ACTA ARITHMETICA
X (1964)

Equivalence classes of functions over a finite field*

by

S. R. Cavior (Buffalo)

1. Introduction. Let $GF(q)$ denote a finite field, and suppose f, g are functions of r variables, $r \geqslant 1$, with coefficients in the $GF(q)$. In [2] L. Carlitz defined f and g to be *equivalent* if there exists an invertible set of transformations

$$\varphi\colon\ \beta_i = \varphi_i(a_1, \ldots, a_r) \qquad (a_i, \beta_i \in GF(q)) \tag{1.1}$$

such that

$$f\varphi = g, \tag{1.2}$$

where $f\varphi(a_1, \ldots, a_r) = f\big(\varphi(a_1, \ldots, a_r)\big)$. When $r = 1$, φ is called a *permutation function*. The functional equation is in fact an equivalence relation which separates the functions over $GF(q)$ into equivalence classes. Carlitz in [2] described completely the invariants of these classes.

The chief object of this present paper is to study five different families of equivalence classes of functions in one variable. They are determined respectively by the five following functional equations, where φ, φ_1, and φ_2 are permutation functions:

$$g\varphi = h \quad \text{right equivalence,} \tag{1.3}$$

$$\varphi g = h \quad \text{left equivalence,} \tag{1.4}$$

$$\varphi_1 g \varphi_2 = h \quad \text{weak equivalence,} \tag{1.5}$$

$$\varphi^{-1} g \varphi = h \quad \text{similarity,} \tag{1.6}$$

$$\varphi_1 g = h;\ \ g\varphi_2 = h \quad \text{strong equivalence.} \tag{1.7}$$

All the functional equations are easily verified to be equivalence relations.

* This research was supported by National Science Foundation grant G-16485.

For each equivalence we shall attempt to find the number of classes, the number of functions in a class, and the number of automorphisms, where an automorphism of a function g, say with respect to (1.4), is a permutation function φ such that $\varphi g = g$. We shall also discuss the relations among the various types of equivalence and give a few examples of them.

In the final section of the paper we obtain necessary and sufficient conditions for the solvability of some functional equations over a finite field and derive several formulas for the number of solutions. The equations we study are:

(1.8) $$fg = f,$$

(1.9) $$gf = f,$$

(1.10) $$ff = f,$$

(1.11) $$fg = h.$$

We should mention that most of the results in this paper do not depend on the properties of a finite field. In fact, with the exception of Theorem 4.2, all the theorems in Sections 4, 5, 6, 7, and 9 will hold for functions defined over an arbitrary finite set.

2. Preliminaries. Let $q = p^n$, where p is an arbitrary prime and $n \geqslant 1$. GF(q) will denote the unique finite field of order q, and its numbers will be denoted by lower case α, β, γ, and δ.

f will be called a *function over* GF(q), or simply a function, if f maps GF(q) into itself. If f is an arbitrary function, R_f will denote the range of f, and f will be called a *permutation function* if $R_f = \mathrm{GF}(q)$. Functions in general will be denoted by lower case f, g, and h, but permutation functions will be written as lower case φ, ψ, and η. By the Lagrange Interpolation Formula ([3], p. 55) an arbitrary function f over GF(q) can be expressed as a polynomial of degree $< q$:

(2.1) $$f(x) = -\sum_{\alpha} \{(x-\alpha)^{q-1}-1\} f(\alpha).$$

We define Π_f, the partition of f, to be the decomposition of GF(q) into disjoint subsets $\{S_i : i = 1, \ldots, t\}$ such that $\alpha, \beta \in S_i$ provided $f(\alpha) = f(\beta)$. If $\alpha \in S_i$ and $f(\alpha) = \beta$, $f(S_i)$ is defined to be β, and $f^{-1}(\beta)$ is defined to be S_i. If S is a subset of GF(q), $o(S)$ will denote the number of elements in S. For example, if $R_f = \{\alpha_i : i = 1, \ldots, t\}$, then $o(R_f) = t$.

If $\alpha \in \mathrm{GF}(q)$ we define

$$t(\alpha) = \alpha + \alpha^p + \ldots + \alpha^{p^{n-1}}.$$

We next put

(2.2) $$e(\alpha) = e^{\frac{2\pi i}{p} t(\alpha)},$$

so that

(2.3) $$\sum_{\alpha \in \mathrm{GF}(q)} e(\alpha\beta) = \begin{cases} q & (\beta = 0), \\ 0 & (\beta \neq 0). \end{cases}$$

We define

(2.4) $$M(f) = \sum_{\alpha} e(f(\alpha))$$

and

(2.5) $$N_f(\alpha) = N\{f(x) = \alpha\},$$

where the N on the right denotes the number of solutions x of the indicated equation. (2.5) can be expressed in terms of (2.4) by the formula ([2], Theorem 3.3, p. 408)

(2.6) $$M(f) = \sum_{\alpha} e(\alpha) N_f(\alpha).$$

3. Right equivalence.

DEFINITION. Two functions g, h are called *right equivalent* (we write $g\mathrm{R}h$) when there exists a permutation function φ such that

(3.1) $$g\varphi = h.$$

The equivalence relation R separates all functions into *right equivalence classes*, or simply *R-classes*.

THEOREM 3.1. *Let g, h be functions over* GF(q). *Write*

(3.2) $$\Pi_g = \{S_i : i = 1, \ldots, t\}; \quad g(S_i) = \gamma_i \quad (i = 1, \ldots, t),$$

(3.3) $$\Pi_h = \{Q_i : i = 1, \ldots, k\}; \quad h(Q_i) = \delta_i \quad (i = 1, \ldots, k).$$

Then $g\mathrm{R}h$ if and only if

(3.4) $$\{o(S_i)\} \text{ is a permutation of } \{o(Q_i)\},$$

and

(3.5) $$g(S_i) = h(Q_j),$$

where $i = 1, \ldots, t$ and the j's are a permutation of the i's.

Proof. Suppose first that $g\mathrm{R}h$; that is, $g\varphi = h$. We can show easily that $\varphi(Q_i)$ comprises a set in Π_g. Suppose $\alpha, \beta \in Q_i$, while $\varphi(\alpha) \in S_j$ and $\varphi(\beta) \notin S_j$. Then $g\varphi(\alpha) \neq g\varphi(\beta)$ or $h(\alpha) \neq h(\beta)$, which contradicts (3.3). So $\varphi(\alpha), \varphi(\beta) \in S_j$. Next suppose $\alpha \in Q_i$, $\beta \notin Q_i$, while $\varphi(\alpha), \varphi(\beta) \in S_j$. Then $g\varphi(\alpha) = g\varphi(\beta)$, or $h(\alpha) = h(\beta)$, contradicting (3.3). Therefore $\varphi(\alpha)$, $\varphi(\beta)$ belong to a single set S_j if and only if α, β belong to a single set Q_i. Consequently $\varphi(Q_i) \in \Pi_g$ and we write $\varphi(Q_i) = S_i$ for simplicity. This proves (3.4) and (3.5).

The sufficiency of Theorem 3.1 is obvious.

In [2] L. Carlitz defined right equivalence for functions over GF(q) of r variables, $r \geqslant 1$, and described the invariants of R-classes. The remaining theorems in this section will be statements of his results for the case $r = 1$.

THEOREM 3.2. *Let g, h be functions over* GF(q). *Then $g\mathrm{R}h$ if and only if $N_g(\alpha) = N_h(\alpha)$ for all $\alpha \in \mathrm{GF}(q)$, where $N_g(\alpha)$ is defined in* (2.5).

THEOREM 3.3. *$g\mathrm{R}h$ if and only if $M(\beta g) = M(\beta h)$ for all $\beta \neq 0$, where $M(f)$ is defined in* (2.4).

The permutation function φ is called an *R-automorphism of g* if $g\varphi = g$, and the totality of R-automorphisms of g form a group $G = G_g$ of order $\nu(g)$. If $g\varphi = h$, the group of R-automorphisms $G_h = \varphi^{-1}G_g\varphi$, and in particular $\nu(g) = \nu(h)$. Thus the number of R-automorphisms is the same for any function of a fixed class K; accordingly we write $\nu_R(K)$ for this number.

THEOREM 3.4. *The number of R-automorphisms $\nu_R(K)$ of the class K is determined by*

$$\nu_R(K) = \prod_{\alpha} N_K(\alpha)!,$$

where $N_K(\alpha) \equiv N_g(\alpha)$ for any function g in K.

THEOREM 3.5. *The number of functions $\mu_R(K)$ in the class K satisfies*

$$\mu_R(K) \cdot \nu_R(K) = q!.$$

THEOREM 3.6. *The number λ_R of R-classes is given by*

$$\lambda_R = \binom{2q-1}{q-1}.$$

It is convenient to recall Carlitz's definition of a category of functions. Two functions g, h *belong to the same category* if the set of integers $\{N_g(\alpha)\}$ is some permutation of the set $\{N_h(\alpha)\}$. Thus, by Theorem 3.2, if $g\mathrm{R}h$, g and h fall in the same category; in other words, each category consists of R-classes. We shall return to this point in Section 9.

4. Left equivalence.

DEFINITION. Two functions g, h are *left-equivalent* ($g\mathrm{L}h$) if and only if there exists a permutation function φ such that

$$\varphi g = h. \tag{4.1}$$

The equivalence relation L separates all functions into *left-equivalence classes*, or simply *L-classes*.

THEOREM 4.1. *$g\mathrm{L}h$ if and only if $\Pi_g = \Pi_h$.*

Proof. Suppose first that $\Pi_g = \Pi_h$ and write

$$\Pi_g = \{S_i\colon\ i = 1, \ldots, t\}, \tag{4.2}$$

$$g(S_i) = \gamma_i \quad (i = 1, \ldots, t), \tag{4.3}$$

$$h(S_i) = \delta_i \quad (i = 1, \ldots, t). \tag{4.4}$$

If we choose φ to be a permutation function satisfying

$$\varphi(\gamma_i) = \delta_i \quad (i = 1, \ldots, t)$$

then $\varphi g = h$.

Conversely suppose that $\varphi g = h$. If $g(\alpha) = g(\beta)$, then $\varphi g(\alpha) = \varphi g(\beta)$, so $h(\alpha) = h(\beta)$. If $g(\alpha) \neq g(\beta)$, then $\varphi g(\alpha) \neq \varphi g(\beta)$, so $h(\alpha) \neq h(\beta)$.

We might note, using (2.1), that if g satisfies (4.2) and (4.3), then it can be written

$$g(x) = -\sum_{i=1}^{t} \sum_{\alpha \in S_i} \{(x-\alpha)^{q-1} - 1\}\gamma_i.$$

It clearly follows from Theorem 4.1 that if $g\mathrm{L}h$ then the set of integers $\{N_g(\alpha)\}$ is a permutation of the integers $\{N_h(\alpha)\}$. However, we cannot make the stronger statement $N_g(\alpha) = N_h(\alpha)$ for all $\alpha \in \mathrm{GF}(q)$ unless $g = h$. Therefore, $N_g(\alpha)$ is not an L-class invariant.

We can see with a simple counter-example that $M(f)$ is not an L-class invariant. Suppose g, h are constant functions, so that $g\mathrm{L}h$. If $g(\alpha) = \gamma$ and $h(\alpha) = \delta$ for all $\alpha \in \mathrm{GF}(q)$, then

$$N_g(\alpha) = \begin{cases} q & \text{if} \quad \alpha = \gamma, \\ 0 & \text{if} \quad \alpha \neq \gamma, \end{cases} \qquad N_h(\alpha) = \begin{cases} q & \text{if} \quad \alpha = \delta, \\ 0 & \text{if} \quad \alpha \neq \delta. \end{cases}$$

Thus by (2.6)

$$M(g) = \sum_{\alpha} e(\alpha) N_g(\alpha) = e(\gamma) \cdot q$$

and

$$M(h) = \sum_{\alpha} e(\alpha) N_h(\alpha) = e(\delta) \cdot q.$$

Now if γ, δ are chosen so that $e(\gamma) \neq e(\delta)$, then $M(g) \neq M(h)$.

THEOREM 4.2. *For every L-class K we have*

$$\sum_{f \in K} M(f) = 0. \tag{4.5}$$

Proof. First we see that

$$\sum_{f \in K} N_f(\alpha) = \sum_{f \in K} N_f(\beta). \tag{4.6}$$

Using (2.6) and (4.6) we write

$$\sum_{f\in K} M(f) = \sum_{f\in K}\sum_{\alpha} e(\alpha)N_f(\alpha) = \sum_{\alpha} e(\alpha)\sum_{f\in K} N_f(\alpha). \tag{4.7}$$

By (2.3), (4.7) will be 0.

THEOREM 4.3. *If g is a function over* GF(q) *such that* $o(R_g) = t$, *the number* $\mu_L(K)$ *of polynomials in the L-class* K *containing* g *is given by*

$$\mu_L(K) = \frac{q!}{(q-t)!}. \tag{4.8}$$

Proof. By Theorem 4.1 we see that $\mu_L(K)$ equals the number of permutations of q objects t at a time.

THEOREM 4.4. *If* $\lambda_L(q)$ *denotes the number of L-classes of functions over* GF(q), *then* λ_L *is given by*

$$\lambda_L(q) = H(q), \tag{4.9}$$

where $H(q)$ *is defined inductively by*

$$H(q) = \sum_{i=0}^{q-1} \binom{q-1}{i} H(i), \quad H(0) = 1 \tag{4.10}$$

and has the generating function

$$e^{e^x-1} = \sum_{t=0}^{\infty} H(t)x^t/t!. \tag{4.11}$$

Proof. $\lambda_L(q)$ is simply the number of partitions of q objects. See ([1], p. 108) for a statement of (4.10) and (4.11).

DEFINITION. φ is called a *L-automorphism* of g if $\varphi g = g$.

Remark. φ is an L-automorphism of g if and only if $\varphi(a) = a$ for all $a \in R_g$.

THEOREM 4.5. *The totality of L-automorphisms of* g *form a group* $G = G_g$ *of order* $\nu_L(g) = (q-t)!$, *where* $t = o(R_g)$.

Proof. First we show that the set of L-automorphisms forms a group. If $\varphi g = g$, and $\psi g = g$, then $(\varphi\psi)g = g$, hence the set is closed. To show that the inverse of an L-automorphism belongs to the set, we note that if $\varphi g = g$, then $g = \varphi^{-1}g$. Next, regarding the order of the group, we observe that since φ must be an identity on R_g, $\nu_L(g)$ equals the number of permutations on $(q-t)$ letters. This completes the proof.

By Theorems 4.1 and 4.5 we see that $\nu_L(g) = \nu_L(h)$ if gLh. Hence if g belongs to L-class K, and $o(R_g) = t$, we define

$$\nu_L(K) = \nu_L(g) = (q-t)! \tag{4.12}$$

and refer to the number of L-automorphisms of a class.

THEOREM 4.6. *The number* $\nu_L(K)$ *of L-automorphisms of an L-class* K *satisfies*

$$\mu_L(K)\cdot\nu_L(K) = q!. \tag{4.13}$$

Proof. This result follows immediately from (4.8) and (4.12).

THEOREM 4.7. *If* $\varphi g = h$, *then* $G_h = \varphi G_g \varphi^{-1}$.

Proof. Let $\psi \in G_g$ and put $\theta = \varphi\psi\varphi^{-1}$. First we show $\theta \in G_h$. Suppose $a \in R_h$. Since $\varphi^{-1}(R_h) = R_g$,

$$\varphi^{-1}(a) \in R_g.$$

Since $\psi \in G_g$, $\psi\varphi^{-1}(a) = \varphi^{-1}(a)$, so

$$\varphi\psi\varphi^{-1}(a) = \varphi\varphi^{-1}(a) = a.$$

Therefore, $\theta \in G_h$. Next if $\psi_1, \psi_2 \in G_g$, and if $\psi_1 \neq \psi_2$,

$$\varphi\psi_1\varphi^{-1} \neq \varphi\psi_2\varphi^{-1}.$$

Finally, since the order of G_h must equal the order of G_g, every automorphism θ in G_h must be expressible in the form

$$\theta = \varphi\psi\varphi^{-1}, \quad \text{where} \quad \psi \in G_g.$$

5. Weak equivalence.

DEFINITION. Two functions g, h are *weakly equivalent* (gWh) if there exist two permutation functions φ_1, φ_2 such that

$$\varphi_1 g \varphi_2 = h. \tag{5.1}$$

The equivalence relation W separates all functions into *weak equivalence classes*, or simply *W-classes*.

THEOREM 5.1. *Suppose* g *and* h *are functions over* GF(q). *Write*

$$\Pi_g = \{S_i\colon i = 1, \ldots, t\}; \quad g(S_i) = \gamma_i \quad (i = 1, \ldots, t),$$
$$\Pi_h = \{Q_i\colon i = 1, \ldots, r\}; \quad h(Q_i) = \delta_i \quad (i = 1, \ldots, r).$$

Then gWh *if and only if*

(5.2) $\{o(S_i)\colon i = 1, \ldots, t\}$ *is a permutation of* $\{o(Q_i)\colon i = 1, \ldots, r\}$.

Proof. Suppose first that (5.2) holds. Then we may assume, for simplicity, that $o(S_i) = o(Q_i)$, $i = 1, \ldots, t$. If we choose φ_2 to be a permutation function such that

$$\varphi_2(Q_i) = S_i \quad (i = 1, \ldots, t), \tag{5.3}$$

and φ_1 to be a permutation function such that

$$\varphi_1(\gamma_i) = \delta_i \quad (i = 1, \ldots, t), \tag{5.4}$$

then

$$\varphi_1 g \varphi_2 = h.$$

Conversely if we suppose that $g \mathrm{W} h$, then it is obvious that (5.2) holds.

THEOREM 5.2. *The number λ_W of W-classes is*

$$\lambda_W = \sum_{i=1}^{q} p_i(q) = p(q), \tag{5.5}$$

where $p_i(q)$ denotes the number of partitions of q with exactly t parts, and $p(q)$ denotes the number of unrestricted partitions of q.

Proof. The number of W-classes of functions f such that

$$o(R_f) = t \quad (1 \leqslant t \leqslant q)$$

is equal to $p_t(q)$, where $p_t(q)$ is defined above. It is clear then that (5.5) holds.

DEFINITION. Suppose that Π is a partition consisting of t sets, $1 \leqslant t \leqslant q$, and that exactly k_i are of order m_i, $i = 1, \ldots, r$. Then we say that Π induces the number partition

$$q = k_1 m_1 + \ldots + k_r m_r, \tag{5.6}$$

where $m_1 > m_2 > \ldots > m_r \geqslant 1$, $k_1, \ldots, k_r \geqslant 1$, $k_1 + \ldots + k_r = t$.

We notice that if f belongs to W-class K, then the number partition induced by Π_f actually characterizes K. That is, a function g belongs to K if and only if Π_g and Π_f induce the same number partition.

THEOREM 5.3. *Suppose a W-class K is defined by the number partition* (5.6). *Then the number $\mu_W(K)$ of functions in K is*

$$\mu_W(K) = \frac{(q!)^2}{(q-t)! \prod_{i=1}^{r} (m_i!)^{k_i} \prod_{i=1}^{r} (k_i!)}. \tag{5.7}$$

Proof. Let $\prod$ denote the family of partitions such that $\Pi \in \prod$ provided $\Pi = \Pi_f$ for some function $f \in K$. The number of partitions in $\prod$ is

$$\frac{q!}{\prod_{i=1}^{r} (m_i!)^{k_i} \prod_{i=1}^{r} k_i!}.$$

Now the number of functions f such that $\Pi_f = \Pi$ equals $q!/(q-t)!$, the number of permutations of q things t at a time. Hence the total number of functions in the W-class defined by (5.6) is given by (5.7).

DEFINITION. A pair (φ_1, φ_2) of permutation functions is called a *W-automorphism* of g if $\varphi_1 g \varphi_2 = g$.

THEOREM 5.4. *If g belongs to the W-class K defined by* (5.6), *the number $\nu_W(g)$ of W-automorphisms of g is given by*

$$(q-t)! \prod_{i=1}^{r} k_i! (m_i!)^{k_i}. \tag{5.8}$$

Proof. A necessary condition for a permutation function φ_2 to satisfy $\varphi_1 g \varphi_2 = g$ is that φ_2 map a set of order m_i onto a set of equal order. Since there are $m_i!$ ways to map a fixed set of order m_i onto a fixed set of equal order, and $k_i!$ ways to permute k_i objects, there are altogether

$$\prod_{i=1}^{r} k_i! (m_i!)^{k_i}$$

choices for φ_2. Having chosen φ_2, we see there are $(q-t)!$ choices for φ_1, since φ_1 is chosen only to map a set of order $(q-t)$ onto a set of equal order. (5.8) follows immediately.

THEOREM 5.5. *If K is an arbitrary W-class, we have*

$$\mu_W(K) \cdot \nu_W(K) = (q!)^2. \tag{5.9}$$

Proof. This result follows immediately from (5.7) and (5.8).

Recalling now the definition of a category (at the end of Section 3), we note that a W-class is a category. Therefore a W-class consists of R-classes. We shall discuss this point in some detail in Section 9.

6. Similarity.

DEFINITION. Two functions g, h are *similar* ($g \mathrm{A} h$) if there exists a permutation function φ such that

$$\varphi^{-1} g \varphi = h. \tag{6.1}$$

The equivalence relation A separates all functions into *similarity classes*, or simply *A-classes*.

THEOREM 6.1. *Suppose g, h are functions over* GF(q). *Write*

$$\begin{aligned} &\Pi_g = \{S_i\colon\ i = 1, \ldots, t\}; \quad g(S_i) = \gamma_i \quad (i = 1, \ldots, t), \\ &\Pi_h = \{Q_i\colon\ i = 1, \ldots, r\}; \quad h(Q_i) = \delta_i \quad (i = 1, \ldots, r). \end{aligned} \tag{6.2}$$

$g \mathrm{A} h$ if and only if

(6.3) *$\{o(S_i)\colon\ i = 1, \ldots, t\}$ is a permutation of $\{o(Q_i)\colon\ i = 1, \ldots, r\}$.*

(6.4) *There is a one-one correspondence between sets of equal order in Π_h and Π_g (as a convention write $Q_i \leftrightarrow S_i$) such that if $\delta_k \in Q_i$, then $\gamma_k \in S_i$.*

Proof. To prove sufficiency, we suppose that $o(S_i) = o(Q_i)$, $i = 1, \ldots, t$. Choose φ to be a permutation function such that

$$\varphi(Q_i) = S_i, \quad \varphi(\delta_i) = \gamma_i \quad (i = 1, \ldots, t). \tag{6.5}$$

By (6.3) and (6.4) it is clear we can choose such a function. We have then that

$$\varphi(Q_i) = S_i, \quad g(S_i) = \gamma_i, \quad \varphi^{-1}(\gamma_i) = \delta_i \quad \text{and} \quad h(Q_i) = \delta_i.$$

We prove next that (6.3) and (6.4) are necessary conditions for $g\mathrm{A}h$. Since similarity is a special case of weak equivalence, (6.3) is necessary. To show (6.4) is necessary, we observe first that φ maps a set Q_i onto a set S_i of equal order. That is, suppose $\alpha, \beta \in Q_i$. If $\varphi(\alpha) \in S_i$ while $\varphi(\beta) \notin S_i$, then $g\varphi(\alpha) \neq g\varphi(\beta)$. Since φ is a permutation function, $\varphi^{-1}g\varphi(\alpha) \neq \varphi^{-1}g\varphi(\beta)$, which contradicts the fact that $h(\alpha) = h(\beta)$. Similarly we can show that if $\varphi(\alpha)$ and $\varphi(\beta) \in S_i$, then $\alpha, \beta \in Q_i$. Therefore, $\varphi(Q_i) = S_i$. Finally, if $\varphi^{-1}g\varphi = h$ is to hold, we see that $\varphi^{-1}(\gamma_k) = \delta_k$; that is, $\varphi(\delta_k) = \gamma_k$. This evidently completes the proof.

Determining the number λ_A of A-classes is essentially the following unsolved problem about permutations: Suppose $Z_N = \{1, 2, \ldots, N\}$ and that g, h are functions from Z_N into Z_N. If $h = p^{-1}gp$, where p is a permutation of Z_N, we say g and h are in the same class. The problem is: what is the total number of classes into which the N^N functions f: $Z_N \to Z_N$ are separated?

7. Strong equivalence.

Definition. Two functions g, h are *strongly equivalent* ($g\mathrm{S}h$) if there exist two permutation functions φ_1, φ_2 such that

$$\varphi_1 g = h; \quad g\varphi_2 = h. \tag{7.1}$$

The equivalence relation S separates all functions into *strong-equivalence classes*, or simply *S-classes*.

Theorem 7.1. *If g, h are functions over* GF(q), $g\mathrm{S}h$ *if and only if*

$$\Pi_g = \Pi_h \tag{7.2}$$

and

$$N_g(\alpha) = N_h(\alpha) \quad \textit{for all } \alpha \in \mathrm{GF}(q). \tag{7.3}$$

Proof. This theorem follows immediately from Theorems 3.2 and 4.1, which give necessary and sufficient conditions for right-equivalence and left-equivalence.

Recalling (5.6), we might point out an important difference between W-classes and S-classes. If f belongs to S-class K, and Π_f induces a number partition, then that number partition does not characterize K. In fact, there are generally several S-classes all of whose members induce the same number partition.

Theorem 7.2. *If K is an S-class containing g, and Π_g induces the number partition* (5.6), *the number $\mu_S(K)$ of functions in K is*

$$\mu_S(K) = \prod_{i=1}^{r} k_i!. \tag{7.4}$$

Proof. Put

$$R_g/m_i = \{\alpha: \ \alpha \in R_g, \ o(g^{-1}(\alpha)) = m_i\}. \tag{7.5}$$

By (7.3) we see that

$$\mu_S(K) = \prod_{i=1}^{r} o(R_g/m_i)!. \tag{7.6}$$

Since $o(R_g/m_i)$ clearly equals k_i, (7.8) yields (7.6).

Theorem 7.3. *The number λ_S of S-classes is given by*

$$\lambda_S = \sum \frac{(q!)^2}{(q-t)! \prod_{i=1}^{r} (m_i!)^{k_i} \prod_{i=1}^{r} (k_i!)^2}, \tag{7.7}$$

where the summation is over all number partitions of the form (5.6).

Proof. First suppose that Π is a partition that induces the number partition (5.6). The number of S-classes among the functions f such that $\Pi_f = \Pi$ is

$$\frac{p(q, t)}{k_1! \ldots k_r!}, \tag{7.8}$$

where $p(q, t)$ is the number of permutations of q objects t at a time. Next, the number of partitions Π which induce the number partition (5.6) equals

$$\frac{q!}{\prod_{i=1}^{r} (m_i!)^{k_i} \prod_{i=1}^{r} k_i!}, \tag{7.9}$$

which is essentially the number of ways of arranging q things in t sets of which k_i have order m_i ($i = 1, \ldots, r$), not allowing permutations of sets of equal order. Finally, summing over all number partitions (5.6), we have (7.7).

It might be mentioned that if gSh and $k_1 = k_2 = \ldots = k_r = 1$, then $g = h$. This follows from (7.4), since $\mu_s(K) = 1$; that is, the S-class containing g consists of only one function.

From (7.4) and (7.7) it follows that we have the equality

$$\sum \frac{(q!)^2}{(q-t)! \prod_{i=1}^{r} (m_i!)^{k_i} \prod_{i=1}^{r} (k_i)!} = q^q, \tag{7.10}$$

where the summation extends over all number partitions of the form (5.6). This fact can be verified directly by using generating functions. Consequently we have a check for (7.4) and (7.7), since

$$\sum_K \mu_S(K) = q^q,$$

where K runs over all S-classes. We also have a check for (5.7), since

$$\sum_K \mu_W(K) = q^q,$$

where K runs over all W-classes.

8. Illustrations. Let $W(g)$ denote the W-class of an arbitrary function, and $A(g)$, its A-class. Clearly $A(g) \subseteq W(g)$, and in general, $A(f) \subseteq W(g)$ if $f \in W(g)$. Now suppose there is a function $h \in W(g)$ such that $h \notin A(g)$. Then $A(h) \cap A(g)$ is empty, for if there were functions φ, ψ such that

$$\psi^{-1} h \psi = \varphi^{-1} g \varphi,$$

then we should have

$$h = \psi\varphi^{-1} g \varphi\psi^{-1} \quad \text{or} \quad h = \eta^{-1} g \eta \quad (\eta = \varphi\psi^{-1})$$

which implies $h \in A(g)$, a contradiction. Suppose next there is a function $h_1 \in W(g)$ such that $h_1 \notin A(g)$, $h_1 \notin A(h)$. Then we prove as above that $A(h_1)$ is disjoint from both $A(g)$ and $A(h)$. Continuing this process, we see that $W(g)$ can be decomposed completely into disjoint A-classes:

$$W(g) = A(g) \cup A(h_1) \cup \ldots \cup A(h_k). \tag{8.1}$$

Using similar arguments we can prove that a W-class can be decomposed into disjoint R-classes, and also into disjoint L-classes. By means of the partition criteria for various types of equivalence, we can prove that both R-classes and L-classes can be decomposed into S-classes.

We illustrate these relations with the following chart:

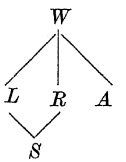

Fig. 1

As an immediate result of the previous discussion, we state

THEOREM 8.1. *For every W-class K, we have*

$$\sum_{f \in K} M(f) = 0. \tag{8.2}$$

Proof. Since K can be decomposed into L-classes $K_1, \ldots, K_r$, we write

$$\sum_{f \in K} M(f) = \sum_{i=1}^{r} \sum_{f \in K_i} M(f). \tag{8.3}$$

By Theorem 4.2 the inner sum vanishes; that is, the sum of $M(f)$ over an L-class is 0.

It might be of interest to note, as an example, that the set of permutation functions comprises an equivalence class with respect to weak, left, right, and strong equivalence. In other words the decomposition of the W-class of permutation functions into L, R, and S-classes is a trivial one.

If we choose the W-class consisting of all constant functions, we can describe the decomposition precisely, according to the pattern of Figure 1:

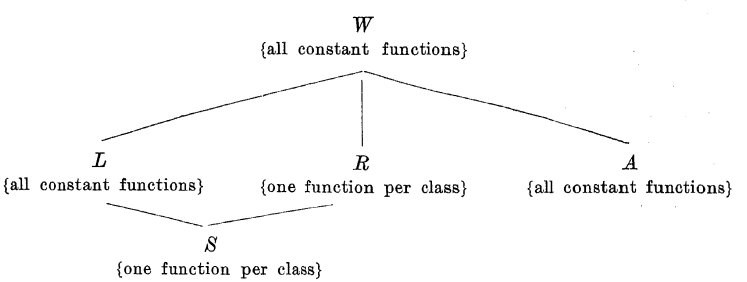

Fig. 2

We might mention, as another type of example, that over a field of characteristic $p > 2$ and order $q > 3$ all quadratics belong to, but do not exhaust, a single W-class. To prove this, we suppose f, g are quadratic. Then $\{N_f(a)\}$ is a permutation of $\{N_g(a)\}$, hence fWg. To find a function of degree greater than 2 that belongs to the class containing the quadratics, we choose a function $h = \varphi g$, where φ is a monomial permutation function of degree m, and $(m, q-1) = 1$.

It might be of interest to note, in connection with this last example, that the set of quadratics is the only set consisting of all the functions of some fixed degree k $(2 \leqslant k \leqslant q-1)$ over GF(q) (q odd) which belong to a single W-class. The proof of this fact proceeds by showing that if f and g are arbitrary functions of degree $k > 2$, $\{N_f(a)\}$ is not necessarily a permutation of $\{N_g(a)\}$. Suppose m is an integer such that $2 \leqslant m \leqslant q-1$, and put $d = (m, q-1)$. It is a familiar result ([3], p. 45, Theorem 63) that GF(q) contains $(q-1)/d$ mth powers. Therefore, if $f(x) = x^m$, Π_f consists of $(q-1)/d$ sets each containing d numbers, and a single set with one number. Let us assume, as case 1, that $d < m$. If we put

$$g(x) = \prod_{i=1}^{m} (x - \alpha_i),$$

where $\alpha_1, \ldots, \alpha_m$ are distinct numbers of GF(q), then Π_g contains a set with m numbers. However, since $d < m$, there is no set of order m in Π_f.

Suppose, as case 2, that $d = m$. Then Π_f consists of $(q-1)/m$ sets each with m numbers, and a single set with one number. If we put

$$h(x) = (x-\alpha_1)^r (x-\alpha_2)^s \qquad (r+s = m)$$

Π_h contains a set of order 2. Therefore, if $m > 2$, f and h are not weakly equivalent. This evidently completes the proof. The fact that the argument breaks down for $m = 2$ agrees with our earlier result about quadratics.

Over a field of characteristic 2 it is also true, by the last argument, that the functions of degree $k > 2$ do not all belong to a single W-class. Furthermore, neither do the quadratics, since x^2 permutes GF(2^n) and $x^2 - x$ does not. Therefore the set of linear functions is the only set consisting of all the functions of some fixed degree over GF(2^n) which belong to a single W-class.

9. Functional equations.

THEOREM 9.1. *Let f be a function over* GF(q) *and suppose that* $\Pi_f = \{S_i : i = 1, \ldots, t\}$. *Then a function g will satisfy*

$$fg = f \tag{9.1}$$

if and only if

$$g(S_i) \subseteq S_i \qquad (i = 1, \ldots, t). \tag{9.2}$$

Furthermore if $o(S_i) = n_i$, $i = 1, \ldots, t$, the number N of solutions g is given by

$$N = \prod_{i=1}^{t} n_i^{n_i}. \tag{9.3}$$

Proof. The sufficiency of Theorem 9.1 is obvious. The necessity follows by noting that if $\alpha \in S_i$ and $g(\alpha) \notin S_i$, then $fg(\alpha) \neq f(\alpha)$.

We prove (9.3) by recalling that a set of order n_i can be mapped into itself in $n_i^{n_i}$ ways.

If g_1, g_2 are solutions of (9.1), then $g_1 g_2$ is also a solution. Therefore we see that the solutions of (9.1) comprise a semi-group.

THEOREM 9.2. *Let f be a function over* GF(q). *Then a function g will satisfy the equation*

$$gf = f \tag{9.4}$$

if and only if g is an identity on R_f. Furthermore, if $o(R_f) = t$, the number $\overline{N}$ of solutions g is given by

$$\overline{N} = q^{q-t}. \tag{9.5}$$

Proof. The necessary and sufficient conditions and the formula are obvious.

We might note, using (2.1), that when (9.4) holds,

$$g(x) = -\sum_{a \in R_f} \{(x-a)^{q-1} - 1\} a - \sum_{a \notin R_f} \{(x-a)^{q-1} - 1\} g(a) = x + m(x).$$

Since each $a \in R_f$ is a root of $m(x)$, we see that

$$s(x) \equiv \prod_{a \in R_f} (x - a)$$

divides $m(x)$. Therefore,

$$g(x) = x + s(x) \cdot n(x). \tag{9.6}$$

THEOREM 9.3. *A function f will satisfy*

$$ff = f \tag{9.7}$$

if and only if f is an identity on R_f. Furthermore, the number N' of such functions is

$$N' = \sum_{i=1}^{q} \binom{q}{i} i^{q-i}. \tag{9.8}$$

Proof. The necessary and sufficient conditions follow from Theorem 9.2, since $ff = f$ is a special case of $gf = f$.

To prove (9.8) we will specify a set R of numbers, determine which functions have range R, and then sum over all possible ranges. Suppose then, that R contains exactly i numbers. By the first result of this theorem, the restriction of f to R_f is the identity, and the restriction of f to $\mathrm{GF}(q) \sim R_f$ is arbitrary; that is, f can map $\mathrm{GF}(q) \sim R_f$ into $\mathrm{GF}(q)$ in i^{q-1} ways. Since there are $\binom{q}{i}$ subsets of $\mathrm{GF}(q)$ of order i, there are

$$\binom{q}{i} i^{q-i}$$

functions f, subject to $o(R_f) = t$, which satisfy (9.7). Summing over all possible range lengths, we see there are

$$N' = \sum_{i=1}^{q} \binom{q}{i} i^{q-i}$$

functions over $\mathrm{GF}(q)$ which satisfy (9.7).

THEOREM 9.4. *Let f, h be functions over $\mathrm{GF}(q)$. A necessary and sufficient condition for the existence of a function g such that*

$$fg = h \tag{9.9}$$

is that $R_f \supseteq R_h$.

Proof. This condition is obviously necessary. To prove it is sufficient, we suppose $R_f \supseteq R_h$ and write

$$\Pi_f = \{S_i\colon i = 1, \ldots, t+k\}, \quad \Pi_h = \{Q_i\colon i = 1, \ldots, t\},$$

$$f(S_i) = h(Q_i) \quad (i = 1, \ldots, t).$$

If we choose g to be a function such that

$$g(Q_i) \subseteq S_i \quad (i = 1, \ldots, t)$$

then g will satisfy (9.9).

It might be of interest to note, in connection with Theorem 9.4, that if f and h satisfy (9.9) and h is a permutation function, then f must be a permutation function, and therefore g must be one. We might also mention, again to illustrate Theorem 9.4, that if $N_f(\alpha) = N_h(\alpha)$ for all $\alpha \in \mathrm{GF}(q)$, thereby implying $R_f \supseteq R_h$, then a permutation function g will satisfy (9.9). This follows from Theorem 3.2.

THEOREM 9.5. *If h is a function over $\mathrm{GF}(q)$, and $o(R_h) = t$, the number N^* of functions f for which there is a solution g to (9.9) is*

$$N^* = \sum_{j=0}^{q-t} \binom{q-t}{j} \sum_{i=0}^{t+j} (-1)^i \binom{t+j}{i} (t+j-i)^q. \tag{9.10}$$

Proof. By Theorem 9.4 there is a solution g to (9.9) if and only if $R_f \supseteq R_h$. Therefore we will pick a set $S \supseteq R_h$, count the functions whose range is S, and sum over S.

Accordingly we choose a set S such that

$$S \supseteq R_h, \quad o(S) = o(R_h) + j, \quad 0 \leqslant j \leqslant q-t. \tag{9.11}$$

The number of functions from $\mathrm{GF}(q)$ onto S is given by

$$\sum_{i=0}^{t+j} (-1)^i \binom{t+j}{i} (t+j-i)^q.$$

Since there are $\binom{q-t}{j}$ sets which satisfy (9.11), the number of functions f such that

$$R_f \supseteq R_h, \quad o(R_f) = o(R_h) + j$$

is

$$\binom{q-t}{j} \sum_{i=0}^{t+j} (-1)^i \binom{t+j}{i} (t+j-i)^q.$$

Summing over j yields (9.10).

DEFINITION. Suppose g and h are functions over $\mathrm{GF}(q)$. Π_g is said to be *finer* than Π_h if each set in Π_h is a union of sets in Π_g.

THEOREM 9.6. *Let g and h be functions over $\mathrm{GF}(q)$. A necessary and sufficient condition for the existence of a function f such that*

$$fg = h \tag{9.12}$$

is that Π_g be finer than Π_h.

Proof. Write

$$\Pi_g = \{S_i\colon i = 1, \ldots, t\}; \quad g(S_i) = \gamma_i \quad (i = 1, \ldots, t),$$
$$\Pi_h = \{Q_i\colon i = 1, \ldots, r\}; \quad h(Q_i) = \delta_i \quad (i = 1, \ldots, r).$$

To prove the necessity, we suppose $\alpha, \beta \in S_i$ and that $\alpha \in Q_j$ but $\beta \notin Q_j$. We have then that $g(\alpha) = g(\beta)$ and $h(\alpha) \neq h(\beta)$. Therefore there can be no function f satisfying (9.12).

Suppose now that Π_g is finer than Π_h. Then

$$Q_i = \bigcup_{J(i)} S_j \quad (i = 1, \ldots, r)$$

where $J(i)$ is an index set depending on i. If we define a function f by specifying that on R_g

$$f(\gamma_j) = \delta_i \quad (j \in J(i),\ i = 1, \ldots, r)$$

and by allowing f to be arbitrary elsewhere, then f will satisfy (9.12).

References

[1] G. Birkhoff, *Lattice Theory*, New York 1948.

[2] L. Carlitz, *Invariantive theory of equations in a finite field*, Trans. Amer. Math. Soc. 75 (1953), pp. 405-427.

[3] L. E. Dickson, *Linear Groups with an Exposition of the Galois Field Theory*, Leipzig 1901.

STATE UNIVERSITY OF NEW YORK, BUFFALO

Reçu par la Rédaction le 29. 5. 1963

ACTA ARITHMETICA
X (1964)

On the abstract theory of primes I

by

E. Fogels (Riga)

Introduction. 1. For a semi-group $\mathfrak{G}$ (with respect to multiplication) of real numbers $a \geqslant 1$ satisfying some given asymptotical laws of distribution Beurling [2] investigated the asymptotical distribution of the generators b of $\mathfrak{G}$. He proved a general theorem which, applied to the semi-group of natural integers, gives the prime number theorem of Hadamard and Vallée-Poussin (1). Forman and Shapiro [11] divided the numbers a into classes H_i $(1 \leqslant i \leqslant h)$ forming a group K (for any $a \in H_i$ and $a' \in H_j$ we have $aa' \in H_k$ where k depends only on i and j) and satisfying

$$\sum_{x \geqslant a \in H_i} 1 = \alpha_i x + O(x^{1-\vartheta}) \tag{1}$$

with some positive constants α_i, ϑ $(\vartheta \leqslant 1)$. They proved that under those circumstances the numbers $\pi(x, H_i)$ of the generators $b \leqslant x$, $b \in H_i$ are asymptotically the same for all the classes H_i forming a sub-group K_0 of K, whereas the number of the remaining generators $\leqslant x$ (if $K_0 \neq K$) has a smaller order of magnitude as $x \to \infty$ (2). As special cases of this abstract theorem we may deduce the asymptotical laws for primes in arithmetical progressions or prime ideals in ideal classes.

The aim of all the work in the abstract theory of primes up to now has been the proof of the asymptotical law for $\pi(x, H)$. In a short note [9] I have mentioned that in the abstract scheme used by Forman and Shapiro one can treat the smallest prime problem for different progressions simultaneously. For this purpose it is necessary to change the

---

(1) Other writers after Beurling (as Nyman [16], Erdös [3]) either start from different conditions or use, instead of the analytical method of the zeta function, the elementary method of A. Selberg.

(2) This is an intentionally simplified description. Actually Forman and Shapiro start from a free Abelian group G on a countable number of generators and use a homomorphism into positive rationals such that the images of the generators are all integral. The distribution of the generators in the classes H of a semi-group is also the subject of a recent work of Amitsur [1], who replaces the remaining term in (1) by $O(x/\log^c x)$.