Bull. Korean Math. Soc. **37** (2000), No. 4, pp. 803–810

COUNTING FORMULA FOR SOLUTIONS OF DIAGONAL EQUATIONS

YOUNGGU MOON, JUNE BOK LEE, AND YOUNG HO PARK

ABSTRACT. Let $N(d_1,\dots,d_n;c_1,\dots,c_n)$ be the number of solutions $(x_1,\dots,x_n)\in\mathbb{F}_q^n$ of the diagonal equation

$$c_1{x_1}^{d_1}+c_2{x_2}^{d_2}+\cdots+c_n{x_n}^{d_n}=0 \quad n\geq 2,\ c_j\in\mathbb{F}_q^*,\ \ j=1,2,\dots,n$$

where $d_j>1$ and $d_j \mid q-1$ for all $j=1,2,\dots,n$. In this paper, we find all n-tuples $(d_1,\dots,d_n)$ such that the reduced form of $(d_1,\dots,d_n)$ and $N(d_1,\dots,d_n;c_1,\dots,c_n)$ are the same as in the theorem obtained by Sun Qi [3]. Improving this, we also get an explicit formula for the number of solutions of the diagonal equation, under a certain natural restriction on the exponents.

Let $\mathbb{F}_q$ be the finite field of q elements, where $q=p^f,\ f\geq 1$, and p is an odd prime. A diagonal equation over $\mathbb{F}_q$ is of the form

(1)
$$a_1{x_1}^{d_1}+a_2{x_2}^{d_2}+\cdots+a_n{x_n}^{d_n}=b \quad n\geq 2,\ a_j\in\mathbb{F}_q^*,\ j=1,2,\dots,n,\ b\in\mathbb{F}_q.$$

It is well known[5] that the number of solutions of (1) can be obtained by the number of solutions of the equations of the form

$$(2)\quad c_1{x_1}^{d_1}+c_2{x_2}^{d_2}+\cdots+c_n{x_n}^{d_n}=0 \quad n\geq 2,\ c_j\in\mathbb{F}_q^*,\ j=1,2,\dots,n,$$

where $d_j>1$ and $d_j \mid q-1$ for all $j=1,2,\dots,n$.

The number $N(d_1,\dots,d_n;c_1,\dots,c_n)$ of solutions $(x_1,\dots,x_n)\in\mathbb{F}_q^n$ of the equation (2) is given [2] by

Received March 17, 2000.
2000 Mathematics Subject Classification: 11D41, 11D61, 11D85.
Key words and phrases: diagonal equations, finite fields.
This work is supported by Project Number 1998-015-D00015.

(3)

$$N(d_1,\dots,d_n;c_1,\dots,c_n)$$
$$= q^{n-1} + \sum_{\substack{y_1/d_1+\cdots+y_n/d_n\equiv 0 \pmod 1 \\ 1\le y_j\le d_j-1,\ j=1,\dots,n}} \bar{\lambda}_1^{y_1}(c_1)\cdots\bar{\lambda}_n^{y_n}(c_n)J_0(\lambda_1{}^{y_1},\dots,\lambda_n{}^{y_n})$$

where $\lambda_j(a) = e^{2\pi i \mathrm{ind}a/d_j}$ is a multiplicative character of order d_j on $\mathbb{F}_q$, $\bar{\lambda}_j$ is the conjugate of λ_j, $a \in \mathbb{F}_q^*$, $j = 1,\dots,n$. $J_0(\lambda_1,\dots,\lambda_n)$ is the Jacobi sum over $\mathbb{F}_q$, that is,

$$J_0(\lambda_1,\dots,\lambda_n) = \sum_{\substack{a_1+\cdots+a_n=0 \\ a_j\in\mathbb{F}_q}} \lambda_1(a_1)\cdots\lambda_n(a_n).$$

Thus, it is necessary to find the solutions to the following equation.

$$(4) \qquad \frac{y_1}{d_1}+\cdots+\frac{y_n}{d_n} \equiv 0 \pmod 1, \quad 1 \le y_j \le d_j - 1,\ j = 1,\dots,n.$$

But, Granville, Shuguang Li, and Sun Qi [1] proved that

$$(5) \qquad N(d_1,\dots,d_n;c_1,\dots,c_n) = N(w_1,\dots,w_n;c_1,\dots,c_n),$$

where $w_j = \Big(d_j, \mathrm{lcm}[d_i : i \ne j]\Big)$, $j = 1,\dots,n$.

In order to obtain an explicit formula for the equation (3), we will use the above reduction theorem before considering the equation (4).

DEFINITION. Let $w_j = (d_j, \mathrm{lcm}[d_i : i \ne j])$, $d_j \mid q-1$, $d_j \in \mathbb{N}$ for $j = 1, \dots, n$. We call $(w_1,\dots,w_n)$ the **reduced form** of $(d_1,\dots,d_n)$ and denote $(w_1,\dots,w_n) = (d_1,\dots,d_n)_R$. If $w_j = d_j$ for all j, then $(d_1,\dots,d_n)$ is said to be **reduced**.

REMARK 1. A reduced form is reduced (See [1], Theorem 1. (ii)).

THEOREM 1. *The reduced form* $(d_1, \dots, d_n)_R$ *of* $(d_1, \dots, d_n)$ *is either* $(\overbrace{2, \dots, 2}^{n-2}, k, k)$ *or* $(\overbrace{2, \dots, 2}^{n-2}, k, 2k)$ *if and only if*

$$(6) \qquad (d_1, \dots, d_n) = (2^t m_1, 2m_2, \dots, 2m_{n-2}, km_{n-1}, km_n),$$

where $t \geq 1$; $(m_j, k) = 1$, $j = 1, 2, \dots, n-2$; $(m_i, m_j) = 1$, $1 \leq i < j \leq n$, m_j *is odd for* $j = 1, 2, \dots, n-1$ *and when* $t \geq 2$, $4 \nmid km_n$.

Proof. Suppose that $(w_1, \dots, w_n) = (d_1, \dots, d_n)_R$ is either $(\overbrace{2, \dots, 2}^{n-2}, k, k)$ or $(\overbrace{2, \dots, 2}^{n-2}, k, 2k)$. Then we can take $(d_1, \dots, d_n) = (2l_1, 2l_2, \dots, 2l_{n-2}, kl_{n-1}, kl_n)$ for some $l_j \in \mathbb{N}$, $1 \leq j \leq n$. Now consider the following cases;

(a) $(l_j, k) > 1$ implies $w_j \geq 2(l_j, k) > 2$ for $j = 1, 2, \dots, n-2$.
(b) $(l_i, l_j) > 1$ implies $w_i \geq 2(l_i, l_j) > 2$ for $i < j$, $i = 1, 2, \dots, n-2$.
(c) $(l_{n-1}, l_n) > 1$ implies $w_{n-1} \geq k(l_{n-1}, l_n) > k$.

But all of these contradict to our assumption. Thus, at most one l_j can be even for $1 \leq j \leq n-2$. Take $l_1 = 2^{t-1} m_1 (t \geq 1)$, $l_j = m_j$ for $2 \leq j \leq n$. And since one of m_{n-1} and m_n must be odd, we can take m_{n-1} to be odd. Finally, suppose $t \geq 2$ and $4 \mid km_n$. Then $w_1 \geq 4$. This leads to a contradiction. Thus, if $t \geq 2$, then $4 \nmid km_n$.

Conversely, suppose that (6) holds. Let $\epsilon_s(k) = \max\{0, s - e_k\}$, where e_k is the exact power of 2 dividing k. Then we have

$$\begin{aligned}
w_1 &= (2^t m_1, 2^{\epsilon_1(km_n)} km_2 \cdots m_n) = (2^t, 2^{\epsilon_1(km_n)} km_n) = 2 \\
&\quad \text{(Here, if } t \geq 2, \text{ then } 4 \nmid km_n), \\
w_j &= (2m_j, \operatorname{lcm}[2^t, km_{n-1}m_n] m_1 \cdots m_{n-2}/m_j) = 2 \text{ for } j = 1, \dots, n-2, \\
w_{n-1} &= (km_{n-1}, \operatorname{lcm}[2^t, km_n] m_1 \cdots m_{n-2}) = (km_{n-1}, 2^{\epsilon_t(km_n)} km_n) = k, \\
w_n &= (km_n, \operatorname{lcm}[2^t, k] m_1 \cdots m_{n-1}) = (km_n, 2^{\epsilon_t(k)} km_{n-1}) = k(m_n, 2^{\epsilon_t(k)}) \\
&= \begin{cases} k & \text{if } 2 \nmid m_n \\ 2k & \text{if } 2 \mid m_n \text{ (then } 2 \nmid k,\ \epsilon_t(k) = t). \end{cases}
\end{aligned}$$

Hence, the proof is completed. □

THEOREM 2. *If* $2 \mid n$ *and* $d_1, \ldots, d_n$ *satisfy* (6) *in* Theorem 1, *then*

$$N(d_1, \ldots, d_n; \overbrace{1, \ldots, 1}^{n})$$

$$= \begin{cases} q^{n-1} + (k-1)(q-1)(-1)^{((q-1)/2)(n-2)/2} q^{(n-2)/2} & \text{if } 2 \mid \frac{q-1}{k} \\ q^{n-1} - (q-1)(-1)^{((q-1)/2)(n-2)/2} q^{(n-2)/2} & \text{if } 2 \nmid \frac{q-1}{k}. \end{cases}$$

Proof. Consider the case $(d_1, \ldots, d_n)_R = (w_1, \ldots, w_n) = (\overbrace{2, \ldots, 2}^{n-2}, k, 2k)$. In fact, k is odd since $(\overbrace{2, \ldots, 2}^{n-2}, k, 2k)$ is reduced. Then the equation

$$\frac{y_1}{2} + \cdots + \frac{y_{n-2}}{2} + \frac{y_{n-1}}{k} + \frac{y_n}{2k} \equiv 0 \pmod 1,$$

where $y_j = 1$ for $j = 1, \ldots, n-2$, $1 \le y_{n-1} \le k-1$, *and* $1 \le y_n \le 2k-1$ has $k-1$ solutions:

$$(\overbrace{1, \ldots, 1}^{n-2}, i, 2k-2i), \quad i = 1, \ldots, k-1. \tag{7}$$

From (3), (5), and (7), We have

$$N(d_1, \ldots, d_n; \overbrace{1, \ldots, 1}^{n}) = N(\overbrace{2, \ldots, 2}^{n-2}, k, 2k; \overbrace{1, \ldots, 1}^{n})$$
$$= q^{n-1} + \sum_{i=1}^{k-1} J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^i, \tau^{2k-2i}),$$

where $\sigma(a) = e^{2\pi i \operatorname{ind} a/k}$ is a multiplicative character of order k on $\mathbb{F}_q$, $\tau(a) = e^{\pi i \operatorname{ind} a/k}$ is a multiplicative character of order $2k$ on $\mathbb{F}_q$, and $\eta(a)$ is a quadratic character of $\mathbb{F}_q$, $a \in \mathbb{F}_q{}^*$. Similarly, we can also obtain that

$$N(\overbrace{2, \ldots, 2}^{n-2}, k, k; \overbrace{1, \ldots, 1}^{n}) = q^{n-1} + \sum_{i=1}^{k-1} J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^i, \sigma^{k-i}).$$

It is obvious that $\sigma = \tau^2$ and $J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^i, \tau^{2k-2i}) = J_0(\overbrace{\eta, \ldots, \eta}^{n-2}, \sigma^i, \sigma^{k-i})$. Hence, $N(\overbrace{2, \ldots, 2}^{n-2}, k, 2k; \overbrace{1, \ldots, 1}^{n}) = N(\overbrace{2, \ldots, 2}^{n-2}, k, k; \overbrace{1, \ldots, 1}^{n})$. Thus, it is sufficient to consider $N(\overbrace{2, \ldots, 2}^{n-2}, k, k; \overbrace{1, \ldots, 1}^{n})$. The result in this case is already obtained in [3] and we will give a proof for somewhat general case in Theorem 3. □

REMARK 2. If $t = 1$, m_n is odd and $(m_{n-1}, k) = (m_n, k) = 1$, $k \geq 3$ in Theorem 1, then Theorem in [3] follows from Theorem 2.

It is very difficult to find an explicit formula for $N(d_1, \ldots, d_n ; c_1, \ldots, c_n)$ except when $(d_1, \ldots, d_n)$ has a nice reduced form. Now we obtain an explicit formula which improves Theorem 2, under the restriction of the exponents to the reduced form.

THEOREM 3. *Let n be even and $(k_i, k_j) = 1$, $1 \leq i < j \leq t$. Then*

$$N(\overbrace{2, \ldots, 2}^{n-2t}, k_1, k_1, k_2, k_2, \ldots, k_t, k_t; \overbrace{1, \ldots, 1}^{n})$$

$$= q^{n-1} + (q-1)q^{(n-2)/2}(-1)^{((q-1)/2)(n/2-t)} \prod_{j=1}^{t} \alpha(k_j), \tag{8}$$

$$\text{where } \alpha(k) = \begin{cases} k-1 & \text{if } \ 2 \mid \frac{q-1}{k} \\ -1 & \text{if } \ 2 \nmid \frac{q-1}{k}. \end{cases}$$

Proof. Clearly $(\overbrace{2, \ldots, 2}^{n-2t}, k_1, k_1, k_2, k_2, \ldots, k_t, k_t)$ is reduced. Consider the equation

$$\frac{y_1}{2} + \cdots + \frac{y_{n-2t}}{2} + \frac{x_1}{k_1} + \frac{z_1}{k_1} + \frac{x_2}{k_2} + \frac{z_2}{k_2} + \cdots + \frac{x_t}{k_t} + \frac{z_t}{k_t} \equiv 0 \pmod 1, \tag{9}$$

where $y_j = 1$ for $j = 1, \dots, n-2t$ and $1 \le x_j, z_j \le k_j - 1$ for $j = 1, \dots, t$. By multiplying $k_1 \cdots k_t / k_j$ to (9), we have

$$\frac{x_j}{k_j} + \frac{z_j}{k_j} \equiv 0 \pmod 1,\ 1 \le x_j, z_j \le k_j - 1 \quad \text{for all } j = 1, \dots, t.$$

Thus the equation (9) has $\prod_{j=1}^{t}(k_j - 1)$ solutions:

(10)
$$(\overbrace{1, \dots, 1}^{n-2t}, i_1, k_1 - i_1, i_2, k_2 - i_2, \dots, i_t, k_t - i_t),\ i_j = 1, \dots, k_j - 1,\ j = 1, \dots, t.$$

From (3) and (10), we have

$$N(\overbrace{2, \dots, 2}^{n-2t}, k_1, k_1, k_2, k_2, \dots, k_t, k_t; \overbrace{1, \dots, 1}^{n})$$
$$= q^{n-1} + \sum_{i_1=1}^{k_1-1} \cdots \sum_{i_t=1}^{k_t-1} J_0(\overbrace{\eta, \dots, \eta}^{n-2t}, {\sigma_1}^{i_1}, {\sigma_1}^{k_1-i_1}, {\sigma_2}^{i_2}, {\sigma_2}^{k_2-i_2}, \dots, {\sigma_t}^{i_t}, {\sigma_t}^{k_t-i_t}),$$

where $\sigma_j(a) = e^{2\pi i \mathrm{ind} a / k_j}$ is a multiplicative character of order k_j on $\mathbb{F}_q$, $1 \le j \le t$ and $\eta(a) = e^{\pi i \mathrm{ind} a}$ is a quadratic character of $\mathbb{F}_q$, $a \in \mathbb{F}_q^*$. Using some properties about Gaussian sums and Jacobi sums in $\mathbb{F}_q$(See [2], Theorem 5.20, 5.21), we have

(11)
$$J_0(\overbrace{\eta, \dots, \eta}^{n-2t}, {\sigma_1}^{i_1}, {\sigma_1}^{k_1-i_1}, \dots, {\sigma_t}^{i_t}, {\sigma_t}^{k_t-i_t})$$
$$= {\sigma_t}^{k_t-i_t}(-1)(q-1) J(\overbrace{\eta, \dots, \eta}^{n-2t}, {\sigma_1}^{i_1}, {\sigma_1}^{k_1-i_1}, \dots, {\sigma_{t-1}}^{i_{t-1}}, {\sigma_{t-1}}^{k_{t-1}-i_{t-1}}, {\sigma_t}^{i_t})$$
$$= {\sigma_t}^{k_t-i_t}(-1)(q-1) \frac{G^{n-2t}(\eta, \chi) \prod_{j=1}^{t-1} \left(G({\sigma_j}^{i_j}, \chi) G({\sigma_j}^{k_j-i_j}, \chi)\right) G({\sigma_t}^{i_t}, \chi)}{G(\eta^{n-2t} \prod_{j=1}^{t-1} ({\sigma_j}^{i_j} {\sigma_j}^{k_j-i_j})\, {\sigma_t}^{i_t}, \chi)},$$

where $\chi(a) = e^{2\pi i Tr(a)/p}$ is a canonical additive character on $\mathbb{F}_q$ and $G(\sigma, \chi) = \sum_{a \in \mathbb{F}_q} \sigma(a)\chi(a)$ for each multiplicative character σ on $\mathbb{F}_q$. But, we know that $G({\sigma_j}^{i_j}, \chi)\ G({\sigma_j}^{k_j-i_j}, \chi) = G({\sigma_j}^{i_j}, \chi)\ G(\bar{\sigma_j}^{i_j}, \chi) = {\sigma_j}^{i_j}(-1)q$ and ${\sigma_t}^{k_t-i_t}(-1) = {\sigma_t}^{i_t}(-1)$. Also, since n is even, we have that $G^{n-2t}(\eta, \chi) = \Big(\eta(-1)q\Big)^{(n-2t)/2}$ and $G\Big(\eta^{n-2t} \prod_{j=1}^{t-1} ({\sigma_j}^{i_j}$

$\sigma_j{}^{k_j-i_j})\sigma_t{}^{i_t}, \chi\Big) = G(\sigma_t{}^{i_t}, \chi)$. So, (11) can be written as

$$\begin{aligned} &J_0(\overbrace{\eta,\dots,\eta}^{n-2t}, \sigma_1{}^{i_1}, \sigma_1{}^{k_1-i_1}, \dots, \sigma_t{}^{i_t}, \sigma_t{}^{k_t-i_t}) \\ &= \sigma_t{}^{i_t}(-1)(q-1)(\eta(-1)q)^{(n-2t)/2} \prod_{j=1}^{t-1} \Big(\sigma_j{}^{i_j}(-1)q\Big) \\ &= (q-1)q^{(n-2)/2}(-1)^{((q-1)/2)(n/2-t)} \prod_{j=1}^{t} \sigma_j{}^{i_j}(-1). \end{aligned}$$

Therefore,

$$\begin{aligned} &N(\overbrace{2,\dots,2}^{n-2t}, k_1, k_1, k_2, k_2, \dots, k_t, k_t; \overbrace{1,\dots,1}^{n}) \\ &= q^{n-1} + \sum_{i_1=1}^{k_1-1} \cdots \sum_{i_t=1}^{k_t-1} (q-1)q^{(n-2)/2}(-1)^{((q-1)/2)(n/2-t)} \prod_{j=1}^{t} \sigma_j{}^{i_j}(-1) \\ &= q^{n-1} + (q-1)q^{(n-2)/2}(-1)^{((q-1)/2)(n/2-t)} \prod_{j=1}^{t} \left(\sum_{i_j=1}^{k_j-1} \sigma_j{}^{i_j}(-1) \right). \end{aligned}$$

Since $k_j \mid q-1$ and $\sigma_j(-1) = e^{\pi i(q-1)/k_j}$,

$$\begin{aligned} \sum_{i_j=1}^{k_j-1} \sigma_j{}^{i_j}(-1) &= \begin{cases} k_j - 1 & \text{if} \quad 2 \mid \frac{q-1}{k_j} \\ -1 & \text{if} \quad 2 \nmid \frac{q-1}{k_j} \end{cases} \\ &= \alpha(k_j). \end{aligned}$$

This completes the proof. □

COROLLARY 4. *Let n be even and $(k_i, 2k_j) = 1$, $i \neq j$. Then*

$$\begin{aligned} &N(\overbrace{2,\dots,2}^{n-2t}, k_1, 2k_1, k_2, k_2, \dots, k_t, k_t; \overbrace{1,\dots,1}^{n}) \\ &= N(\overbrace{2,\dots,2}^{n-2t}, k_1, k_1, k_2, k_2, \dots, k_t, k_t; \overbrace{1,\dots,1}^{n}). \end{aligned}$$

Proof. Since k_1 is odd, $(2,\ldots,\ 2, k_1,\ 2k_1,\ k_2,\ k_2,\ \ldots,\ k_t,\ k_t)$ is reduced. As in the proof of the Theorem 3, we can have

$$\frac{x_1}{k_1} + \frac{z_1}{2k_1} \equiv 0 \pmod 1, \quad 1 \le x_1 \le k_1 - 1,\ 1 \le z_1 \le 2k_1 - 1,$$
$$\frac{x_j}{k_j} + \frac{z_j}{k_j} \equiv 0 \pmod 1, \quad 1 \le x_j, z_j \le k_j - 1 \text{ for all } j = 2,\ldots,t.$$

The conclusion is obtained in the same way as in the proof of the Theorem 2. □

Finally, we note that if $t = 0$ in Theorem 3, then we have

$$N(\overbrace{2,\ldots,2}^{n};\overbrace{1,\ldots,1}^{n}) = q^{n-1} + (q-1)q^{(n-2)/2}(-1)^{((q-1)/2)n/2}.$$

This is the result of the Corollary of Theorem 2 in [4] since $\eta(-1) = (-1)^{(q-1)/2}$ (where $c_j = 1$ for all $j = 1,\ldots,n$). If $t = 1$, then Theorem 2 follows from Theorem 3 and Corollary 4.

References

[1] Granville, Shuguang Li, and Sun Qi, *On the Number of Solution of the Equation* $\sum_{i=1}^{n} x_i/d_i \equiv 0$ *(mod* 1*) and of Diagonal Equations in Finite Fields*, J. Sichuan Univ. Natural Sci. **3** (1995), 243–248.

[2] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl., Addison–Wesley, Reading, MA, **20** (1983).

[3] Sun Qi, *On Diagonal Equations over Finite Fields*, Finite Fields Appl. **3** (1997), 175–179.

[4] Sun Qi and Ping-Zhi Yuan, *On the Number of Solutions of Diagonal Equations over a Finite Field*, Finite Fields Appl. **2** (1996), 35–41.

[5] Daqing Wan, *Zeros of Diagonal Equations over Finite Fields*, Proc. Amer. Math. Soc. **103** (1988), 1049–1052.

YOUGNGGU MOON AND JUNE BOK LEE, DEPARTMENT OF MATHEMATICS, YONSEI UNIVERSITY, SEOUL 120-749, KOREA

YOUNG HO PARK, DEPARTMENT OF MATHEMATICS, KANGWON NATIONAL UNIVERSITY, CHUNCHEON 200-701, KOREA