsymbol{u})}\Big)(q-1)^{n+1} \\
&\quad + \sum_{i\in\mathcal{I}} \Big(\prod_{\boldsymbol{u}} \alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}\Big)\Big(\prod_{\boldsymbol{u}} c_{i(\boldsymbol{u})}\Big)(q-1)^{n} q.
\end{aligned}
$$

We know that

$$
(2.14)\qquad c_{i(\boldsymbol{u})} \equiv \frac{(\zeta_p-1)^{s(i(\boldsymbol{u}))}}{\gamma(i(\boldsymbol{u}))} \pmod{(\zeta_p-1)^{s(i(\boldsymbol{u}))}\wp}.
$$

(Indeed, (2.14) is obvious when $i(\boldsymbol{u}) = 0$, and follows from (2.4) and (2.1) when $1 < i(\boldsymbol{u}) < q-1$. When $i(\boldsymbol{u}) = q-1$, (2.14) is easily verified directly.) Also note that

$$
\begin{aligned}
(2.15)\qquad p = \prod_{j=1}^{p-1}(\zeta_p^j - 1) &= (\zeta_p-1)^{p-1}\prod_{j=1}^{p-1}\frac{\zeta_p^j-1}{\zeta_p-1} \\
&\equiv (\zeta_p-1)^{p-1}(p-1)! \pmod{\zeta_p-1)^p} \\
&\equiv -(\zeta_p-1)^{p-1} \pmod{\zeta_p-1)^p}.
\end{aligned}
$$

Now combining (2.13)–(2.15) gives

$$
\begin{aligned}
(2.16)\qquad q|Z(f)| &\equiv \sum_{i\in\mathcal{I}} \Big(\prod_{\boldsymbol{u}} \alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}\Big)\frac{(\zeta_p-1)^{m(p-1)\lceil n/d\rceil}}{\prod_{\boldsymbol{u}}\gamma(i(\boldsymbol{u}))}(q-1)^{n+1} \\
&\quad + \sum_{i\in\mathcal{I}'} \Big(\prod_{\boldsymbol{u}} \alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}\Big)\frac{(\zeta_p-1)^{m(p-1)(\lceil n/d\rceil-1)}}{\prod_{\boldsymbol{u}}\gamma(i(\boldsymbol{u}))}(q-1)^{n} q \pmod{q^{\lceil n/d\rceil}\wp} \\
&\equiv q^{\lceil n/d\rceil}(-1)^{n+m\lceil n/d\rceil}\Big[-\sum_{i\in\mathcal{I}}\prod_{\boldsymbol{u}}\frac{\alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))} + (-1)^m\sum_{i\in\mathcal{I}'}\prod_{\boldsymbol{u}}\frac{\alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))}\Big] \\
&\qquad \pmod{q^{\lceil n/d\rceil}\wp}.
\end{aligned}
$$

Let

$$
(2.17)\qquad \mathcal{E}(f) = (-1)^{n+m\lceil n/d\rceil}\Big[-\sum_{i\in\mathcal{I}}\prod_{\boldsymbol{u}}\frac{\alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))} + (-1)^m\sum_{i\in\mathcal{I}'}\prod_{\boldsymbol{u}}\frac{\alpha_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))}\Big],
$$

and write (2.16) as

$$
(2.18)\qquad |Z(f)| \equiv q^{\lceil n/d\rceil-1}\mathcal{E}(f) \pmod{q^{\lceil n/d\rceil-1}\wp}.
$$

Since $\mathcal{E}(f) \in \mathbb{Q}(\zeta_{q-1})$, (2.18) gives

$$|Z(f)| \equiv q^{\lceil n/d \rceil - 1} \mathcal{E}(f) \pmod{q^{\lceil n/d \rceil - 1} p}. \tag{2.19}$$

Since $|Z(f)| \in \mathbb{Z}$, there exists $N \in \mathbb{Z}$ such that

$$\mathcal{E}(f) \equiv N \pmod{p}. \tag{2.20}$$

Taking the images of both sides of (2.20) in $\mathfrak{o}_{\mathbb{Q}(\zeta_{q-1})}/\mathfrak{p} = \mathbb{F}_q$, we have

$$E(f) = N \quad (\text{in } \mathbb{F}_q), \tag{2.21}$$

where

$$E(f) = (-1)^{n+m\lceil n/d \rceil} \Big[-\sum_{i \in \mathcal{I}} \prod_{\boldsymbol{u}} \frac{a_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))} + (-1)^m \sum_{i \in \mathcal{I}'} \prod_{\boldsymbol{u}} \frac{a_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))} \Big]. \tag{2.22}$$

In fact, $E(f) \in \mathbb{F}_p$ because of (2.21).

To summarize, we have the following theorem.

Theorem 2.4. *Let $n \geq 1$, $d \geq 2$, and*

$$f = \sum_{\boldsymbol{u} \in U_d} a_{\boldsymbol{u}} \boldsymbol{X}^{\boldsymbol{u}} \in \mathbb{F}_q[X_1, \ldots, X_n],$$

where $\boldsymbol{X} = (X_1, \ldots, X_n)$. We have

$$|Z(f)| \equiv q^{\lceil n/d \rceil - 1} E(f) \pmod{q^{\lceil n/d \rceil - 1} p}, \tag{2.23}$$

where $E(f)$ is given in (2.22). In particular, $\nu_p(|Z(f)|) \geq m(\lceil n/d \rceil - 1) + 1$ if and only if $E(f) = 0$.

Remark 2.5. $E(f)$ is a homogeneous polynomial of degree $(q-1)\lceil n/d \rceil$ over $\mathbb{F}_p$ in the coefficients of f. In general, this expression is not explicit because $\mathcal{I}$ and $\mathcal{I}'$ are not. In the next section, we explore several special cases where $E(f)$ can be made explicit.

3. Applications to Reed–Muller codes

3.1. Reed–Muller codes. For a prime power $q = p^m$ and integers n, d with $n > 0$ and $0 \leq d \leq n(q-1)$, the q-ary Reed–Muller code $R_q(d, n)$ is defined as

$$R_q(d, n) = \{ f \in \mathbb{F}_q[X_1, \ldots, X_n] : \deg f \leq d,\ \deg_{X_j} f \leq q - 1,\ 1 \leq j \leq n \}. \tag{3.1}$$

(For convenience, we define $R_q(-1, n) = \{0\}$.) It is known [DK, Result 1] that

$$\dim_{\mathbb{F}_q} R_q(d, n) = \sum_{j \leq \lfloor d/q \rfloor} (-1)^j \binom{n}{j} \binom{d - qj + n}{n}. \tag{3.2}$$

For each $f \in R_q(d,n)$, its (*Hamming*) *weight* is $|f| = q^n - |Z(f)|$. The weight enumerator of $R_q(d,n)$ is not known except in the following special cases:

(i) $d \le 2$ or $d \ge n(q-1)-3$. (For $d=2$ and $q=2$, see [MS, Ch. 15, §2]; for $d=2$ and q general, use the well known classification of quadratic forms over $\mathbb{F}_q$. For $d \ge n(q-1)-3$, note that the dual of $R_q(d,n)$ is $R_q(d',n)$, where $d' = n(q-1)-1-d \le 2$.)
(ii) $q=2$ and $n \le 8$ [KTA, SITK].
(iii) $q=2$, $n=9$, $d=3$ [SKF].

For $t \ge 0$, let

$$N_q(d,n;t) = \bigl|\{f \in R_q(d,n) : \nu_p(|f|) \ge t\}\bigr|.$$

Ax's theorem implies that $N_q(d,n;t) = |R_q(d,n)|$ for $t \le m(\lceil n/d\rceil - 1)$. We will use Theorem 2.4 to determine $N_q(d,n;t)$ with $t = m(\lceil n/d\rceil - 1)+1$ in several cases; such formulas provide new information concerning the weight enumerators of the Reed–Muller codes involved. The cases we consider share a common assumption that $(p-1)\lceil n/d\rceil = 2$, that is, $p=2$ and $\lceil n/d\rceil = 2$, or $p=3$ and $\lceil n/d\rceil = 1$. Under this assumption, for each $i \in \mathcal{I}$ (Definition 2.3),

$$\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(j)} = 2 \quad \text{for all } 0 \le j \le m-1. \tag{3.3}$$

3.2. The case $q = 2^m$ and $d = n/2$. Assume that $q = 2^m$, $n \ge 4$ is even, and $d = n/2$. Let $f = \sum_{\boldsymbol{u}\in U_{n/2}} a_{\boldsymbol{u}} \boldsymbol{X}^{\boldsymbol{u}} \in \mathbb{F}_q[X_1,\dots,X_n]$. Since $d \nmid n-1$, $\mathcal{I}' = \emptyset$ in Definition 2.3. Hence

$$E(f) = (-1)^{n+1} \sum_{i\in\mathcal{I}} \prod_{\boldsymbol{u}} \frac{a_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))}. \tag{3.4}$$

If $i \in \mathcal{I}$, then

$$\sum_{\boldsymbol{u}\in U_d} i(\boldsymbol{u}) = \sum_{\boldsymbol{u}} \sum_{j=0}^{m-1} i(\boldsymbol{u})^{(j)} 2^j = 2\sum_{j=0}^{m-1} 2^j = 2(q-1).$$

Since

$$n(q-1) \le \sum_{\boldsymbol{u}\in U_{n/2}} i(\boldsymbol{u})|\boldsymbol{u}| \le \frac{n}{2} \sum_{\boldsymbol{u}\in U_{n/2}} i(\boldsymbol{u}) = n(q-1),$$

we have $|\boldsymbol{u}| = n/2$ for all $\boldsymbol{u} \in U_{n/2}$ with $i(\boldsymbol{u}) > 0$ and we have

$$\sum_{|\boldsymbol{u}|=n/2} i(\boldsymbol{u})\boldsymbol{u} = (q-1,\dots,q-1). \tag{3.5}$$

LEMMA 3.1. *$i \in \mathcal{I}$ if and only if there exist $\boldsymbol{u}_j, \boldsymbol{v}_j \in \{0,1\}^n$, $0 \le j \le m-1$, with $|\boldsymbol{u}_j| = |\boldsymbol{v}_j| = n/2$, $\boldsymbol{u}_j + \boldsymbol{v}_j = (1,\ldots,1)$, such that for all $0 \le j \le m-1$,*

$$\begin{cases} i(\boldsymbol{u}_j)^{(j)} = i(\boldsymbol{v}_j)^{(j)} = 1, \\ i(\boldsymbol{u})^{(j)} = 0 \quad \text{if } \boldsymbol{u} \in U_{n/2} \setminus \{\boldsymbol{u}_j, \boldsymbol{v}_j\}. \end{cases} \tag{3.6}$$

Proof. $(\Rightarrow)$ By Definition 2.3,

$$\sum_{|\boldsymbol{u}|=n/2} i(\boldsymbol{u})^{(j)} = 2 \quad \text{for all } 0 \le j \le m-1. \tag{3.7}$$

Choose $\boldsymbol{u}_{m-1}, \boldsymbol{v}_{m-1} \in U_{n/2}$ with $|\boldsymbol{u}_{m-1}| = |\boldsymbol{v}_{m-1}| = n/2$ and $i(\boldsymbol{u}_{m-1})^{(m-1)} = i(\boldsymbol{v}_{m-1})^{(m-1)} = 1$. Since

$$\begin{aligned}(2^m - 1)(1,\ldots,1) = \sum_{|\boldsymbol{u}|=n/2} i(\boldsymbol{u})\boldsymbol{u} &\ge i(\boldsymbol{u}_{m-1})\boldsymbol{u}_{m-1} + i(\boldsymbol{v}_{m-1})\boldsymbol{v}_{m-1} \\ &\ge 2^{m-1}(\boldsymbol{u}_{m-1} + \boldsymbol{v}_{m-1}),\end{aligned}$$

it follows that $\boldsymbol{u}_{m-1} + \boldsymbol{v}_{m-1} \le (1,\ldots,1)$, that is, $\boldsymbol{u}_{m-1}, \boldsymbol{v}_{m-1} \in \{0,1\}^n$ and $\boldsymbol{u}_{m-1} + \boldsymbol{v}_{m-1} = (1,\ldots,1)$. For any $\boldsymbol{u} \in U_{n/2}$ with $|\boldsymbol{u}| = n/2$ and $\boldsymbol{u} \ne \boldsymbol{u}_{m-1}, \boldsymbol{v}_{m-1}$, we have $i(\boldsymbol{u})^{(m-1)} = 0$ by (3.7).

Now

$$\begin{aligned}\sum_{|\boldsymbol{u}|=n/2} \sum_{j=0}^{m-2} i(\boldsymbol{u})^{(j)} 2^j \boldsymbol{u} &= (2^m - 1)(1,\ldots,1) - 2^{m-1}(1,\ldots,1) \\ &= (2^{m-1} - 1)(1,\ldots,1).\end{aligned}$$

By the same argument, there exist $\boldsymbol{u}_{m-2}, \boldsymbol{v}_{m-2} \in \{0,1\}^n$ with $|\boldsymbol{u}_{m-2}| = |\boldsymbol{v}_{m-2}| = n/2$ and $\boldsymbol{u}_{m-2} + \boldsymbol{v}_{m-2} = (1,\ldots,1)$ such that $i(\boldsymbol{u}_{m-2})^{(m-2)} = i(\boldsymbol{v}_{m-2})^{(m-2)} = 1$ and $i(\boldsymbol{u})^{(m-2)} = 0$ for all $\boldsymbol{u}$ with $|\boldsymbol{u}| = n/2$ and $\boldsymbol{u} \ne \boldsymbol{u}_{m-2}, \boldsymbol{v}_{m-2}$. Continuing this way, we get $\boldsymbol{u}_j, \boldsymbol{v}_j$, $0 \le j \le m-1$, with the desired property.

$(\Leftarrow)$ For each $0 \le j \le m-1$,

$$\sum_{\boldsymbol{u}} i(\boldsymbol{u})^{(j)} = i(\boldsymbol{u}_j)^{(j)} + i(\boldsymbol{v}_j)^{(j)} = 2 = (p-1)\lceil n/d \rceil.$$

Also,

$$\begin{aligned}\sum_{\boldsymbol{u}} i(\boldsymbol{u})\boldsymbol{u} &= \sum_{\boldsymbol{u}} \Big(\sum_{j=0}^{m-1} i(\boldsymbol{u})^{(j)} 2^j\Big)\boldsymbol{u} = \sum_{j=0}^{m-1} 2^j(\boldsymbol{u}_j + \boldsymbol{v}_j) \\ &= \Big(\sum_{j=0}^{m-1} 2^j\Big)(1,\ldots,1) = (q-1)(1,\ldots,1).\end{aligned}$$

Hence $i \in \mathcal{I}$. ∎

It follows from Lemma 3.1 that

(3.8)

$$\sum_{i\in\mathcal{I}}\prod_{\boldsymbol{u}} a_{\boldsymbol{u}}^{i(\boldsymbol{u})} = \sum_{\substack{\{\boldsymbol{u}_0,\boldsymbol{v}_0\},\dots,\{\boldsymbol{u}_{m-1},\boldsymbol{v}_{m-1}\}\\ \boldsymbol{u}_j,\boldsymbol{v}_j\in\{0,1\}^n,\,|\boldsymbol{u}_j|=|\boldsymbol{v}_j|=n/2\\ \boldsymbol{u}_j+\boldsymbol{v}_j=(1,\dots,1)}} a_{\boldsymbol{u}_0}a_{\boldsymbol{v}_0}(a_{\boldsymbol{u}_1}a_{\boldsymbol{v}_1})^2\cdots(a_{\boldsymbol{u}_{m-1}}a_{\boldsymbol{v}_{m-1}})^{2^{m-1}}$$

$$= \Big(\sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\}\\ \boldsymbol{u},\boldsymbol{v}\in\{0,1\}^n,\,|\boldsymbol{u}|=|\boldsymbol{v}|=n/2\\ \boldsymbol{u}+\boldsymbol{v}=(1,\dots,1)}} a_{\boldsymbol{u}}a_{\boldsymbol{v}}\Big)^{1+2+\dots+2^{m-1}}.$$

Combining Theorem 2.4, (3.4) and (3.8) gives the following corollary.

Corollary 3.2. *Let $q=2^m$ and $n\ge 4$ be even. Let*

$$f=\sum_{\boldsymbol{u}\in U_{n/2}} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}}\in\mathbb{F}_q[X_1,\dots,X_n].$$

Then $v_2(|Z(f)|)\ge m+1$ if and only if

$$\sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\}\\ \boldsymbol{u},\boldsymbol{v}\in\{0,1\}^n,\,|\boldsymbol{u}|=|\boldsymbol{v}|=n/2\\ \boldsymbol{u}+\boldsymbol{v}=(1,\dots,1)}} a_{\boldsymbol{u}}a_{\boldsymbol{v}}=0. \tag{3.9}$$

Replacing each $a_{\boldsymbol{u}}$ in (3.9) by an indeterminate $Y_{\boldsymbol{u}}$, we obtain a quadratic form

$$Q=\sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\}\\ \boldsymbol{u},\boldsymbol{v}\in\{0,1\}^n,\,|\boldsymbol{u}|=|\boldsymbol{v}|=n/2\\ \boldsymbol{u}+\boldsymbol{v}=(1,\dots,1)}} Y_{\boldsymbol{u}}Y_{\boldsymbol{v}}$$

in $N=\binom{n}{n/2}$ indeterminates over $\mathbb{F}_q$. Order the indeterminates in a row $\boldsymbol{Y}=(Y_{\boldsymbol{u}}:\boldsymbol{u}\in\{0,1\}^n,\ |\boldsymbol{u}|=n/2)$ such that the indices $\boldsymbol{u}$ and $\boldsymbol{u}^c:=(1,\dots,1)-\boldsymbol{u}$ appear in positions symmetric with respect to the center of the row. Then

$$Q=\boldsymbol{Y}A\boldsymbol{Y}^t,$$

where

$$A=\begin{bmatrix}0 & \Delta_{N/2}\\ 0 & 0\end{bmatrix}_{N\times N}$$

and $\Delta_{N/2}$ is defined in (1.4). By [LN, Theorem 6.32], the number of roots of Q in $\mathbb{F}_q^N$ is

$$q^{N-1}+(q-1)q^{\frac{1}{2}N-1}. \tag{3.10}$$

Corollary 3.3. *Let $q=2^m$ and $n\ge 4$ be even. Then*

$$N_q(n/2,n;\, m+1) = \Big(q^{\binom{n}{n/2}-1}+(q-1)q^{\frac12\binom{n}{n/2}-1}\Big)q^{\dim_{\mathbb{F}_q} R_q(n/2,n)-\binom{n}{n/2}}, \tag{3.11}$$

where

$$\dim_{\mathbb{F}_q} R_q(n/2,n) = \sum_{j\le\lfloor n/2q\rfloor}(-1)^j\binom{n}{j}\binom{3n/2-qj}{n}. \tag{3.12}$$

Proof. (3.11) follows from Corollary 3.2 and (3.10), while (3.12) follows from (3.2). ■

In the remaining three subsections, arguments and computations are similar to those in Subsection 3.2. Therefore, a fair amount of details is omitted.

3.3. The case $q=2$ and $n/2\le d\le n-2$. Assume that $q=2$, $n\ge 4$, and $n/2\le d\le n-2$. Let $f=\sum_{\boldsymbol{u}\in U_d} a_{\boldsymbol{u}}\boldsymbol{X}^{\boldsymbol{u}}\in\mathbb{F}_2[X_1,\dots,X_n]$. Then $\mathcal{I}'=\emptyset$ and

$$E(f)=(-1)^{n+1}\sum_{i\in\mathcal{I}}\prod_{\boldsymbol{u}}\frac{a_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))}.$$

Moreover, $i\in\mathcal{I}$ if and only if there exist $\boldsymbol{u}_0,\boldsymbol{v}_0\in U_d\cap\{0,1\}^n$ with $\boldsymbol{u}+\boldsymbol{v}=(1,\dots,1)$ such that

$$i(\boldsymbol{u}_0)=i(\boldsymbol{v}_0)=1,\qquad i(\boldsymbol{u})=0 \text{ for all } \boldsymbol{u}\in U_d\setminus\{\boldsymbol{u}_0,\boldsymbol{v}_0\}.$$

Consequently,

$$\sum_{i\in\mathcal{I}}\prod_{\boldsymbol{u}}\frac{a_{\boldsymbol{u}}^{i(\boldsymbol{u})}}{\gamma(i(\boldsymbol{u}))}=\sum_{\substack{\{\boldsymbol{u}_0,\boldsymbol{v}_0\}\\ \boldsymbol{u}_0,\boldsymbol{v}_0\in\{0,1\}^n,\ |\boldsymbol{u}_0|,|\boldsymbol{v}_0|\in[n-d,d]\\ \boldsymbol{u}_0+\boldsymbol{v}_0\ge(1,\dots,1)}} a_{\boldsymbol{u}_0}a_{\boldsymbol{v}_0}.$$

Thus $\nu_2(|Z(f)|)\ge 2$ if and only if $(a_{\boldsymbol{u}}:\boldsymbol{u}\in\{0,1\}^n,\ |\boldsymbol{u}|\in[n-d,d])$ is a root of the quadratic form

$$Q=\sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\}\\ \boldsymbol{u},\boldsymbol{v}\in\{0,1\}^n,\ |\boldsymbol{u}|,|\boldsymbol{v}|\in[n-d,d]\\ \boldsymbol{u}+\boldsymbol{v}\ge(1,\dots,1)}} Y_{\boldsymbol{u}}Y_{\boldsymbol{v}}.$$

Order the indeterminates of Q in a row $\boldsymbol{Y}=(Y_{\boldsymbol{u}}:\boldsymbol{u}\in\{0,1\}^n,\ |\boldsymbol{u}|\in[n-d,d])$ in such a way that $|\boldsymbol{u}|$ is increasing and the indices $\boldsymbol{u}$ and $\boldsymbol{u}^c:=(1,\dots,1)-\boldsymbol{u}$ appear in positions symmetric with respect to the center of the row. Then

$$Q = \boldsymbol{Y} A \boldsymbol{Y}^T,$$

where

$$A = \begin{bmatrix} & & & & & & 1 \\ & & & & & \cdot & * \\ & & & & \cdot & \cdot & \cdot \\ & & & \cdot & \cdot & & \cdot \\ & & 1 & * & \cdot & \cdot & * \\ & & * & * & \cdot & \cdot & * \\ & & & \cdot & \cdot & & \cdot \\ & & & & \cdot & \cdot & \cdot \\ & & & & & \cdot & * \\ & & & & & & * \end{bmatrix}_{N\times N}, \qquad N = \sum_{j=n-d}^{d} \binom{n}{j}.$$

(The unmarked entries of A are all 0.) There exists $P \in \mathrm{GL}(N, \mathbb{F}_2)$ such that

$$PAP^T = \begin{bmatrix} 0 & \Delta_{N/2} \\ 0 & 0 \end{bmatrix}.$$

Therefore the number of roots of Q in $\mathbb{F}_2^N$ is $2^{N-1} + 2^{\frac{1}{2}N-1}$ [LN, Theorem 6.32].

COROLLARY 3.4. *For $n \geq 4$ and $n/2 \leq d \leq n-2$,*

$$N_2(d, n; 2) = 2^{\binom{n}{0}+\cdots+\binom{n}{d}-1} + 2^{2^{n-1}-1}.$$

3.4. The case $q = 3^m$ and $d = n$. Assume that $q = 3^m$, $n \geq 2$, and $d = n$. Let $f = \sum_{\boldsymbol{u}\in U_n} a_{\boldsymbol{u}} \boldsymbol{X}^{\boldsymbol{u}} \in \mathbb{F}_q[X_1, \ldots, X_n]$. Then $\mathcal{I}' = \emptyset$. Moreover, $i \in \mathcal{I}$ if and only if there exist $\boldsymbol{u}_j, \boldsymbol{v}_j \in \{0, 1, 2\}^n$, $0 \leq j \leq m-1$, with $|\boldsymbol{u}_j| = |\boldsymbol{v}_j| = n$ and $\boldsymbol{u}_j + \boldsymbol{v}_j = (2, \ldots, 2)$ such that for all $0 \leq j \leq m-1$,

$$\begin{cases} i(\boldsymbol{u}_j)^{(j)} = i(\boldsymbol{v}_j)^{(j)} = 1 & \text{if } \boldsymbol{u}_j \neq \boldsymbol{v}_j, \\ i(\boldsymbol{u}_j)^{(j)} = 2 & \text{if } \boldsymbol{u}_j = \boldsymbol{v}_j, \\ i(\boldsymbol{u})^{(j)} = 0 & \text{if } \boldsymbol{u} \in U_n \setminus \{\boldsymbol{u}_j, \boldsymbol{v}_j\}. \end{cases}$$

We have

$$E(f) = (-1)^{n+m+1} \Bigg(\sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\} \\ \boldsymbol{u},\boldsymbol{v}\in\{0,1,2\},\, |\boldsymbol{u}|=|\boldsymbol{v}|=n \\ \boldsymbol{u}+\boldsymbol{v}=(2,\ldots,2)}} a_{\boldsymbol{u}} a_{\boldsymbol{v}} \Bigg)^{1+3+\cdots+3^{m-1}}.$$

Thus $\nu_3(|Z(f)|) \geq 1$ if and only if $(a_{\boldsymbol{u}} : \boldsymbol{u} \in \{0,1,2\}^n,\ |\boldsymbol{u}| = n)$ is a root of the quadratic form

$$Q = \sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\} \\ \boldsymbol{u},\boldsymbol{v}\in\{0,1,2\},\,|\boldsymbol{u}|=|\boldsymbol{v}|=n \\ \boldsymbol{u}+\boldsymbol{v}=(2,\dots,2)}} Y_{\boldsymbol{u}} Y_{\boldsymbol{v}}.$$

Order the indeterminates of Q in a row $\boldsymbol{Y} = (Y_{\boldsymbol{u}} : \boldsymbol{u} \in \{0,1,2\}^n,\ |\boldsymbol{u}| = n)$ such that the indices $\boldsymbol{u}$ and $\boldsymbol{u}^c := (2,\dots,2) - \boldsymbol{u}$ appear in positions symmetric with respect to the center of the row. Then

$$Q = \boldsymbol{Y} A \boldsymbol{Y}^T,$$

where

$$A = \begin{bmatrix} 0 & \Delta_{(N+1)/2} \\ 0 & 0 \end{bmatrix}_{N\times N}, \qquad N = \sum_{j\leq n/2} \binom{n}{j}\binom{n-j}{n-2j}.$$

The number of roots of Q in $\mathbb{F}_q^N$ is q^{N-1} [LN, Theorem 6.27].

Corollary 3.5. *Let $q = 3^m$ and $n \geq 2$. Then*

$$N_q(n,n;1) = q^{\dim_{\mathbb{F}_q} R_q(n,n)-1},$$

where

$$\dim_{\mathbb{F}_q} R_q(n,n) = \sum_{j\leq\lfloor n/q\rfloor} (-1)^j \binom{n}{j}\binom{2n-qj}{n}.$$

3.5. The case $q = 3$ and $n \leq d \leq 2n$. Assume that $q = 3$, $n \geq 2$, and $n \leq d \leq 2n$. Let $f = \sum_{\boldsymbol{u}\in U_d} a_{\boldsymbol{u}} \boldsymbol{X}^{\boldsymbol{u}} \in \mathbb{F}_q[X_1,\dots,X_n]$. Then $\mathcal{I}' = \emptyset$. Moreover, $i \in \mathcal{I}$ if and only if there exist $\boldsymbol{u}_0, \boldsymbol{v}_0 \in \{0,1,2\}^n$ with $\boldsymbol{u}_0 \equiv \boldsymbol{v}_0 \pmod 2$ and $\boldsymbol{u}_0 + \boldsymbol{v}_0 \geq (2,\dots,2)$ such that

$$\begin{cases} i(\boldsymbol{u}_0) = i(\boldsymbol{v}_0) = 1 & \text{if } \boldsymbol{u}_0 \neq \boldsymbol{v}_0, \\ i(\boldsymbol{u}_0) = 2 & \text{if } \boldsymbol{u}_0 = \boldsymbol{v}_0, \\ i(\boldsymbol{u}) = 0 & \text{if } \boldsymbol{u} \in U_d \setminus \{\boldsymbol{u}_0, \boldsymbol{v}_0\}. \end{cases}$$

We have

$$E(f) = (-1)^{n+m+1} \sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\} \\ \boldsymbol{u},\boldsymbol{v}\in\{0,1,2\}^n,\,|\boldsymbol{u}|,|\boldsymbol{v}|\in[2n-d,d] \\ \boldsymbol{u}\equiv\boldsymbol{v}\,(\mathrm{mod}\,2),\,\boldsymbol{u}+\boldsymbol{v}\geq(2,\dots,2)}} a_{\boldsymbol{u}} a_{\boldsymbol{v}}.$$

Thus $\nu_3(|Z(f)|) \geq 1$ if and only if $(a_{\boldsymbol{u}} : \boldsymbol{u} \in \{0,1,2\}^n,\ |\boldsymbol{u}| \in [2n-d,d])$ is a root of the quadratic form

$$Q = \sum_{\substack{\{\boldsymbol{u},\boldsymbol{v}\} \\ \boldsymbol{u},\boldsymbol{v}\in\{0,1,2\}^n,\,|\boldsymbol{u}|,|\boldsymbol{v}|\in[2n-d,d] \\ \boldsymbol{u}\equiv\boldsymbol{v}\,(\mathrm{mod}\,2),\,\boldsymbol{u}+\boldsymbol{v}\geq(2,\dots,2)}} Y_{\boldsymbol{u}} Y_{\boldsymbol{v}}.$$

Order the indeterminates of Q in a row $\boldsymbol{Y} = (Y_{\boldsymbol{u}} : \boldsymbol{u} \in \{0,1,2\}^n,\ |\boldsymbol{u}| \in [2n-d, d])$ in such a way that $|\boldsymbol{u}|$ is increasing and the indices $\boldsymbol{u}$ and $\boldsymbol{u}^c := (2,\dots,2) - \boldsymbol{u}$ appear in positions symmetric with respect to the center of the row. Then

$$Q = \boldsymbol{Y} A \boldsymbol{Y}^T,$$

where

$$A = \begin{bmatrix} & & & & & & 1 \\ & & & & & \cdot & * \\ & & & & \cdot & \cdot & \cdot \\ & & & \cdot & \cdot & & \cdot \\ & & 1 & * & \cdot & \cdot & * \\ & & & * & \cdot & \cdot & * \\ & & & & \cdot & \cdot & \cdot \\ & & & & & \cdot & \cdot \\ & & & & & & * \end{bmatrix}_{N\times N},$$

$$N = \sum_{j=2n-d}^{d} \bigl|\bigl\{\boldsymbol{u} \in \{0,1,2\}^n : |\boldsymbol{u}| = j\bigr\}\bigr|.$$

There exists $P \in \mathrm{GL}(N, \mathbb{F}_3)$ such that

$$PAP^T = \begin{bmatrix} 0 & \varDelta_{(N+1)/2} \\ 0 & 0 \end{bmatrix}.$$

Hence the number of roots of Q in $\mathbb{F}_3^N$ is 3^{N-1} [LN, Theorem 6.27].

Corollary 3.6. *Let $n \ge 2$ and $n \le d \le 2n$. Then*

$$N_3(d, n; 1) = 3^{\dim_{\mathbb{F}_3} R_3(d,n) - 1},$$

where

$$\dim_{\mathbb{F}_3} R_3(d,n) = \sum_{j \le \lfloor d/3 \rfloor} (-1)^j \binom{n}{j} \binom{d-3j+n}{n}.$$

References

[A] J. Ax, *Zeroes of polynomials over finite fields*, Amer. J. Math. 86 (1964), 255–261.

[C] W. Cao, *A partial improvement of the Ax–Katz theorem*, J. Number Theory 132 (2012), 485–494.

[CS] W. Cao and Q. Sun, *Improvements upon the Chevalley–Warning–Ax–Katz-type estimates*, J. Number Theory 122 (2007), 135–141.

[Ch] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg 11 (1935), 73–75.

[DM] P. Delsarte and R. J. McEliece, *Zeros of functions in finite abelian group algebras*, Amer. J. Math. 98 (1976), 197–224.

[DK] P. Ding and J. D. Key, *Minimum-weight codewords as generators of generalized Reed–Muller codes*, IEEE Trans. Inform. Theory 46 (2000), 2152–2158.

[H] X. Hou, *A note on the proof of a theorem of Katz*, Finite Fields Appl. 11 (2005), 316–319.

[KTA] T. Kasami, N. Tokura and S. Azumi, *On the weight enumeration of weights less than* $2.5d$ *of Reed–Muller codes*, Inform. Control 30 (1976), 380–395.

[K] D. J. Katz, *On theorems of Delsarte–McEliece and Chevalley–Warning–Ax–Katz*, Des. Codes Cryptogr. 65 (2012), 291–324.

[Ka] N. M. Katz, *On a theorem of Ax*, Amer. J. Math. 93 (1971), 485–499.

[L] S. Lang, *Algebraic Number Theory*, 2nd ed., Springer, New York, 1994.

[LN] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Cambridge Univ. Press, Cambridge, 1997.

[MS] F. J. MacWilliams and N. J. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam, 1977.

[MM] O. Moreno and C. J. Moreno, *Improvements of the Chevalley–Warning and the Ax–Katz theorems*, Amer. J. Math. 117 (1995), 241–244.

[SITK] M. Sugino, Y. Ienaga, N. Tokura and T. Kasami, *Weight distribution of* $(128, 64)$ *Reed–Muller code*, IEEE Trans. Inform. Theory 17 (1971), 627–628.

[SKF] T. Sugita, T. Kasami and T. Fujiwara, *The weight distribution of the third-order Reed–Muller code of length* 512, IEEE Trans. Inform. Theory 42 (1996), 1622–1625.

[S] Z. W. Sun, *Extensions of Wilson's lemma and the Ax–Katz theorem*, arXiv:math/0608560.

[W1] D. Wan, *An elementary proof of a theorem of Katz*, Amer. J. Math. 111 (1989), 1–8.

[W2] D. Wan, *A Chevalley–Warning approach to p-adic estimates of character sums*, Proc. Amer. Math. Soc. 123 (1995), 45–54.

[Wa] H. N. Ward, *Weight polarization and divisibility*, Discrete Math. 83 (1990), 315–326.

[War] E. Warning, *Bermerkung zur vorstehenden Arbeit von Herrn Chevalley*, Abh. Math. Sem. Univ. Hamburg 11 (1935), 76–83.

[Wi] R. M. Wilson, *A lemma on polynomials modulo* p^m *and applications to coding theory*, Discrete Math. 306 (2006), 3154–3165.

Xiang-dong Hou
Department of Mathematics and Statistics
University of South Florida
Tampa, FL 33620, U.S.A.
E-mail: xhou@usf.edu