EQUIVALENCE CLASSES OF SUBSETS OF A FINITE FIELD

Ju-Yong Xu
(Dept. of Basic Science, Wuhan Urban Construction Institute, Wuhan 430074,Hubei,China)
and
Wan-Di Wei
(Dept. of Math. Sichuan University, Chengdu 610064,Sichuan, China)

ABSTRACT

For a finite field $F=F(q), q = p^n$ is a prime power, we will introduce the notion of equivalence of subsets of F which stems out of the equivalence of cyclic difference sets, and give the formulae for the number of equivalence classes of k-subsets of F as well for the number of equivalence classes of subsets of F by using Polya's theorem of counting.

§ 1. Introduction

Let Z_v be the residue class ring of integers. Wei, Gao and Yang [3] propose the notion of equivalence of subsets of Z_v, which stems out of the equivalence of cyclic difference sets [1], and give the formulae for the number of equivalence classes of k-subsets of Z_{p^n} $(0 \le k \le p^n)$,and for the number of equivalence classes of subset of Z_{p^n} ,where p is a prime and n is a positive integer, latter

ARS COMBINATORIA 62(2002), pp. 33-49

Wei and Xu[1] introduce the direct product of permutation groups, and then give the formulae for the number of equivalence classes of k-subsets of Z_v ($0 \le k \le v$),and for the number of equivalence classes of subsets of Z_v,where v is an arbitrary positive integer. In this paper, we will introduce the notion of equivalence of subsets of a finite field, and give the formulae for the number of equivalence classes of k-subsets of the field as well for the number of equivalence classes of subsets of the field.

Let F=GF(q) be a finite field with q elements, where $q = p^n$ is a prime power. Let D be a subset of F, Then we denote

$$tD+s=\{td+s \mid d \in D\}, \quad t,s \in F \tag{1.1}$$

Definition 1. Two subsets D_1 and D_2 of F are said to be equivalent, denoted by $D_1 \sim D_2$,if there are $t \neq 0, s \in F$ such that

$$D_1 = tD_2 + s \tag{1.2}$$

It is easy to verify that the relationship "~" so defined is indeed an equivalence relation. Therefore, all the subsets of F are partitioned into equivalence classes. Evidently, in an equivalence class, every subset has the same cardinality, which will be called the subset-cardinality of the class.

The following problems arise naturally.

Problem 1 find a formula for the number of equivalence classes of subsets of GF(q).This number will be denoted by N(q).

Problem 2 Find a formula for the number of equivalence classes of k-subsets of GF(q), $0 \le k \le q$ .This number will be denoted by N(q, k).

These two problems will be solved in § 3;To prepare the way, a related permutation group and its cycle index will be investigated in § 2;and two illustrative examples will be given in § 4.

§ 2. A permutation group

From (1.2),it is natural to introduce the following subset of F×F:

$$X = X(F) = \{(t,s) \in F \times F \mid t \neq 0\}$$

Let α be a primitive root of F, then

$$F = \{0,1,\alpha,\alpha^2,\cdots,\alpha^{q-2}\}.$$

For $(t,s) \in X$, let $\sigma(t,s)$ be the mapping from F to F:

$$\sigma(t,s): f \to tf+s \quad \text{, for all } f \in F,$$

or

$$\sigma(t,s)(f) = tf+s.$$

Clearly, $\sigma(t,s)$ is a permutation on F, and can be written into the usual form of a permutation:

$$\begin{pmatrix} 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{q-2} \\ s & t+s & t\alpha+s & t\alpha^2+s & \cdots & t\alpha^{q-2}+s \end{pmatrix}$$

Let

$$P = P(q) = \{\sigma(t,s) \mid (t,s) \in X\}. \tag{2.1}$$

For two permutations $\sigma(u,v)$ and $\sigma(t,s)$ in P, according to the multiplication of permutations, we have

$$(\sigma(u,v)\sigma(t,s))(f) = \sigma(u,v)(\sigma(t,s)(f)), \quad (u,v),(t,s) \in X, f \in F.$$

Then we have

Lemma 1. P is a permutation group.

Proof. Evidently, $\sigma(1,0) \in P$ and is the identity permutation. If $\sigma(u,v),\sigma(t,s) \in P$, then

$$\begin{aligned} &(\sigma(u,v),\sigma(t,s))(f) = \sigma(u,v)(\sigma(t,s)(f)) \\ &= \sigma(u,v)(tf+s) \\ &= (ut)f+(us+v) \\ &= \sigma(ut,us+v)(f), f \in F. \end{aligned}$$

Therefore, $\sigma(u,v)\sigma(t,s) = \sigma(ut,us+v)$ .Since $u \neq 0$ and $t \neq 0$,it follows that $ut \neq 0$ and then $\sigma(u,v)\sigma(t,s) \in P$.

If $\sigma(t,s) \in P$,then $\sigma(t^{-1},-t^{-1}s) \in P$ and

$$\sigma(t^{-1},-t^{-1}s)\sigma(t,s)(f) = \sigma(t^{-1},-t^{-1}s)(tf+s)$$
$$= t^{-1}(tf+s) - t^{-1}s = f, f \in F$$

Therefore, the inverse of $\sigma(t,s)$ exists and $(\sigma(t,s))^{-1} = \sigma(t^{-1},-t^{-1}s)$. Hence the lemma.

It is important for our purpose to obtain the expression of the cycle index of group *P*, which we discuss now.

Let *T={1,x}* be a 2-set, where *x* is an indeterminate. Let

$$T^F = \{h : F \to T\}$$

be the set of mappings from *F* into *T*. For any $h \in T^F$,write

$$W(h) = \prod_{f \in F} h(f)$$

which will be called the weigh of the mapping *h*. As usual, the *{1,x}*-Characteristic function of a subset *D* of *F* is the mapping $h \in T^F$ satisfying

$$h(f) = \begin{cases} x, & f \in D, \\ 1, & f \notin D. \end{cases}$$

A subset of *F* and its characteristic function will be regarded as the same thing.

Definition 2. Two mappings $h_1, h_2 \in T^F$ are said to be equivalent, written $h_1 \sim h_2$,if there is a permutation $\sigma(t,s) \in P$ such that

$$h_1(\sigma(t,s)(f)) = h_2(f), \text{ for all } f \in F.$$

It is easy to see the equivalence "$\sim$" so defined is an equivalence relation.

The following lemma states the relationship between the equivalence of two subsets of F and the equivalence of two mappings in T^F.

Lemma 2 . Two subsets of F are equivalent iff their characteristic functions are equivalent.

Proof. Let D_1, D_2 be two subsets of F, and h_1,h_2 their characteristic functions, respectively. If there is a (t, s)$\in$ X such that D_1 =tD_2 +s, then

$$h_1(\sigma(t,s)(f)) = \begin{cases} x, tf+s \in D_1 \\ 1, otherwise \end{cases}$$

$$= \begin{cases} x, f \in D_2 \\ 1, otherwise \end{cases}$$

$$= h_2(f).$$

And vice versa. Hence the lemma.

As usual, a permutation of type $1^{l_1}2^{l_2}...q^{l_q}$ or a $1^{l_1}2^{l_2}...q^{l_q}$-permutation, is a permutation on q elements with l_i cycles of length i($1 \le i \le q$)when it is written as a product of disjoint cycles. Such a permutation π corresponds to the following element of ring $Z[x_1,x_2,...,x_q]$:

$$\pi[x_1,x_2,...,x_q] = x_1^{l_1}x_2^{l_2}...x_q^{l_q},$$

Where Z is the integer ring, and x_i ($1 \le i \le q$) are indeterminate. This $\pi[x_1, x_2,...,x_q]$ is called the cycle index of π.Furthermore, the cycle index of the permutation group P is

$$Q_p(x_1,x_2,...,x_q) = \frac{1}{|P|}\sum_{\pi \in P} \pi[x_1,x_2,...,x_q] \qquad (2.2)$$

We will now seek the expression of (2.2).

Let (t, s)$\in X$ and f$\in F$.Denote by c(f) the length of the cycle of $\sigma(t,s)$ to which f belongs. Then c(f) is the smallest positive integer m such that

$$\sigma^m(t,s)(f) = f \ . \tag{2.3}$$

By induction, it is easy to prove

$$\sigma^m(t,s) = \sigma(t^m, \sum_{i=0}^{m-1} t^i s), \quad m \geq 0 \tag{2.4}$$

Then (2.3) becomes

$$t^m f + \sum_{i=0}^{m-1} t^i s = f \ . \tag{2.5}$$

Lemma 3. Let $(t,s) \in X$ with $t \neq 1$,then the cycle index of $\sigma(t,s)$ is

$$\sigma(t,s)[x_1, x_2, ..., x_q] = x_1 x_e^{\frac{q-1}{e}} \tag{2.6}$$

where e is the order of t in the multiplicative group $F^* = F \setminus \{0\}$.

Proof. When $t \neq 1$,(2.5) can be rewritten as

$$(t^m - 1)(f + (t-1)^{-1} s) = 0. \tag{2.7}$$

There are two cases to consider.

Case 1. $f = -(t-1)^{-1} s$.

In this case, (2.7) holds for any $m \geq 1$ .Therefore, c(f)=1.On the other hand, such f is unique, which itself forms a 1-cycle of $\sigma(t,s)$.

Case 2. $f \neq -(t-1)^{-1} s$.

In this case,(2.7) holds iff

$$t^m = 1 \ . \tag{2.8}$$

i.e., c(f) is nothing but the order of t in the group F^* :c(f)=e. Since the length of the cycle containing such f if c(f) and the number of such f is q-1,the number of the c(f)-cycles is

$$\frac{q-1}{c(f)} = \frac{q-1}{e}.$$

Hence (2.6).

Lemma 4. The cycle index of $\sigma(1,s)$ is

$$\sigma(1,s)[x_1,...,x_q] = \begin{cases} x_1^q, s = 0 \\ x_p^{p^{n-1}}, s \neq 0 \end{cases} \tag{2.9}$$

Proof. When t=1,(2.5) becomes f+ms=f, i.e.,

$$ms=0 \tag{2.10}$$

There are two cases to consider.

Case 1. $s \neq 0$.

Since F has characteristic p, (2.10) holds iff $m \equiv 0 \pmod{p}$ .Therefore, c(f)=p for all $f \in F$ .Since each cycle has length p, there are $q/p = p^{n-1}$ cycles.

Case 2. S=0.

In this case, (2.10) is true for any m. In fact, $\sigma(1,0)$ is the identity permutation of P. Therefore, $\sigma(1,0)[x_1,...,x_q] = x_1^q$. This completes the proof.

We are now in a position to give the cycle index of P.

Theorem 1. Let $q = p^n$ be a prime power and P the permutation group defined in (2.1).Then the cycle index of P is

$$Q_p(x_1,...,x_q) = \frac{1}{q(q-1)}\{x_1^q + (q-1)x_p^{p^{n-1}} + q\sum_{\substack{e|(q-1) \\ e>1}} \varphi(e)x_1 x_e^{\frac{q-1}{e}}\} \tag{2.11}$$

where $\varphi(e)$ is the Euler function.

Proof. The factor q(q-1) in the denominator on the right hand side of (2.11) is due to |P|=q(q-1).The first term in the brace corresponds to the identity permutation $\sigma(1,0)$ of P; the second term corresponds to the (q-1) permutations $\sigma(1,s)$ with $s \neq 0$.The reason for the third term in the brace is as follows. It is well known that a positive integer e is the order of some element of the multiplicative group F* iff

$$q-1 \equiv 0 \pmod{e}, \qquad (2.12)$$

and when e satisfies (2.12),there are $\varphi(e)$ elements of order e in F*. Therefore, there are $\varphi(e)q$ permutation of the form $\sigma(t,s)$,the order of t is e.

This completes the proof.

Note: when q is a prime,i.e.,n=1,(2.11) becomes

$$\frac{1}{p(p-1)}\{x_1^p+(p-1)x_p+p\sum_{\substack{e|(p-1)\\ e>1}}\varphi(e)x_1x_e^{\frac{p-1}{e}}\},$$

which coincides with the result in [3].

§ 3 Formulae for N(q) and N(q, k)

We are ready to apply Polya's theorem of counting to obtain formulae for N(q) and N(q, k).

Theorem 2.

$$N(q)=\frac{1}{q(q-1)}\{2^q+(q-1)2^{\frac{q-1}{e}+1}+q\sum_{\substack{e|(q-1)\\ e>1}}\varphi(e)2^{\frac{q-1}{e}+1}\} \qquad (3.1)$$

Proof. By Polya's theorem of counting,

$$N(q)=[Q_p(x_1,x_2,\ldots,x_q)]_{x_1=x_2=\ldots=x_q=|T|}=Q_p(2,2,\ldots,2).$$

which is, by Theorem 1,the expression on the right hand side of (3.1).

For the next theorem, we need the notation: For integer m and real number y, denote

$$\binom{m}{y}=\begin{cases}\binom{m}{y}, & \text{if } y \text{ is a nonnegative int eger},\\ 0, & \text{otherwies.}\end{cases}$$

Theorem 3. For $0 \le k \le q$

$$N(q,k)=\frac{1}{q(q-1)}\{\binom{q}{k}+(q-1)\binom{\frac{q}{p}}{\frac{k}{p}}+q\sum_{\substack{e|(k-1,q-1)\\ e>1}}\varphi(e)\binom{\frac{q-1}{e}}{\frac{k-1}{e}}+q\sum_{\substack{e|(k,q-1)\\ e>1}}\varphi(e)\binom{\frac{q-1}{e}}{\frac{k}{e}}\} \qquad (3.2)$$

Proof. By Polya's theorem of counting, N(q, k) is the coefficient of x^k in $Q_p(x+1, x^2+1, ..., x^q+1)$:

$$N(q,k) = \frac{1}{k!}[(\frac{d}{dx})^k Q_p(x+1, x^2+1, ..., x^q+1)]_{x=0} \qquad (3.3)$$

By Theorem 1,

$$Q_p(x+1, x^2+1, ..., x^q+1) =$$

$$\frac{1}{q(q-1)}\{(x+1)^q + (q-1)(x^p+1)^{q/p} + q\sum_{\substack{e|(q-1)\\ e>1}} \varphi(e)(x+1)(x^e+1)^{(q-1)/e}\} \qquad (3.4)$$

The coefficient of x^k in $(x^p+1)^{q/p}$ is

$$\binom{q/p}{k/p}. \qquad (3.5)$$

The coefficient of x^k in $(x^e+1)^{(q-1)/e}$ with e|(q-1) is

$$\binom{(q-1)/e}{k/e}, \qquad (3.6)$$

and then the coefficient of x^k in $(x+1)(x^e+1)^{(q-1)/e}$ is

$$\binom{(q-1)/e}{k/e} + \binom{(q-1)/e}{(k-1)/e}$$

Therefore,

$$N(q,k) = \frac{1}{q(q-1)}\{\binom{q}{k} + (q-1)\binom{q/p}{k/p} + q\sum_{\substack{e|(q-1)\\ e>1}} \varphi(e)[\binom{(q-1)/e}{(k-1)/e} + \binom{(q-1)/e}{k/e}]\}$$

which leads to (3.2).

The following theorem states some properties of N(q, k).

Theorem 4.

$$N(q,k) = N(q,q-k), \quad 0 \le k \le q, \tag{3.7}$$

$$\sum_{k=0}^{q} N(q,k) = N(q), \tag{3.8}$$

$$N(q,0) = 1, \tag{3.9}$$

$$N(q,1) = 1, \tag{3.10}$$

$$N(q,2) = 1, \tag{3.11}$$

$$N(q,3) = \begin{cases} \frac{q+5}{6}, q \equiv 1 \pmod 6 & (3.12) \\ \frac{q-2}{6}, q \equiv 2 \pmod 6 & (3.13) \\ \frac{q+3}{6}, q \equiv 3 \pmod 6 & (3.14) \\ \frac{q+2}{6}, q \equiv 4 \pmod 6 & (3.15) \\ \frac{q+1}{6}, q \equiv 5 \pmod 6 & (3.16) \end{cases}$$

Proof. It is easy to see that for any $(t,s) \in X$, we have $tF + s = F$ and then for any subsets D_1, D_2 of F, $D_1 = tD_2 + s$ *iff* $\overline{D}_1 = t\overline{D}_2 + s$,where $\overline{D}$ means the complement of D in F. This proves (3.7).(3.7) can also be proved by applying (3.2) and noticing that

$$\binom{q}{k} = \binom{q}{q-k}, \quad \binom{q/p}{k/p} = \binom{q/p}{q-k/p}, \quad e \mid (k-1, q-1) \text{ iff } e \mid (q-k, q-1),$$

$$\binom{q-1/e}{k-1/e} = \binom{q-1/e}{q-k/e}, \quad e \mid (k, q-1) \quad \text{iff} \quad e \mid (q-k-1, q-1),$$

$$\binom{q-1/e}{k/e} = \binom{q-1/e}{(q-k)-1/e}$$

By the combinatorial meaning of N(q,0),(3.9) is evident. For any two elements $f_1, f_2 \in F$, $\sigma(t, f_2 - tf_1)(f_1) = tf_1 + (f_2 - tf_1) = f_2$, which proves (3.10).

For any two subsets $\{d_1, d_2\}, \{d_3, d_4\}$ of F, we have

$$d_1 \neq d_2, d_3 \neq d_4, \frac{d_3 - d_4}{d_1 - d_2} \neq 0, \quad \text{and}$$

$$\sigma(\frac{d_3 - d_4}{d_1 - d_2}, \frac{d_1 d_4 - d_2 d_3}{d_1 - d_2})(d_1) = \frac{d_3 - d_4}{d_1 - d_2} d_1 + \frac{d_1 d_4 - d_2 d_3}{d_1 - d_2} = d_3,$$

$$\sigma(\frac{d_3 - d_4}{d_1 - d_2}, \frac{d_1 d_4 - d_2 d_3}{d_1 - d_2})(d_2) = \frac{d_3 - d_4}{d_1 - d_2} d_2 + \frac{d_1 d_4 - d_2 d_3}{d_1 - d_2} = d_4.$$

Therefore,(3.11) holds.

All of (3.9)-(3.11) can also be proved by applying (3.2). As verification of the validity of (3.2) for these cases, we give it as follows. According to (3.2),

$$N(q,0) = \frac{1}{q(q-1)}\{1 + (q-1) + q \sum_{\substack{e|(q-1) \\ e>1}} \varphi(e)(0+1)\}$$

$$= \frac{1}{q(q-1)}\{q + q[(q-1)-1]\} = 1$$

$$N(q,1) = \frac{1}{q(q-1)}\{q + (q-1)\cdot 0 + q \sum_{\substack{e|(q-1) \\ e>1}} \varphi(e)(0+1)\}$$

$$= \frac{1}{q(q-1)}\{q + q[(q-1)-1]\} = 1$$

$$N(q,2) = \frac{1}{q(q-1)}\{\frac{q(q-1)}{2} + (q-1)\cdot 0 + q \sum_{\substack{e|(q-1) \\ e>1}} \varphi(e)\left[\binom{\frac{q-1}{e}}{\frac{1}{e}} + \binom{\frac{q-1}{e}}{\frac{2}{e}}\right]\}$$

$$= \frac{1}{q(q-1)}\{\frac{q(q-1)}{2} + q\varphi(2)\frac{q-1}{2}\}$$

$$= 1 \quad , \qquad if \quad p \neq 2$$

$$N(q,2)=\frac{1}{q(q-1)}\{\frac{q(q-1)}{2}+(q-1)\binom{q}{p}+q\sum_{\substack{e|q-1\\ e>1}}\varphi(e)\left[\binom{\frac{q-1}{e}}{\frac{1}{e}}+\binom{\frac{q-1}{e}}{\frac{2}{e}}\right]\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)}{2}+\frac{q(q-1)}{2}\}$$

$$=1, \qquad if \quad p=2.$$

We now prove (3.12)-(3.16).

When

$$p\neq 2, q\equiv 1 \pmod 3, \tag{3.17}$$

we have

$$N(q,3)=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+(q-1)\cdot 0+q\sum_{\substack{e|(q-1)\\ e>1}}\varphi(e)[\binom{\frac{q-1}{e}}{\frac{2}{e}}+\binom{\frac{q-1}{e}}{\frac{3}{e}}]\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+q\{\varphi(2)[\binom{\frac{q-1}{2}}{1}+0]+\varphi(3)[0+\binom{\frac{q-1}{3}}{1}]\}\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+q(\frac{q-1}{2}+\frac{2(q-1)}{3})\}=\frac{q+5}{6.}$$

When

P=2, q is not congruent to 1 modulo 3, (3.18)

we have

$$N(q,3)=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+0+q\sum_{\substack{e|(q-1)\\ e>1}}\varphi(e)[\binom{\frac{q-1}{e}}{\frac{2}{e}}+\binom{\frac{q-1}{e}}{\frac{3}{e}}]\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+0\}=\frac{q-2}{6}$$

When

$$p=3, \tag{3.19}$$

we have

$$N(q,3)=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+(q-1)\binom{\frac{q}{p}}{1}+q\sum_{\substack{e|(q-1)\\ e>1}}\varphi(e)[\binom{\frac{q-1}{e}}{\frac{2}{e}}+\binom{\frac{q-1}{e}}{\frac{3}{e}}]\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+(q-1)\frac{q}{3}+q\varphi(2)\binom{\frac{q-1}{2}}{1}\}=\frac{q+3}{6}$$

When

$$p=2, q\equiv 1 \pmod 6 \tag{3.20}$$

we have

$$N(q,3)=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+0+q\sum_{\substack{e|(q-1)\\ e>1}}\varphi(e)[\binom{\frac{q-1}{e}}{\frac{2}{e}}+\binom{\frac{q-1}{e}}{\frac{3}{e}}]\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+q\varphi(3)\frac{q-1}{3}\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+\frac{2q(q-1)}{3}\}=\frac{q+2}{6}.$$

When

$$p\neq 2,3\text{ , q is not congruent to 1 modulo 3,} \tag{3.21}$$

we have

$$N(q,3)=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+0+q\sum_{\substack{e|(q-1)\\ e>1}}\varphi(e)[\binom{\frac{q-1}{e}}{\frac{2}{e}}+\binom{\frac{q-1}{e}}{\frac{3}{e}}]\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+q\varphi(2)\frac{q-1}{2}\}$$

$$=\frac{1}{q(q-1)}\{\frac{q(q-1)(q-2)}{6}+\frac{q(q-1)}{2}\}=\frac{q+1}{6.}$$

On the other hand,(3.17)-(3.21) are equivalent to $q\equiv 1,2,3,4.5 \pmod 6$ respectively.

§ 4 Examples

Two examples will be given to illustrate what we have got in the previous sections.

Example 1. Let α be a root of the irreducible quadratic polynomial x^2+x+2 over GF(3).Then $GF(3^2)$ can be expressed as

$$GF(9)=\{0,1,2,\alpha,\alpha+1,\alpha+2,2\alpha,2\alpha+1,2\alpha+2\}.$$

Applying Theorem 4 we have

$$\begin{cases} N(9,0)=N(9,9)=N(9,1)=N(9,8)=N(9,2)=N(9,7)=1 \\ N(9,3)=N(9,6)=(9+3)/6=2. \end{cases} \tag{4.1}$$

Besides,(3.2') gives

$$N(9,4)=N(9,5)=\frac{1}{9\cdot 8}\{\binom{9}{4}+8\cdot 0+9\sum_{\substack{e\mid 8\\ e>1}}\varphi(e)[\binom{8/e}{3/e}+\binom{8/e}{4/e}]\}$$

$$=\frac{1}{9\cdot 8}\{\binom{9}{4}+9[\varphi(2)\binom{4}{2}+\varphi(4)\binom{2}{1}]\}=3. \tag{4.2}$$

It can be verified that the equivalence classes corresponding to (4.1) are A and $\binom{GF(9)}{3}\setminus A$, where $\binom{S}{k}$ stands for the family of k-subsets of S if S is a set, and

$$A=\{\{0,1,2\},\{\alpha,\alpha+1,\alpha+2\},\{2\alpha,2\alpha+1,2\alpha+2\},\{0,\alpha,2\alpha\},$$
$$\{1,\alpha+1,2\alpha+1\}.\{2,\alpha+2,2\alpha+2\},\{0,\alpha+1,2\alpha+2\},\{1,\alpha+2,2\alpha\},$$
$$\{2,\alpha,\alpha+1\},\{0,\alpha+2,2\alpha+1\},\{1,\alpha,2\alpha+2\},\{2,\alpha+1,2\alpha\}\}$$

and the equivalence classes corresponding to (4.2) are B,C and $\binom{GF(9)}{4}\setminus(B\cup C)$, where

$$B = \{\{0,1,\alpha+1,\alpha\},\{1,2,\alpha+1,\alpha+2\},\{2,0,\alpha+2,\alpha\},\{\alpha,\alpha+1,2\alpha,2\alpha+1\},$$
$$\{\alpha+1,\alpha+2,2\alpha+1,2\alpha+2\},\{\alpha+2,\alpha,2\alpha+2,2\alpha\},\{2\alpha,2\alpha+1,0,1\},$$
$$\{2\alpha+2,2\alpha.2,0\},\{0,\alpha,2\alpha+1,1\},\{1,\alpha+1,2\alpha+2,2\},\{2\alpha+1,1,\alpha+2,2\alpha+2\},$$
$$\{\alpha+1,2\alpha+1,2,\alpha+2\},\{\alpha+2,2\alpha+2,0,\alpha\},\{2\alpha,0,\alpha+1,2\alpha+1\},\{2\alpha+1,2\alpha+2,1,2\},$$
$$\{2\alpha+2,2,\alpha,2\alpha\},\{0,\alpha+1,1,\alpha+2\},\{1,\alpha+2,2,\alpha\},\{2,\alpha,0,\alpha+1\},\{2,\alpha+2,2\alpha,0\},$$
$$\{\alpha+1,2\alpha+2,\alpha+2,2\alpha\},\{\alpha+2,2\alpha,\alpha,2\alpha+1\},\{2\alpha,1,2\alpha+1,2\},\{2\alpha+1,2,2\alpha+2,0\},$$
$$\{2\alpha+2,0,2\alpha,1\},\{0,\alpha+2,\alpha+1,2\alpha\},\{1,\alpha,\alpha+2,2\alpha+1\},\{2,\alpha+1,\alpha,2\alpha+2\},$$
$$\{\alpha,2\alpha+2,2\alpha+1,0\},\{\alpha+1,2\alpha,2\alpha+2,1\},\{\alpha+2,2\alpha+1,2\alpha,2\},\{2\alpha,2,1,\alpha\},$$
$$\{2\alpha+1,0,2,\alpha+1\}\{2\alpha+2,1,0,\alpha+2\},\{\alpha,2\alpha+1,\alpha+1,2\alpha+2\},\{\alpha,2\alpha,1,\alpha+1\}\}$$

$$C = \{\{0,1,\alpha,\alpha+2\},\{1,2,\alpha+1,\alpha\},\{2,0,\alpha+2,\alpha+1\},\{\alpha,\alpha+1,2\alpha,2\alpha+2\},$$
$$\{\alpha+1,\alpha+2,2\alpha+1,2\alpha\},\{\alpha+2,\alpha,2\alpha+2,2\alpha+1\},\{2\alpha,2\alpha+1,0,2\},$$
$$\{2\alpha+2,2\alpha,2,1\},\{0,\alpha,2\alpha+1,\alpha+1\},\{1,\alpha+1,2\alpha+2,\alpha+2\},\{2,\alpha+2,2\alpha,\alpha\},$$
$$\{\alpha,2\alpha,1,2\alpha+2\},\{\alpha+1,2\alpha+1,2,2\alpha+2\},\{\alpha+2,2\alpha+2,0,2\alpha\},\{2\alpha,0,\alpha+1,1\},$$
$$\{2\alpha+1,1,\alpha+2,2\},\{2\alpha+2,2,\alpha,0\}\{2\alpha+1,2\alpha+2,1,0\}\}.$$

Also by Theorem 4,

$$N(9) = 2[N(9,0) + N(9,1) + N(9,2) + N(9,3) + N(9,4)] = 16.$$

Half of the 16 equivalence classes are

$$\phi, \{\{f\} \mid f \in GF(9)\}, \binom{GF(9)}{2}, A, \binom{GF(9)}{3} \setminus A,$$
$$B, C, \binom{GF(9)}{4} \setminus (B \cup C), \tag{4.3}$$

and the other half can be produced from these eight as follows:

$$\{D \mid \overline{D} \in H\}$$

where H is one of the classes in (4.3).

Example 2. Let β be a root of the irreducible polynomial $x^3 + x + 1$ over GF(2).Then $GF(2^3)$ can be expressed as

$$GF(8) = \{0,1,\beta,\beta+1,\beta^2+1,\beta^2+\beta,\beta^2,\beta^2+\beta+1\}.$$

Applying Theorem 4,we have

$$N(8,0) = N(8,8) = N(8,1) = N(8,7) = N(8,2) = N(8,6) = 1$$

$$N(8,3) = N(8,5) = \frac{8-2}{6} = 1.$$

Besides,(3.2') gives

$$N(8,4) = \frac{1}{8\cdot 7}\{\binom{8}{4} + 7\cdot\binom{8/2}{4/2} + 8\sum_{\substack{e|7\\ e>1}}\varphi(e)[\binom{7/e}{3/e} + \binom{7/e}{4/e}]\}$$

$$= \frac{1}{8\cdot 7}[\binom{8}{4} + 7\cdot 6] = 2,$$

and it can be verified that these two equivalence classes are E and $\binom{GF(8)}{4} \setminus E$,where

$$E = \{\{1,0,\beta,\beta+1\},\{\beta^2,\beta^2+1,\beta^2+\beta,\beta^2+\beta+1\},\{0,\beta,\beta^2,\beta^2+\beta\},$$
$$\{1,\beta^2+1,\beta+1,\beta^2+\beta+1\},\{0,\beta+1,\beta^2+1,\beta^2+\beta\},\{1,\beta,\beta^2,\beta^2+\beta+1\},$$
$$\{\beta^2,\beta+1,0,\beta^2+\beta+1\},\{1,\beta^2+1,\beta^2+\beta,\beta\},\{0,\beta^2+1,\beta^2,1\},$$
$$\{\beta,\beta+1,\beta^2+\beta,\beta^2+\beta+1\},\{0,1,\beta^2+\beta,\beta^2+\beta+1\},\{\beta,\beta^2+1,\beta^2,\beta+1\},$$
$$\{0,\beta^2+1,\beta,\beta^2+\beta+1\},\{\beta^2,1,\beta^2+\beta,\beta+1\}\},$$

Again by Theorem 4,

$$N(8) = 2[N(8,0) + N(8,1) + N(8,2) + N(8,3) + N(8,4)] = 10$$

Half of the 10 equivalence classes are

$$\phi,\quad \{\{f\} \mid f \in GF(8)\},\binom{GF(8)}{2},\binom{GF(8)}{3}, E, \tag{4.4}$$

and the other half can be produced from these five as follows:

$$\{D \mid \overline{D} \in H\},$$

where H is one of the classes in (4.4).

References

1. M.Hall Jr., A Survey of Difference Sets, Proc. Amer. Math. Soc., 7(1956).975-986.
2. G.Po'lya, Kombinatorische Anzahlbestimmungen für Gruppen,Graphen und Chemische Verbindungen,Acta Math.,68(1937),145-254.
3. W.-D. Wei,X.-H. Gao and B.-F. Yang, Equivalence Relation on the Set of Subsets of Z_v and Enumeration of the Equivalence Classes(Research Announcement),Advances in Math.,17(1988),326-327.
4. W.-D. Wei and J.-Y. Xu, Cycle Index of Direct Product of Permutation Groups and Number of Equivalence Classes of Subsets of Z_v,Discrete Math. 123(1993),179-188.