BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 83, Number 2, March 1977

FUNCTIONS AND CORRESPONDENCES IN A FINITE FIELD

BY L. CARLITZ[1]

1. Introduction. It is well known that any function from a finite field into itself can be represented by a polynomial with coefficients in the field. More precisely, if the field is of order q, then the function is represented by a *unique* polynomial of degree less than q. Conversely, any field with the property that any function from the field into itself can be represented by a polynomial with coefficients in the field, is necessarily finite **[14]**. It has been proved recently **[1]**, **[16]** that if a ring R with identity has the property that any function from R into itself can be represented by a *generalized* polynomial, then R is isomorphic to the matric ring $(\mathrm{GF}(q))_n$, for some prime power q and some $n \geqslant 1$. As customary, we denote by $\mathrm{GF}(q)$ the finite field of order q. By a generalized polynomial is meant a sum of multinomials of the form

$$a_0x^{e_1}a_1x^{e_2}\cdots a_{k-1}x^{e_k}a_k,$$

where $a_i \in R$, $e_i > 0$ and k is arbitrary.

With every function f from $F_q = GF(q)$ into itself we may associate a set of numbers $a_1, a_2, \ldots, a_k \in F_q$ and a partition **[5]**–**[8]**, **[13]**

$$F_q = A_1 \cup A_2 \cup \cdots \cup A_k, \tag{1.1}$$

where

$$A_i \cap A_j = \varnothing \qquad (i \neq j), \tag{1.2}$$

the sets A_i are nonvacuous and

$$f(b_i) = a_i \qquad (b_i \in A_i;\ i = 1, 2, \ldots, k). \tag{1.3}$$

For example, for the function $f(x) = x^{q-1}$, we have $k = 2$, $a_1 = 0$, $a_2 = 1$, $A_1 = \{0\}$, $A_2 = \{a | a \in F_q,\ a \neq 0\}$. On the other hand, for the function $f(x) = x^{q-2}$, $k = q$ and each A_i consists of a single element. Thus x^{q-2} is a *permutation function*. Clearly, for any permutation function, the number of sets A_i in the partition (1.1) is equal to q.

We can generalize the above in the following way. Let

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k \tag{1.4}$$

denote partitions of F_q. It is assumed that each of the sets

$$A_1, \ldots, A_k, \quad B_1, \ldots, B_k \tag{1.5}$$

is nonvacuous; however A_0, B_0 are unrestricted. Then (by the Lagrange interpolation formula for several variables) there exists a polynomial **[9]** $f(x, y) \in F_q[x, y]$ such that

An address delivered to the American Mathematical Society in Tallahassee, Florida, March 4, 1976; received by the editors April 22, 1976.

AMS (MOS) subject classifications (1970). Primary 12C05.

Key words and phrases. Finite fields, functions, correspondences.

[1] Supported in part by NSF grant GP-37924X.

$$f(a,b) = \begin{cases} 0 & (a \in A_i, b \in B_i, 1 \leqslant i \leqslant k), \\ 1 & (\text{otherwise}). \end{cases} \tag{1.6}$$

We shall say that the polynomial $f(x,y)$ *characterizes* the *correspondence* Γ induced by the partitions (1.4); the integer k is called the *rank* of the correspondence.

A polynomial $h(x,y) \in F_q[x,y]$ is said to be *admissible* for the correspondence Γ defined by (1.4) if it satisfies

$$\begin{aligned} h(a,b) &= 0 \qquad (a \in A_i, b \in B_i, 1 \leqslant i \leqslant k), \\ &\neq 0 \qquad (\text{otherwise}). \end{aligned} \tag{1.7}$$

A polynomial is admissible if it is *admissible* for some correspondence.

It follows at once that if $h(x,y)$ is admissible for Γ then

$$f(x,y) = (h(x,y))^{q-1} \tag{1.8}$$

satisfies (1.6).

It is to be understood that (1.8) asserts that the two *functions* are equal; the precise relationship between the polynomials is

$$f(x,y) \equiv (h(x,y))^{q-1} \qquad (x^q - x, y^q - x).$$

As an example of an admissible polynomial consider $h(x, y) = x^{q-1} - y^{q-1}$. It is easily verified that $k = 2$, $A_0 = B_0 = \varnothing$, $A_1 = B_1 = \{0\}$, $A_2 = B_2 = F_q \setminus \{0\}$.

As a second example, the polynomial $h(x, y) = 1 - x^{q-1}y^{q-1}$ is also admissible. In this example $k = 1$, $A_0 = B_0 = \{0\}$, $A_1 = B_1 = F_q \setminus \{0\}$.

As example of a polynomial that is not admissible (for any correspondence) we cite

$$h(x,y) = xy. \tag{1.9}$$

A basic problem is to characterize all admissible polynomials. This is apparently a difficult problem. For example consider correspondences of rank $k = q$, so that each of the sets $A_1, \ldots, A_q$, $B_1, \ldots, B_q$ consists of a single element, while A_0, B_0 are vacuous. An admissible polynomial for this correspondence is evidently $h_1(x, y) = y - \psi(x)$, where $\psi(x)$ denotes some permutation polynomial. Another admissible polynomial for the same correspondence is given by $h_2(x,y) = x - \psi^{-1}(y)$, where ψ^{-1} denotes the inverse of the permutation defined by ψ.

If $f(x)$, $g(x)$ are arbitrary polynomials in $F_q[x]$, it is not difficult to show that

$$h(x,y) = f(x) - g(y) \tag{1.10}$$

is admissible for some correspondence. Conversely, given any correspondence of rank $\neq q - 1$, it has been proved that there exists an admissible polynomial of the form (1.10). For rank $q - 1$, however, an admissible polynomial of this type does not exist when $A_0 \neq \varnothing$, $B_0 \neq \varnothing$; this is, in fact, the only exceptional case.

The definition of a correspondence can be extended in several directions. In the first place, instead of (1.4), we may consider the three partitions of F_q:

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k; \quad C_0, C_1, \ldots, C_k, \tag{1.11}$$

where

$$A_1, \ldots, A_k, \quad B_1, \ldots, B_k, \quad C_1, \ldots, C_k \tag{1.12}$$

are nonvacuous while A_0, B_0, C_0 are arbitrary. There exists a polynomial $f(x, y, z) \in F_q[x, y, z]$ such that

$$f(a, b, c) = \begin{cases} 0 & (a \in A_i, b \in B_i, c \in C_i, 1 \leqslant i \leqslant k), \\ 1 & (\text{otherwise}). \end{cases} \tag{1.13}$$

The polynomial $f(x, y, z)$ is said to characterize the correspondence defined by (1.11).

A polynomial $h(x, y, z) \in F_q[x, y, z]$ is *admissible* for the correspondence defined by (1.11) provided

$$\begin{aligned} h(a, b, c) &= 0 \quad && (a \in A_i, b \in B_i, c \in C_i, 1 \leqslant i \leqslant k), \\ &\neq 0 && (\text{otherwise}). \end{aligned} \tag{1.14}$$

It follows that $h(x, y, z)$ is admissible for the correspondence defined by (1.11) if and only if

$$(h(x, y, z))^{q-1} = f(x, y, z), \tag{1.15}$$

where $f(x, y, z)$ satisfies (1.13).

For brevity the correspondence defined by (1.4) may be called a (1, 1) correspondence, the correspondence defined by (1.11) a (1, 1, 1) correspondence. In either case k is the *rank* of the correspondence.

In the next place let F_q^m denote the direct product of m copies of F_q. Consider the partitions

$$F_q^m = A_0 \cup A_1 \cup \cdots \cup A_k, \qquad F_q^n = B_0 \cup B_1 \cup \cdots \cup B_k, \tag{1.16}$$

where

$$A_1, \ldots, A_k, \quad B_1, \ldots, B_k \tag{1.17}$$

are nonvacuous while A_0, B_0 are arbitrary. There exists a polynomial

$$f(\mathbf{x}, \mathbf{y}) \in F_q[\mathbf{x}, \mathbf{y}],$$

where $\mathbf{x} = (x_1, \ldots, x_m)$, $\mathbf{y} = (y_1, \ldots, y_n)$ such that

$$f(\mathbf{a}, \mathbf{b}) = \begin{cases} 0 & (\mathbf{a} \in A_i, \mathbf{b} \in B_i, 1 \leqslant i \leqslant k), \\ 1 & (\text{otherwise}). \end{cases} \tag{1.18}$$

The polynomial $f(\mathbf{x}, \mathbf{y})$ is said to characterize the correspondence defined by (1.16). The correspondence defined by (1.16) may be called an (m, n) correspondence.

A polynomial $h(\mathbf{x}, \mathbf{y}) \in F_q[\mathbf{x}, \mathbf{y}]$ is admissible for the correspondence defined by (1.17) provided

$$\begin{aligned} h(\mathbf{a}, \mathbf{b}) &= 0 \quad && (\mathbf{a} \in A_i, \mathbf{b} \in B_i, 1 \leqslant i \leqslant k), \\ &\neq 0 && (\text{otherwise}). \end{aligned} \tag{1.19}$$

Hence, $h(\mathbf{x}, \mathbf{y})$ is admissible for the correspondence (1.16) if and only if

$$(h(\mathbf{x}, \mathbf{y}))^{q-1} = f(\mathbf{x}, \mathbf{y}). \tag{1.20}$$

It is evident how the notion of correspondence can be extended to r-fold partitions:

$$F_q^{m_i} = A_{i0} \cup A_{i1} \cup \cdots \cup A_{ik} \qquad (i = 1, 2, \ldots, r). \tag{1.21}$$

A correspondence defined in this way may be called an $(m_1, m_2, \ldots, m_r)$ correspondence. Characteristic and admissible polynomials are defined in the obvious way.

The object of the present paper is to discuss some basic properties of correspondences. For the most part we shall confine ourselves to (1, 1) correspondences. Also we shall usually state results without proof. For fuller details the reader is referred to [**2**], [**3**].

The reader may find it helpful to refer to the numerous examples of correspondences given in §§3, 10.

2. Preliminaries.

Lemma 2.1. *Let A denote an arbitrary nonvacuous subset of F_q. The polynomial*

$$L_A(x) = \sum_{a \in A} \{1 - (x - a)^{q-1}\} \tag{2.1}$$

satisfies

$$L_A(a) = \begin{cases} 1 & (a \in A), \\ 0 & (a \not\in A). \end{cases} \tag{2.2}$$

Let

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k \tag{2.3}$$

denote partitions of F_q such that $A_1, \ldots, A_k$, $B_1, \ldots, B_k$ are nonvacuous while A_0, B_0 are arbitrary.

Theorem 2.2. *There exists a polynomial $f(x, y) \in F_q[x, y]$ such that*

$$f(a, b) = \begin{cases} 0 & (a \in A_i, b \in B_i, 1 \leqslant i \leqslant k), \\ 1 & (\textit{otherwise}). \end{cases} \tag{2.4}$$

Proof. Put

$$g(x,y) = \sum_{i=1}^{k} L_{A_i}(x) L_{B_i}(y),$$

where $L_A(x)$, $L_B(y)$ are defined by (2.1). Then

$$g(a, b) = \begin{cases} 1 & (a \in A_i, b \in B_i, 1 \leqslant i \leqslant k), \\ 0 & (\text{otherwise}). \end{cases}$$

It follows that $f(x, y) = 1 - g(x, y)$ satisfies (2.4).

We have already defined characteristic and admissible polynomials. We now state a few properties of admissible polynomials that follow immediately from the definition. In the first place, as stated in the Introduction, $h(x, y)$ is admissible for the correspondence (2.3) if and only if $(h(x, y))^{q-1} = f(x, y)$, where $f(x, y)$ satisfies (2.4).

If $h(x, y)$ is admissible for some correspondence Γ, and $g(x, y)$ is a polynomial $\in F_q[x, y]$ that never vanishes, then $g(x, y)h(x, y)$ is also admissible for Γ. Indeed if $h(x, y)$ is admissible for Γ, then the polynomial $h_1(x, y)$ is also admissible for Γ if and only if there exists some $g(x, y)$ that never vanishes such that

$$h_1(x, y) = g(x, y)h(x, y). \tag{2.5}$$

If $h(x, y)$ is admissible for Γ and $\phi(x)$, $\psi(y)$ are permutation polynomials such that each A_i is carried into itself by $\phi(x)$ and each B_i is carried into itself by $\psi(y)$, $0 \leqslant i \leqslant k$, then the polynomial $h_1(x, y) = h(\phi(x), \psi(y))$ is also admissible for Γ.

If $h(x, y)$ is admissible for Γ and $\phi(x)$ is a polynomial that vanishes if and only if $x = 0$, then $h_1(x, y) = \phi(h(x, y))$ is also admissible for Γ. In particular, the polynomials

$$h_1(x, y) = (h(x, y))^r \qquad (r = 1, 2, 3, \dots)$$

are all admissible.

It should be pointed out that we are using the terms *function* and *polynomial* interchangeably. Thus, if $f(x)$, $g(x)$ are polynomials $\in F_q[x]$, the statement $f(x) = g(x)$ is short for $f(x) \equiv g(x) \pmod{x^q - x}$. Similarly, for polynomials in several variables, the statement $f(x, y) = g(x, y)$ is short for

$$f(x, y) \equiv g(x, y) \ (\mathrm{mod}\ x^q - x, y^q - y).$$

A convenient form for the polynomial characterizing the correspondence (2.3) is given by the following theorem.

THEOREM 2.3. *Put*

$$\phi_i(x) = \prod_{a \in A_i} (x - a), \quad \psi_i(y) = \prod_{b \in B_i} (y - b) \qquad (0 \leqslant i \leqslant k), \tag{2.6}$$

so that

$$\prod_{i=0}^{k} \phi_i(x) = x^q - x, \qquad \prod_{j=0}^{k} \psi_j(y) = y^q - y. \tag{2.7}$$

Then the polynomial $f(x, y)$ characterizing the correspondence satisfies

$$f(x, y) = 1 - \sum_{i=1}^{k} \frac{x^q - x}{\phi_i(x)} \frac{y^q - y}{\psi_i(y)} \phi_i'(x)\psi_i'(y). \tag{2.8}$$

Conversely, if $\phi_i(x)$, $\psi_i(y)$ are any polynomials satisfying (2.7) *and* $\deg \phi_i(x) > 0$, $\deg \psi_i(y) > 0$ $(1 \leqslant i \leqslant k)$, *then the partitions defined by* (2.6) *give a correspondence with characteristic polynomial* (2.8).

3. Some examples. (i) If $g(x)$ is an arbitrary polynomial in $F_q[x]$, then $h(x, y) = g(x) - y$ is admissible for some correspondence. For let $c_1, \dots, c_k$ denote the range of $g(x)$ and put

$$F_q = A_1 \cup A_2 \cup \cdots \cup A_k, A_i = \{a | g(a) = c_i\} \qquad (1 \leqslant i \leqslant k).$$

Then A_0 is vacuous while

$$B_i = \{c_i\} \qquad (1 \leqslant i \leqslant k), \quad B_0 = F_q \setminus \bigcup_{i=1}^{k} B_i.$$

(ii) The polynomial $h(x,y) = x^2 - y^2$ is admissible. We may assume q odd. The sets A_i, B_i are defined by

$$\begin{cases} A_1 = \{0\}, & A_2 = \{\pm 1\}, \ldots; \\ B_1 = \{0\}, & B_2 = \{\pm 1\}, \ldots; \\ A_0 = B_0 = \varnothing. \end{cases}$$

(iii) The polynomials $h(x, y) = x^r y^s$, $r \geqslant 1$, $s \geqslant 1$ are not admissible for any correspondence.

(iv) Let $h(x, y)$ denote a polynomial that never vanishes. Then $h(x, y)$ is admissible. The rank $k = 0$ and $A_0 = B_0 = F_q$.

(v) $h(x,y) = 1 - x^{q-1}y^{q-1}$ is admissible.

(vi) $h(x,y) = x^{q-1} - y^{q-1}$ is admissible.

(viii) Let $h(x,y)$ be admissible for the correspondence defined by

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k. \tag{3.1}$$

Let $g(a, b) \neq 0$ except possibly for some (a, b) such that

$$a \in A_i, \quad b \in B_j \qquad (1 \leqslant i \leqslant k); \tag{3.2}$$

then $h_1(x,y) = g(x,y)h(x,y)$ is also admissible for Γ.

(viii) Let $h(x, y)$ be admissible for Γ as defined by (3.1). Then the set of polynomials

$$\{g(x,y)h(x,y)\}, \tag{3.3}$$

where the $g(x,y)$ vanish only as in (3.2), are all admissible for Γ.

(ix) $h(x,y) = x^{q-1}$ is admissible for the correspondence defined by $A_0 = F_q \setminus \{0\}$, $A_1 = \{0\}$; $B_0 = \varnothing$, $B_1 = F_q$.

(x) $h(x, y) = 1 - x^{q-1}$ is admissible for the correspondence defined by $A_0 = \{0\}$, $A_1 = F_q \setminus \{0\}$; $B_0 = \varnothing$, $B_1 = F_q$.

(xi) $h(x,y) = 1$ is admissible for the correspondence of rank 0 defined by $A_0 = B_0 = F_q$.

(xii) $xy + 1$, $xy - 1$ are admissible polynomials; however, for q odd, the sum is not. Thus the sum of two admissible polynomials need not be admissible.

4. Normal forms. In general, there are numerous admissible polynomials for any given correspondence. The following theorem describes a normal form that can be found for rank $k < q - 1$.

THEOREM 4.1. *Let the partitions*

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k \tag{4.1}$$

define the correspondence Γ. *If* $k < q - 1$, *there exists an admissible polynomial of the form*

$$h(x,y) = f(x) - g(y) \tag{4.2}$$

for some $f(x) \in F_q[x]$, $g(y) \in F_q[y]$.

PROOF. Choose $k + 2$ distinct numbers $a_0, a_0', a_1, \ldots, a_k \in F_q$ and define polynomials $f(x)$, $g(y)$ by means of

$$f(c) = \begin{cases} a_0 & (c \in A_0), \\ a_i & (c \in A_i, 1 \leqslant i \leqslant k), \end{cases}$$

$$g(c) = \begin{cases} a_0' & (c \in B_0), \\ a_i & (c \in B_i, 1 \leqslant i \leqslant k). \end{cases}$$

Then $h(x, y) = f(x) - g(y)$ is admissible for Γ.

THEOREM 4.2. *Let the partitions $A_1, \ldots, A_q$; $B_1, \ldots, B_q$ define the correspondence Γ of rank q. Then there exists an admissible polynomial*

$$h(x,y) = f(x) - g(y),$$

where $f(x)$, $g(y)$ are permutation polynomials. In particular, we may take $f(x) = x$ or $g(y) = y$.

PROOF. Number the elements of F_q so that $A_i = \{a_i\}$, $B_i = \{b_i\}$ $(1 \leqslant i \leqslant q)$. Let $c_1, c_2, \ldots, c_k$ be an arbitrary numbering of the elements of F_q. Define $f(x)$, $g(y)$ by means of

$$f(a_i) = c_i, \quad g(b_i) = c_i \qquad (1 \leqslant i \leqslant q).$$

Then $h(x, y) = f(x) - g(y)$ is the desired polynomial.

For $c_i = b_i$, $g(y) = y$; for $c_i = a_i$, $f(x) = x$.

THEOREM 4.3. *Let the partitions*

$$A_0, A_1, \ldots, A_{q-1}; \quad B_0, B_1, \ldots, B_{q-1} \tag{4.3}$$

define a correspondence of rank $q - 1$. Then, if either A_0 or B_0 is vacuous, there exists an admissible polynomial of the form $h(x, y) = f(x) - g(y)$.

PROOF. 1. Let $B_0 = \varnothing$, $A_0 \neq \varnothing$ and let $F_q = \{a_0, a_1, \ldots, a_{q-1}\}$. Define $f(x)$, $g(y)$ by means of

$$f(c) = \begin{cases} a_0 & (c \in A_0), \\ a_i & (c \in A_i, 1 \leqslant i \leqslant q - 1), \end{cases}$$

$$g(c) = a_i \qquad (c \in B_i, 1 \leqslant i \leqslant q - 1).$$

Then $h(x, y) = f(x) - g(y)$ is the desired polynomial.

2. Let $A_0 = B_0 = \varnothing$. Let $a_1, \ldots, a_{q-1}$ be distinct numbers of F_q and define $f(x)$, $g(y)$ by means of

$$f(c) = a_i \qquad (c \in A_i, 1 \leqslant i \leqslant q - 1),$$

$$g(c) = a_i \qquad (c \in B_i, 1 \leqslant i \leqslant q - 1).$$

Then $h(x, y) = f(x) - g(y)$ is admissible.

The remaining theorems in this section are stated without proof.

THEOREM 4.4. *Let $f(x) \in F_q[x]$, $g(y) \in F_q[y]$. Then $h(x, y) = f(x) - g(y)$ is admissible for some Γ.*

REMARK. Either $f(x)$ or $g(y)$ may be the zero polynomial.

THEOREM 4.5. *Let the partitions $A_0, A_1, \ldots, A_k$; $B_0, B_1, \ldots, B_k$ define a correspondence Γ. An admissible polynomial of the form $h(x, y) = f(x) - g(y)$ exists if and only if*

(i) *$k \neq q - 1$, or*
(ii) *$k = q - 1$, A_0 or $B_0 = \varnothing$.*

It can be verified that

$$h(x,y) = (1 - x^{q-1})(1 - y^{q-1}) + (x - y)^{q-1}$$

is admissible for the correspondence defined by

$$F_q = \{a_0 = 0, a_1, a_2, \ldots, a_{q-1}\},$$
$$A_i = B_i = \{a_i\} \qquad (0 \leqslant i \leqslant q - 1).$$

This example falls under the exceptional case of Theorem 4.5. By means of the above $h(x, y)$, the following theorem can be proved.

THEOREM 4.6. *In the exceptional case of Theorem 4.5, that is $k = q - 1$, $A_0 \neq \varnothing$, $B_0 \neq \varnothing$, an admissible polynomial is furnished by*

$$h(x,y) = \{1 - \phi^{q-1}(x)\}\{1 - \psi^{q-1}(y)\} + \{\phi(x) - \psi(y)\}^{q-1},$$

where $\phi(x)$, $\psi(y)$ denote permutation polynomials.

THEOREM 4.7. *Let $f(x) - g(y)$ be admissible for the correspondence of rank q defined by $A_1, \ldots, A_q$; $B_1, \ldots, B_q$. Then all admissible polynomials of the form $f_1(x) - g_1(y)$ are given by $f_1(x) = \phi(f(x))$, $g_1(y) = \phi(g(y))$, where $\phi(x)$ is a permutation polynomial.*

5. Admissible polynomials. Let a correspondence be defined by means of the partitions

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k, \tag{5.1}$$

where

$$|A_i| = m_i, \quad |B_i| = n_i \qquad (0 \leqslant i \leqslant k). \tag{5.2}$$

We shall say that two admissible polynomials are equivalent if they are admissible for the same correspondence. Thus the set of all admissible polynomials (for a fixed F_q) breaks up into a number of equivalence classes.

THEOREM 5.1. *Two admissible polynomials $h_1(x, y)$, $h_2(x, y)$ are equivalent if and only if*

$$(h_1(x,y))^{q-1} = (h_2(x,y))^{q-1}. \tag{5.3}$$

THEOREM 5.2. *The number of equivalence classes of admissible polynomials is equal to the number of correspondences.*

LEMMA 5.3. *Let $h_1(x, y)$, $h_2(x, y)$ be equivalent admissible polynomials. The number of polynomials $g(x, y)$ that take on arbitrary values for $a \in A_i$, $b \in B_i$ $(1 \leqslant i \leqslant k)$, but are uniquely determined elsewhere and, moreover, satisfy $h_1(x, y) = g(x, y)h_2(x, y)$, is equal to*

$$q^e, e = \sum_{i=1}^{k} m_i n_i, \tag{5.4}$$

where m_i, n_i are defined by (5.2).

THEOREM 5.4. *The number of admissible polynomials for the correspondence* *defined by* (5.1) *and* (5.2) *is equal to*

$$(5.5) \qquad (q-1)^{e'}, \qquad e' = q^2 - \sum_{i=1}^{k} m_i n_i.$$

The polynomial $f(x, y)$ such that

$$f(a, b) = \begin{cases} 0 & (a \in A_i, b \in B_i, 1 \leqslant i \leqslant k), \\ 1 & \text{(otherwise)} \end{cases}$$

has been defined as the characteristic polynomial of the correspondence defined by (5.1). It is uniquely determined by the correspondence.

THEOREM 5.5. *Let $f(x, y)$ denote the characteristic polynomial of the correspondence Γ. A polynomial $h(x, y)$ is admissible for Γ if and only if*

$$(5.6) \qquad (h(x,y))^{q-1} = f(x,y).$$

THEOREM 5.6. *Let $h_1(x, y)$, $h_2(x, y)$ be admissible polynomials for some correspondence Γ. Then*

$$(5.7) \qquad h(x,y) = h_1(x,y)h_2(x,y)$$

is also admissible for Γ. It follows that the set of polynomials in a fixed equivalence class constitute a commutative group with respect to multiplication as defined by (5.7); *the characteristic polynomial is the identity element of the group.*

The next theorem may be compared with Theorem 4.7.

Admissible polynomials, $q = 2$		
rank	partitions	polynomials
0	$A_0 = B_0 = F_2$	1
1	$A_1 = B_1 = F_2$	0
	$A_0 = B_0 = \{0\}, \ A_1 = B_1 = \{1\}$	$xy + 1$
	$A_0 = B_1 = \{0\}, \ A_1 = B_0 = \{1\}$	$xy + x + 1$
	$A_0 = B_1 = \{1\}, \ A_1 = B_0 = \{0\}$	$xy + y + 1$
	$A_0 = B_0 = \{1\}, \ A_1 = B_1 = \{0\}$	$xy + x + y$
	$A_0 = \{0\}, \ A_1 = \{1\}, \ B_1 = F_2$	$x + 1$
	$A_0 = \{1\}, \ A_1 = \{0\}, \ B_1 = F_2$	x
	$A_1 = F_2, \ B_0 = \{0\}, \ B_1 = \{1\}$	$y + 1$
	$A_1 = F_2, \ B_0 = \{1\}, \ B_1 = \{0\}$	y
2	$A_1 = B_1 = \{0\}, \ A_2 = B_2 = \{1\}$	$x + y$
	$A_1 = B_2 = \{1\}, \ A_2 = B_1 = \{0\}$	$x + y + 1$

THEOREM 5.7. *Given the correspondence* Γ *defined by the partitions* A_0, $A_1, \ldots, A_k$; $B_0, B_1, \ldots, B_k$, *let* $k_1 = k$, $k+1$ *or* $k+2$ *according as none, one or both of the sets* A_0, B_0 *are nonvacuous. Then two admissible polynomials* $f(x) - g(y)$, $f_1(x) - g_1(y)$ *are equivalent if and only if* $f_1 = \phi(f(x))$, $g_1(y) = \phi(g(y))$, *where* $\phi(x)$ *denotes any function that carries an ordered set of* k_1 *numbers into another such set.*

6. Rank. The rank of a correspondence can evidently take on any value between 0 and q, inclusive. For rank $k = 0$, there is the unique correspondence defined by

$$A_0 = B_0 = F_q. \tag{6.1}$$

THEOREM 6.1. *The characteristic polynomial for the unique correspondence of rank* 0 *is*

$$f(x,y) = 1. \tag{6.2}$$

The admissible polynomials for this correspondence are the polynomials $h(x, y)$ *that never vanish. The number of such polynomials is*

$$(q-1)^{q^2}. \tag{6.3}$$

For rank $k = 1$, there are several possibilities. First, for the correspondence defined by

$$A_1 = B_1 = F_q, \tag{6.4}$$

we have the following result.

THEOREM 6.2. *The characteristic polynomial for the correspondence defined by* (6.4) *is*

$$f(x,y) = 0. \tag{6.5}$$

This is also the only admissible polynomial.

The general situation for rank 1 is given by

$$A_0, A_1; \quad B_0, B_1, \tag{6.6}$$

where

$$\begin{gathered} m_i = |A_i|, \quad n_i = |B_i|, \qquad m_1 > 0, n_1 > 0, \\ m_0 + m_1 = n_0 + n_1 = q. \end{gathered} \tag{6.7}$$

The number of correspondences defined by (6.6) and (6.7) is

$$\sum_{m_1, m_2 = 1}^{q} \binom{q}{m_1}\binom{q}{m_2} = (2^q - 1)^2. \tag{6.8}$$

Consider first the correspondence defined by

$$A_0 = B_0 = \{0\}, \qquad A_1 = B_1 = F_q \setminus \{0\}. \tag{6.9}$$

The characteristic polynomial for this correspondence is

$$f(x,y) = 1 - x^{q-1}y^{q-1}. \tag{6.10}$$

The admissible polynomials are

$$(6.11)\quad \begin{aligned} &c_0(1 - x^{q-1})(1 - y^{q-1}) + (1 - x^{q-1}) \sum_{a\neq 0} c_a(1 - (y - a)^{q-1}) \\ &\qquad + (1 - y^{q-1}) \sum_{a\neq 0} c'_a(1 - (x - a)^{q-1}), \end{aligned}$$

where a runs through the nonzero numbers of F_q and c_0, c_a, c'_a are arbitrary nonzero numbers of F_q. Hence the number of such polynomials is

$$(6.12)\qquad (q - 1)^{q^2}$$

in agreement with (5.5).

Another special rank 1 case that can be handled readily is

$$(6.13)\qquad A_0 = B_0 = F_q \setminus \{0\}, \qquad A_1 = B_1 = \{0\}.$$

The characteristic polynomial is

$$(6.14)\qquad f(x,y) = x^{q-1} + y^{q-1} - x^{q-1}y^{q-1}.$$

The admissible polynomials are given by

$$(6.15)\qquad h(x,y) = \sum_{a,\,b\in F_q}{}' c_{a,b}\{1 - (x - a)^{q-1}\}\{1 - (y - b)^{q-1}\},$$

where the summation is over all (a, b) except (0, 0) and the $c_{a,b}$ are arbitrary nonzero numbers of F_q. It follows that the number of admissible polynomials is

$$(6.16)\qquad (q - 1)^{q^2-1}$$

in agreement with (5.5).

Note that for q odd,

$$(x^{q-1} + y^{q-1})^{q-1} = x^{q-1} + y^{q-1} - x^{q-1}y^{q-1},$$

so that $x^{q-1} + y^{q-1}$ is admissible for (6.13).

By Theorem 4.5, an admissible polynomial of the form $f(x) + g(y)$ does not exist for (6.13) with $q = 2$. Let $q = 2^t$, $t > 1$, and let λ denote any number of F_q except 0 or 1. Then it can be verified that

$$(x^{q-1} + \lambda y^{q-1})^{q-1} = x^{q-1} + y^{q-1} - x^{q-1}y^{q-1},$$

so that $x^{q-1} + \lambda y^{q-1}$ is admissible for (6.13).

For the correspondence defined by (6.9) it can be verified that

$$(6.17)\qquad h(x,y) = 2 - x^{q-1} - y^{q-1} \qquad (q \text{ odd})$$

is admissible. This follows from

$$\begin{aligned} (2 - x^{q-1} - y^{q-1})^{q-1} &= \sum_{r=0}^{q-1} 2^{q-r-1}(x^{q-1} + y^{q-1})^r \\ &= 1 + \sum_{r=1}^{q-1} 2^{q-r-1}\{x^{q-1} + y^{q-1} + (2^r - 2)x^{q-1}y^{q-1}\} \\ &= 1 - x^{q-1}y^{q-1}. \end{aligned}$$

For $q = 2^t$, $t > 1$, let α, β be numbers of F_q such that $\alpha + \beta = 1$, $\alpha\beta \neq 0$. We find that

$$(1 + \alpha x^{q-1} + \beta y^{q-1})^{q-1} = 1 + x^{q-1}y^{q-1},$$

and therefore the polynomial $1 + \alpha x^{q-1} + \beta y^{q-1}$ is admissible for (6.9).

For rank 2 consider first the correspondence defined by

$$A_1 = B_1 = \{0\}, \qquad A_2 = B_2 = F_q \setminus \{0\}. \tag{6.18}$$

The characteristic polynomial is

$$f(x,y) = x^{q-1} + y^{q-1} - 2x^{q-1}y^{q-1}. \tag{6.19}$$

An admissible polynomial (compare Example (vi) of §3) is

$$h(x,y) = x^{q-1} - y^{q-1}. \tag{6.20}$$

Another admissible polynomial is

$$h(x,y) = (1 - x^{q-1})y + x(1 - y^{q-1}). \tag{6.21}$$

Another special case of rank 2 of some interest is

$$A_0 = B_0 = \{0\}, \quad A_1 = B_1 = \{a\}, \quad A_2 = B_2 = \{b\} \qquad (q \text{ odd}), \tag{6.22}$$

where a runs through the squares ($\neq 0$) and b the nonsquares of F_q. We find that the characteristic polynomial for (6.22) is

$$f(x,y) = 1 - \tfrac{1}{2}(x^m y^m + x^{q-1}y^{q-1}) \qquad (q = 2m + 1). \tag{6.23}$$

Since

$$(1 - x^m y^m)^{q-1} = 1 + m(x^m y^m + x^{q-1}y^{q-1}),$$

it follows that

$$h(x,y) = 1 - x^m y^m \qquad (q = 2m + 1) \tag{6.24}$$

is admissible for (6.22).

For rank $k = q$, it is clear that A_0 and B_0 are both vacuous and the correspondence is defined by

$$A_1, \ldots, A_q; \quad B_1, \ldots, B_q, \tag{6.25}$$

where each of the sets contains a single element. By Theorem 4.2 there exists an admissible polynomial for this correspondence of the form

$$h(x,y) = f(x) - g(y). \tag{6.26}$$

In particular, for the *identity correspondence*, that is

$$A_i = B_i \qquad (1 \leqslant i \leqslant q), \tag{6.27}$$

the polynomial $x - y$ is evidently admissible, so that

$$f(x,y) = (x - y)^{q-1} \tag{6.28}$$

is the characteristic polynomial. The general admissible polynomial is given by

$$h(x,y) = \sum_{a \neq b} c_{a,b}\{1 - (x - a)^{q-1}\}\{1 - (y - b)^{q-1}\}, \tag{6.29}$$

where the summation is over all a, $b \in F_q$, $a \neq b$, and the $c_{a,b}$ are arbitrary numbers of F_q. The number of such polynomials is $(q - 1)^{q^2-q}$ in agreement with (5.5).

7. Some enumerations. We shall use the following notation. Consider the partitions

$$A_0, A_1, \dots, A_k; \quad B_0, B_1, \dots, B_k \tag{7.1}$$

and put

$$m_i = |A_i|, \quad n_i = |B_i| \qquad (0 \leqslant i \leqslant k), \tag{7.2}$$

where

$$m_0 \geqslant 0, \quad n_0 \geqslant 0, \quad m_i > 0, \quad n_i > 0 \qquad (1 \leqslant i \leqslant k) \tag{7.3}$$

and

$$q = m_0 + m_1 + \cdots + m_k = n_0 + n_1 + \cdots + n_k. \tag{7.4}$$

The set of integers

$$(m_0, m_1, \dots, m_k; n_0, n_1, \dots, n_k) \tag{7.5}$$

will be said to characterize a *correspondence type* of rank k.

In order to enumerate correspondences and correspondence types, it is convenient to consider a somewhat more general problem. Let A, B be finite sets, $|A| = m$, $|B| = n$. Consider the partitions:

$$A = A_0 \cup A_1 \cup \cdots \cup A_k, \quad B = B_0 \cup B_1 \cup \cdots \cup B_k, \tag{7.6}$$

where

$$\begin{cases} m_i = |A_i|, \quad n_i = |B_i| & (0 \leqslant i \leqslant k), \\ m_0 \geqslant 0, \quad n_0 \geqslant 0, \quad m_i > 0, \quad n_i > 0 & (1 \leqslant i \leqslant k). \end{cases} \tag{7.7}$$

Changing the notation, we put

$$\begin{cases} m = m_0 + \Sigma i e_{ij} & (m_0 \geqslant 0), \\ n = n_0 + \Sigma j e_{ij} & (n_0 \geqslant 0), \\ k = \Sigma e_{ij}; \end{cases} \tag{7.8}$$

e_{ij} is the number of pairs (A_s, B_t) such that $|A_s| = i$, $|B_t| = j$.

Let $N(m, n, k)$ denote the number of sets A_i, B_j satisfying (7.6) and (7.8); let $T(m, n, k)$ denote the number of solutions of the system (7.8). Then

$$T(m, n, k) = \sum 1 \tag{7.9}$$

and

$$N(m, n, k) = \sum \frac{m!n!}{m_0!n_0!\Pi e_{ij}!\Pi(i!)^{e_{ij}}\Pi(j!)^{e_{ij}}}; \tag{7.10}$$

in each case the summation is over all solutions of (7.8).

Put

$$F(x, y, z) = \sum_{m,n,k=0}^{\infty} N(m, n, k) \frac{x^m y^n}{m!n!} z^k. \tag{7.11}$$

It then follows from (7.10) that

$$F(x, y, z) = e^{x+y} \sum_{i,j,e_{ij}} \frac{x^{\Sigma i e_{ij}} y^{\Sigma j e_{ij}} z^{e_{ij}}}{\Pi e_{ij}! \, (\Pi i! \Pi j!)^{e_{ij}}}.$$

Now

$$\sum_{i,j=1}^{\infty}\sum_{e_{ij}=0}^{\infty}\frac{x^{\Sigma ie_{ij}}y^{\Sigma je_{ij}}z^{e_{ij}}}{\Pi e_{ij}!\,(\Pi i!\Pi j!)^{e_{ij}}}=\exp\left\{z\sum_{i,j=1}^{\infty}\frac{x^iy^j}{i!j!}\right\}$$

$$=\exp(z(e^x-1)(e^y-1)),$$

so that

$$F(x,y,z)=e^{x+y}\exp(z(e^x-1)(e^y-1)). \tag{7.12}$$

Since the Stirling number of the second kind

$$S(n,k)=\frac{1}{k!}\sum_{j=0}^{k}(-1)^{n-k}\binom{k}{j}j^n$$

satisfies

$$(e^x-1)^k=k!\sum_{n=k}^{\infty}S(n,k)\frac{x^n}{n!},$$

it follows from (7.12) that

$$F(x,y,z)=e^{x+y}\sum_{k=0}^{\infty}k!z^k\sum_{m,n=0}^{\infty}S(m,k)S(n,k)\frac{x^my^n}{m!n!}. \tag{7.13}$$

Comparison of (7.13) with (7.11) gives

$$N(m,n,k)=k!\sum_{i=0}^{m}\sum_{j=0}^{n}\binom{m}{i}\binom{n}{j}S(i,k)S(j,k). \tag{7.14}$$

Since

$$\sum_{j=0}^{n}\binom{n}{j}S(j,k)=S(n+1,k+1),$$

(7.14) reduces to

$$N(m,n,k)=k!S(m+1,k+1)S(n+1,k+1). \tag{7.15}$$

As for $T(m, n, k)$, it follows from (7.8) that

$$T(m,n,k)=\sum_{r=0}^{m}\sum_{s=0}^{n}T'(r,s,k), \tag{7.16}$$

where $T'(r, s, k)$ denotes the number of solutions of

$$r=\sum ie_{ij},\quad s=\sum je_{ij},\quad k=\sum e_{ij}. \tag{7.17}$$

Put

$$\begin{cases} G(x,t,z)=\sum_{m,n,k}T(m,n,k)x^my^nz^k, \\ G'(x,y,z)=\sum_{m,n,k}T'(m,n,k)x^my^nz^k. \end{cases} \tag{7.18}$$

Then by (7.16),

$$G(x,y,z)=(1-x)^{-1}(1-y)^{-1}G'(x,y,z). \tag{7.19}$$

We find that

$$G'(x,y,z) = \prod_{i,j=1}^{\infty} (1 - x^i y^j z)^{-1}, \tag{7.20}$$

and therefore,

$$G(x,y,z) = (1 - x)^{-1}(1 - y)^{-1} \prod_{i,j=1}^{\infty} (1 - x^i y^j z)^{-1}. \tag{7.21}$$

The generating function (7.20) suggests the following combinatorial interpretation of $T'(m, n, k)$. The enumerant $T'(m, n, k)$ is equal to the number of pairs of k-tuples of positive integers (i_s, j_s) satisfying

$$i_1 + i_2 + \cdots + i_k = m, \qquad j_1 + j_2 + \cdots + j_k = n. \tag{7.22}$$

Another way of putting it is that $T'(m, n, k)$ is the number of partitions of the bipartite (m, n) into positive parts. Hence, by (7.16), $T(m, n, k)$ is the number of pairs of positive integers i_s, j_s such that

$$i_1 + i_2 + \cdots + i_k \leqslant m, \qquad j_1 + j_2 + \cdots + j_k \leqslant n. \tag{7.23}$$

Next put

$$T(m, n) = \sum_k T(m, n, k). \tag{7.24}$$

Then (7.21) gives

$$\sum_{m,n=0}^{\infty} T(m, n) x^m y^n = \prod_{i+j>0} (1 - x^i y^j)^{-1}. \tag{7.25}$$

Thus $T(m, n)$ is the number of pairs (i_s, j_s), $i_s + j_s > 0$, such that

$$m = i_1 + i_2 + i_3 + \ldots, \qquad n = j_1 + j_2 + j_3 + \ldots, \tag{7.26}$$

that is, the number of unrestricted partitions of the bipartite (m, n).

For references to multipartite partitions see **[4]**, **[11]**, **[12]**, **[15]**, **[17]**, **[18]**.

For the applications to the enumeration of correspondences and correspondence types we take $m = n = q$.

THEOREM 7.1. *The number of correspondences in F_q of rank k is equal to $k!(S(q + 1, k + 1))^2$, where $S(q + 1, k + 1)$ denotes a Stirling number of the second kind. The total number of correspondences is $\sum_{k=0}^{q} k!(S(q + 1, k + 1))^2$.*

THEOREM 7.2. *The number of correspondence types in F_q of rank k is equal to $T(q, q, k)$, where*

$$\sum_{m,n,k=0}^{\infty} T(m, n, k) x^m y^n z^k = (1 - x)^{-1}(1 - y)^{-1} \prod_{i,j=1}^{\infty} (1 - x^i y^j z)^{-1}.$$

The total number of correspondence types is equal to $T(q, q)$, where

$$\sum_{m,n=0}^{\infty} T(m, n) x^m y^n = (1 - x)^{-1}(1 - y)^{-1} \prod_{i,j=1}^{\infty} (1 - x^i y^j)^{-1}.$$

To get a generating function for the number of admissible polynomials we put

$$N(m, n, k; \lambda) = \sum \frac{m!n!\lambda^{\Sigma ij e_{ij}}}{m_0!n_0!e_{ij}!\,(\Pi i!\Pi j!)^{e_{ij}}}, \tag{7.27}$$

where the summation is over all solutions of (7.8). Also put

$$F(x,y,z;\lambda) = \sum_{m,n,k=0}^{\infty} N(m,n,k;\lambda)\frac{x^m y^n}{m!n!}z^k. \tag{7.28}$$

We find that

$$F(x,y,z;\lambda) = e^{x+y}\exp\left\{z\sum_{i,j=1}^{\infty}\frac{x^i y^j}{i!j!}\lambda^{ij}\right\}. \tag{7.29}$$

Put

$$\left\{\sum_{i,j=1}^{\infty}\frac{x^i y^j}{i!j!}\lambda^{ij}\right\}^k = k!k!\sum_{m,n=0}^{\infty}S(m,n,k;\lambda)\frac{x^m y^n}{m!n!}, \tag{7.30}$$

so that $S(m, n, k; 1) = S(m, k)S(n, k)$. Also

$$N(m,n,k;\lambda) = k!\sum_{i=0}^{m}\sum_{j=0}^{n}\binom{m}{i}\binom{n}{j}S(m,n,k;\lambda). \tag{7.31}$$

Applying Theorem 5.4, we get

THEOREM 7.3. *The number of admissible polynomials of rank k is equal to*

$$k!\,(q-1)^{q^2}\sum_{i,j=0}^{q}\binom{q}{i}\binom{q}{j}S(i,j,k;(q-1)^{-1}), \tag{7.32}$$

where $S(i, j, k; \lambda)$ is defined by (7.30).

The $S(i, j, k; \lambda)$ are not easily computed. However it can be verified that

$$S(m,n,0;\lambda) = 0 \qquad (m+n>0), \quad S(0,0,0;\lambda) = 1,$$

$$S(m,n,1;\lambda) = \lambda^{mn} \qquad (m>0, n>0),$$

$$S(m,n,2;\lambda) = \sum_{i=1}^{m}\sum_{j=1}^{n}\binom{m}{i}\binom{n}{j}\lambda^{ij+(m-i)(n-j)} \qquad (m>1, n>1).$$

Thus, for example, the number of admissible polynomials of rank 1 is equal to $\Sigma_{i,j=1}^{q}(q-1)^{q^2-ij}$ in agreement with earlier results.

8. Composition (this topic is not discussed in [2], [3]). Let the correspondence Γ be defined by the partitions

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k, \tag{8.1}$$

where the A_i, B_i satisfy the usual conditions. Let $\{i_1, \ldots, i_r\}$, $\{j_1, \ldots, j_s\}$ denote two subsets of $1, 2, \ldots, k$, such that $\{i_1, \ldots, i_r\} \cup \{j_1, \ldots, j_s\} \supseteq \{1, 2, \ldots, k\}$ and put $\{i_1, \ldots, i_r\} \cap \{j_1, \ldots, j_s\} = \{h_1, \ldots, h_t\}$. Thus

$$r + s = k + t. \tag{8.2}$$

Now define the correspondences Γ_1, Γ_2, Γ_0 by means of

$$\Gamma_1\colon A_0', A_{i_1}, \ldots, A_{i_r}; \quad B_0', B_{i_1}, \ldots, B_{i_r}, \tag{8.3}$$

$$\Gamma_2\colon A_0'', A_{j_1}, \ldots, A_{j_s}; \quad B_0'', B_{j_1}, \ldots, B_{j_s}, \tag{8.4}$$

$$(8.5)\qquad \Gamma_0: A'''_0, A_{h_1}, \ldots, A_{h_t};\quad B'''_0, B_{h_1}, \ldots, B_{h_t},$$

where

$$A'_0 = F_q \setminus (A_{i_1} \cup \cdots \cup A_{i_r}), B'_0 = F_q \setminus (B_{i_1} \cup \cdots \cup B_{i_r}),$$
$$A''_0 = F_q \setminus (A_{j_1} \cup \cdots \cup A_{j_s}), B''_0 = F_q \setminus (B_{j_1} \cup \cdots \cup B_{j_s}),$$
$$A'''_0 = F_q \setminus (A_{h_1} \cup \cdots \cup A_{h_t}),\quad B'''_0 = F_q \setminus (B_{h_1} \cup \cdots \cup B_{h_t}).$$

Clearly the correspondences Γ_1, Γ_2, Γ_0 are of rank r, s, t, respectively. We shall write

$$(8.6)\qquad \Gamma = \Gamma_1 \cup \Gamma_2, \qquad \Gamma_0 = \Gamma_1 \cap \Gamma_2.$$

Denote the characteristic polynomials of Γ, Γ_1, Γ_2, Γ_0 by $f(x, y)$, $f_1(x, y)$, $f_2(x, y)$, $f_0(x, y)$, respectively. The following theorem is a consequence of Theorem 2.2:

THEOREM 8.1. *The characteristic polynomials of the correspondences* Γ, Γ_1, Γ_2, Γ_0 *satisfy*

$$(8.7)\qquad f(x,y) + f_0(x,y) = f_1(x,y) + f_2(x,y).$$

In particular, for $t = 0$, Γ_0 is the zero correspondence defined by $A_0 = B_0 = F_q$. The characteristic polynomial in this case is 1, so that (8.7) reduces to

$$(8.8)\qquad f(x,y) + 1 = f_1(x,y) + f_2(x,y).$$

For example (see the table in §5) if we take

$$\Gamma: A_1 = B_1 = \{0\},\ \ A_2 = B_2 = \{1\}, f(x,y) = x + y,$$
$$\Gamma_1: A_0 = B_0 = \{1\},\ \ A_1 = B_1 = \{0\}, f_1(x,y) = xy + x + y,$$
$$\Gamma_2: A_0 = B_0 = \{0\},\ \ A_1 = B_1 = \{1\}, f_2(x,y) = xy + 1,$$

it is clear that (8.8) is satisfied.

Returning to (8.1) define the set of correspondences $\Gamma_1, \ldots, \Gamma_k$ by means of

$$\Gamma_i: A_0 = F_q \setminus A_i, A_i;\quad B_0 = \Gamma_q \setminus B_i, B_i \qquad (i = 1, 2, \ldots, k).$$

Each Γ_i is evidently of rank 1.

Let $f_i(x, y)$ denote the characteristic polynomial of Γ_i. Then (8.8) gives

$$(8.9)\qquad f(x,y) + k - 1 = \sum_{i=1}^{k} f_i(x,y).$$

From the above it is clear that with each correspondence Γ of rank k is associated a set of 2^k correspondences that form a Boolean algebra with respect to the operations $\cup$, $\cap$; Γ is the unit element of the algebra and the zero correspondence is the zero element of the algebra. The characteristic polynomials of the correspondences are related by (8.7).

It should, of course, be kept in mind that we have not defined $\Gamma_1 \cup \Gamma_2$, $\Gamma_1 \cap \Gamma_2$ for an arbitrary pair of correspondences.

9. More general correspondences. In the remainder of the paper we shall briefly discuss the more general varieties of correspondence defined in the Introduction. Except for the enumerations in §14, we shall limit the discussion to correspondences of type (1, 1, 1) and (m, n).

To begin with, it is convenient to state several preliminary lemmas. Let F_q^r denote the direct product of r copies of F_q and let

$$(9.1) \qquad \mathbf{a} = (a_1, a_2, \ldots, a_r)$$

denote an arbitrary point of F_q^r.

Lemma 9.1 [9, p. 124]. *Given the numbers* $c(\mathbf{a}) = c(a_1, a_2, \ldots, a_r) \in F_q$ *there exists a polynomial* $f(\mathbf{x}) = f(x_1, x_2, \ldots, x_r) \in F_q[x_1, x_2, \ldots, x_r]$ *such that*

$$(9.2) \qquad f(\mathbf{a}) = c(\mathbf{a}) \qquad (\mathbf{a} \in F_q^r),$$

namely,

$$(9.3) \qquad f(\mathbf{x}) = \sum_{\mathbf{a} \in F_q^r} c(\mathbf{a}) \prod_{i=1}^{r} (1 - (x_i - a_i)^{q-1}).$$

Lemma 9.2. *Let* $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_t$ *be distinct points of* F_q^r. *There exists a polynomial* $f(\mathbf{x}) \in F_q[\mathbf{x}]$ *such that*

$$(9.4) \qquad f(\mathbf{a}) = \begin{cases} 0 & (\mathbf{a} = \mathbf{b}_i,\ 1 \leqslant i \leqslant t), \\ 1 & (\textit{otherwise}). \end{cases}$$

Lemma 9.3. *Let* $t \geqslant 1$ *and let*

$$(9.5) \qquad f_i(\mathbf{x}) \qquad (i = 1, 2, \ldots, t)$$

be arbitrary polynomials in $F_q[\mathbf{x}]$. *Let* $A = \{\mathbf{a}\}$ *denote the set of zeros in* F_q^r *of the system*

$$(9.6) \qquad f_i(\mathbf{x}) = 0 \qquad (i = 1, 2, \ldots, t).$$

There exists a polynomial $f(\mathbf{x}) \in F_q[\mathbf{x}]$ *such that*

$$(9.7) \qquad f(\mathbf{c}) = \begin{cases} 0 & (\mathbf{c} \in A), \\ 1 & (\textit{otherwise}). \end{cases}$$

Now let $k \geqslant 0$ and let

$$(9.8) \qquad A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k; \quad C_0, C_1, \ldots, C_k$$

denote partitions of F_q such that

$$(9.9) \qquad A_1, \ldots, A_k, \quad B_1, \ldots, B_k, \quad C_1, \ldots, C_k$$

are nonvacuous while A_0, B_0, C_0 are arbitrary. Then (9.8) defines a (1, 1, 1) correspondence Γ.

Theorem 9.4. *There exists a polynomial* $f(x, y, z) \in F_q[x, y, z]$ *such that*

$$(9.10) \qquad f(a, b, c) = \begin{cases} 0 & (a \in A_i, b \in B_i, c \in C_i,\ 1 \leqslant i \leqslant k), \\ 1 & (\textit{otherwise}). \end{cases}$$

The polynomial $f(x, y, z)$ is the *characteristic* polynomial of the correspondence Γ defined by (8.8). The definition of an admissible polynomial need not be repeated.

The following properties of admissible polynomials are immediate.

1. If $h(x, y, z)$ is admissible for the correspondence Γ, then

$$f(x, y, z) = (h(x, y, z))^{q-1}$$

is the characteristic polynomial for Γ.

2. If $h(x, y, z)$ is admissible for Γ and $g(x, y, z)$ never vanishes, then

$$g(x, y, z)h(x, y, z)$$

is also admissible for Γ.

3. If $h(x, y, z)$ is admissible for Γ and $\phi_1(x)$, $\phi_2(y)$, $\phi_3(z)$ are permutation polynomials such that each A_i is carried into itself by $\phi_1(x)$, each B_i is carried into itself by $\phi_2(y)$ and each C_i is carried into itself by $\phi_3(z)$, then

$$h_1(x, y, z) = h(\phi_1(x), \phi_2(y), \phi_3(z))$$

is also admissible for Γ.

4. If $h(x, y, z)$ is admissible for Γ and $\phi(x)$ is a polynomial that vanishes only for $x = 0$, then $h_1(x, y, z) = \phi(h(x, y, z))$ is also admissible for Γ. In particular, the polynomials

$$h_t(x, y, z) = (h(x, y, z))^t \qquad (t = 1, 2, 3, \ldots)$$

are all admissible.

A useful form for the chracteristic polynomial of a correspondence is given by the following theorem.

THEOREM 9.5. *With the notation* (9.8), *put*

$$(9.11) \qquad \begin{aligned} \phi_i(x) &= \prod_{a \in A_i} (x - a), \qquad \psi_i(y) = \prod_{b \in B_i} (y - b), \\ \omega_i(z) &= \prod_{c \in C_i} (z - c) \qquad (i = 0, 1, \ldots, k), \end{aligned}$$

so that

$$(9.12) \qquad \prod_{i=0}^{k} \phi_i(x) = x^q - x, \quad \prod_{i=0}^{k} \psi_i(y) = y^q - y, \quad \prod_{i=0}^{k} \omega_i(z) = z^q - z.$$

Then

$$(9.13) \qquad \begin{aligned} f(x, y, z) = 1 + \sum_{i=1}^{k} \frac{x^q - x}{\phi_i(x)} \frac{y^q - y}{\psi_i(y)} \frac{z^q - z}{\omega_i(z)} \\ \times \phi_i'(x)\psi_i'(t)\omega_i'(z). \end{aligned}$$

Conversely if $\phi_i(x)$, $\psi_i(y)$, $\omega_i(z)$, $i = 0, 1, \ldots, k$, *are any polynomials satisfying* (9.12) *and* $\deg \phi_i(x) > 0$, $\deg \phi_i(y) > 0$, $\deg \omega_i(z) > 0$ $(1 \leqslant i \leqslant k)$, *then the partitions defined by* (9.12) *and* (9.8) *give a correspondence with the characteristic polynomial* (9.13).

In the next place, consider the partitions

$$(9.14) \qquad F_q^m = A_0 \cup A_1 \cup \cdots \cup A_k, \qquad F_q^n = B_0 \cup B_1 \cup \cdots \cup B_k,$$

where $m \geqslant 1$, $n \geqslant 1$, $A_1, \ldots, A_k$, $B_1, \ldots, B_k$ are nonvacuous while A_0, B_0 are arbitrary.

THEOREM 9.6. *There exists a polynomial* $f(\mathbf{x}, \mathbf{y}) \in F_q[\mathbf{x}, \mathbf{y}]$, *where* $\mathbf{x} \in F_q^m$, $\mathbf{y} \in F_q^n$, *such that*

$$(9.15)\qquad f(\mathbf{a},\mathbf{b})=\begin{cases}0 & (\mathbf{a}\in A_i,\ \mathbf{b}\in B_i,\ 1\leqslant i\leqslant k),\\ 1 & (\textit{otherwise}).\end{cases}$$

The polynomial $f(\mathbf{x},\ \mathbf{y})$ is the characteristic polynomial of the $(m,\ n)$ correspondence defined by (9.14). The definition of admissible polynomial need not be restated.

For arbitrary $A\subseteq F_q^r$ define

$$g(a,A)=\begin{cases}1 & (\mathbf{a}\in A),\\ 0 & \text{otherwise.}\end{cases}$$

THEOREM 9.7. *With the notation* (9.14), *put*

$$g_i(\mathbf{x},\mathbf{y})=g(\mathbf{x},A_i)\,g(\mathbf{y},B_i)\qquad(1\leqslant i\leqslant k).$$

Then

$$(9.16)\qquad f(\mathbf{x},\mathbf{y})=1-\sum_{i=1}^{k}g_i(\mathbf{x},\mathbf{y})$$

is the characteristic polynomial of the correspondence defined by (9.14).

Composition of correspondences as defined in §8 is easily carried over to more general correspondences. However we shall not take the space to discuss this topic.

10. Some examples. A. (1, 1, 1) admissible and characteristic polynomials.

(i) $f(x,\ y,\ z)=1-x^{q-1}y^{q-1}z^{q-1}$ is characteristic for correspondence of rank 1 defined by $A_0=B_0=C_0=\{0\}$, $A_1=B_1=C_1=F_q\setminus\{0\}$.

(ii) $h(x,y,z)=1-xyz$ $(q>2)$ is not admissible for any correspondence.

(iii) The polynomials $h(x,y,z)=x+y+z$, $xy-z$, $x^{q-1}+y^{q-1}-z^{q-1}$ are not admissible for any correspondence.

(iv) $f(x,y,z)=0$ is characteristic for the correspondence of rank 1 defined by $A_1=B_1=C_1=F_q$.

(v) $f(x,y,z)=1$ is characteristic for the correspondence of rank 0 defined by $A_0=B_0=C_0=F_q$.

(vi) The polynomial

$$\begin{aligned}f(x,y,z)&=(x-y)^{q-1}+(y-z)^{q-1}-(x-y)^{q-1}(y-z)^{q-1}\\&=(y-z)^{q-1}+(z-x)^{q-1}-(y-z)^{q-1}(z-x)^{q-1}\\&=(z-x)^{q-1}+(x-y)^{q-1}-(z-x)^{q-1}(x-y)^{q-1}\end{aligned}$$

is characteristic for the *identity* correspondence defined by $A_i=B_i=C_i=\{a_i\}$ $(1\leqslant i\leqslant q)$, where $F_q=a_1,a_2,\ldots,a_q$.

(vii) $f(x,\ y,\ z)=(1-xy)^{q-1}+(1-yz)^{q-1}-(1-xy)^{q-1}(1-yz)^{q-1}$ is characteristic for the correspondence of rank $q-1$ defined by $A_0=B_0=C_0=\{0\}$, $A_i=\{a_i\}$, $B_i=\{a_i^{q-1}\}$, $C_i=\{a_i\}$ $(1\leqslant i\leqslant q-1)$, where $F_q=\{0,a_1,\ldots,a_{q-1}\}$.

(viii) $f(x,y,z)=1-(1-x^{q-1})(1-y^{q-1})(1-z^{q-1})$ is characteristic for the correspondence of rank 1 defined by $A_0=B_0=C_0=F_q\setminus\{0\}$, $A_1=B_1=C_1=\{0\}$.

B. (2, 1) admissible and characteristic polynomials.

(ix) $h(x_1, x_2, y) = x_1^{q-1}x_2^{q-1} - y^{q-1}$ is admissible for the correspondence of rank 2 defined by

$$A_1 = \{(a_1, a_2)|a_1a_2 \neq 0\}, \qquad A_2 = \{(a_1, a_2), a_1a_2 = 0\},$$
$$B_1 = F_q \setminus \{0\}, \qquad B_2 = \{0\}.$$

(x) $f(x_1, x_2, y) = 1 - x_1^{q-1}x_2^{q-1}y^{q-1}$ is characteristic for the correspondence of rank 1 defined by

$$A_0 = \{(a_1, a_2)|a_1a_2 = 0\}, \qquad A_1 = \{(a_1, a_2)|a_1a_2 \neq 0\},$$
$$B_0 = \{0\}, \qquad B_1 = F_q \setminus \{0\}.$$

(xi) $h(x_1, x_2, y) = x_1 + x_2y$ is not admissible for any (2,1) correspondence.

(xii) $h(x_1, x_2, y) = x_1 + x_2 - y$ is admissible for the correspondence of rank q defined by $A_i = \{(a_1, a_2)|a_1 + a_2 = b_i\}$, $B_i = \{b_i\}$ $(1 \leqslant i \leqslant q)$, where $F_q = (b_1, b_2, \ldots, b_q\}$.

(xiii) $h(x_1, x_2, y) = x_1x_2y$ is not admissible for any (2, 1) correspondence.

(xiv) $f(x_1, x_2, y) = 1 - (1 - x_1^{q-1})(1 - x_2^{q-1})(1 - y^{q-1})$ is characteristic for the correspondence of rank 1 defined by

$$A_0 = F_q^2 \setminus \{(0, 0)\}, \qquad A_1 = \{(0, 0)\},$$
$$B_0 = F_q \setminus \{0\}, \qquad B_1 = \{0\}.$$

(xv) $h(x_1, x_2, y) = x_1^{q-1} + x_2^{q-1} - y^{q-1}$ is admissible for the correspondence of rank 2 defined by

$$A_1 = \{(0, 0)\}, \qquad A_2 = F_2^2 \setminus \{(0, 0)\},$$
$$B_1 = \{0\}, \qquad B_2 = F_q \setminus \{0\}.$$

(xvi) $h(x_1, x_2, y) = 0$ is characteristic for the correspondence of rank 1 defined by $A_1 = F_q^2$, $B_1 = F_q$.

(xvii) $h(x_1, x_2, y) = 1$ is characteristic for the correspondence of rank 0 defined by $A_0 = F_q^2$, $B_0 = F_q$.

C. (2, 2) characteristic polynomials.

(xviii)
$$f(x_1, x_2, y_1, y_2) = 1 - \left(x_1^{q-1} + x_2^{q-1} - x_1^{q-1}x_2^{q-1}\right)\left(y_1^{q-1} + y_2^{q-1} - y_1^{q-1}y_2^{q-1}\right)$$

is characteristic for the rank 1 correspondence $A_0 = B_0 = \{(0, 0)\}$, $A_1 = B_1 = F_q^2 \setminus \{(0, 0)\}$.

(xix) $f(x_1, x_2, y_1, y_2) = 1 - \left(1 - x_1^{q-1}\right)\left(1 - x_2^{q-1}\right)\left(1 - y_1^{q-1}\right)\left(1 - y_2^{q-1}\right)$ is characteristic for the rank 1 correspondence $A_0 = B_0 = F_q^2 \setminus \{(0, 0)\}$, $A_1 = B_1 = \{(0, 0)\}$.

$$f(x_1, x_2, y_1, y_2) = (x_1 - y_1)^{q-1} + (x_2 - y_2)^{q-1} - (x_1 - y_1)^{q-1}(x_2 - y_2)^{q-2}$$

is characteristic for the identity correspondence (rank q^2).

11. Normal forms. A. (1, 1, 1) correspondences. Let the partitions

$$(11.1) \qquad A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k; \quad C_0, C_1, \ldots, C_k,$$

subject to the usual conditions define the (1,1,1) correspondence Γ. We define

k_1, the augmented rank of Γ, as equal to k, $k+1$, $k+2$ according as A_0, B_0, C_0 are all vacuous, at most two are nonvacuous, or all are nonvacuous.

In order to obtain results like those of §4, we extend the notion of an admissible polynomial. Let $h_1(x, y, z)$, $h_2(x, y, z)$ be polynomials in $F_q[x, y, z]$ such that the set of zeros of the system

$$h_1(x,y,z) = 0, \qquad h_2(x,y,z) = 0$$

is given by $\bigcup_{i=1}^{k}(A_i \times B_i \times C_i)$.We shall say that h_1, h_2 are an admissible pair for Γ.

THEOREM 11.1. *Given arbitrary polynomials $\phi(x)$, $\psi(y)$, $\omega(z)$, with coefficients in F_q, the polynomials $\phi(x) - \psi(y)$, $\psi(y) - \omega(z)$ constitute an admissible pair for some* (1, 1, 1) *correspondence. The augmented rank of this correspondence satisfies the inequality $k_1 \leqslant q$.*

THEOREM 11.2. *A* (1, 1, 1) *correspondence possesses an admissible pair of the form $\phi(x) - \psi(y)$, $\psi(y) - \omega(z)$ except when its rank is $q-1$ and its augmented rank is $q+1$.*

THEOREM 11.3. *In the exceptional case of Theorem* 11.2, *that is, $k = q-1$, $k_1 = q+1$, the characteristic polynomial is given by $f(\alpha(x), \beta(y), \gamma(z))$, where*

$$f(x,y,z) = (1 - x^{q-1})(1 - y^{q-1})(1 - z^{q-1}) + (x-y)^{q-1}$$
$$+ (x-z)^{q-1} - (x-y)^{q-1}(x-z)^{q-1}$$

and $\alpha(x)$, $\beta(y)$, $\gamma(z)$ are permutation polynomials.

B. (m, n) correspondences. Let the partitions

$$A_0, A_1, \ldots, A_k; \quad B_0, B_1, \ldots, B_k, \tag{11.2}$$

subject to the usual conditions, define the (m, n) correspondence Γ. We define k_1, the *augmented rank* of Γ, as equal to k, $k+1$, $k+2$ according as A_0, B_0 are both vacuous, one is nonvacuous, or both are nonvacuous.

THEOREM 11.4. *Given arbitrary polynomials $\phi(\mathrm{x}) \in F_q[\mathrm{x}]$, $\psi(\mathrm{y}) \in F_q[\mathrm{y}]$, the polynomial $h(\mathrm{x}, \mathrm{y}) = \phi(\mathrm{x}) - \psi(\mathrm{y})$ is admissible for some (m, n) correspondence. The augmented rank of this correspondence satisfies the inequality $k_1 \leqslant q$.*

THEOREM 11.5. *An (m, n) correspondence possesses an admissible polynomial of the form $\phi(\mathrm{x}) - \psi(\mathrm{y})$ if and only if $k_1 \leqslant q$.*

Note that for (m, n) correspondences, $k \leqslant \min(q^m, q^n)$. Thus only if $m = 1$ or $n = 1$ will an admissible polynomial of the form $\phi(\mathrm{x}) - \psi(\mathrm{y})$ be "usual".

12. Admissible polynomials. A. (1, 1, 1) correspondences. Two admissible polynomials are *equivalent* if they are admissible for the same correspondence. Thus the totality of admissible polynomials breaks up into a number of equivalence classes. Clearly the number of equivalence classes is equal to the number of correspondences. Also two admissible polynomials $h_1(x, y, z)$, $h_2(x, y, z)$ are equivalent if and only if $(h_1(x, y, z))^{q-1} = (h_2(x, y, z))^{q-1}$. Moreover, if $h_1(x, y, z)$ and $h_2(x, y, z)$ are equivalent, then

$$h(x,y,z) = h_1(x,y,z)h_2(x,y,z) \tag{12.1}$$

is in the same equivalence class. Thus the polynomials in an equivalence class constitute a commutative group with respect to multiplication as defined by (12.1); the characteristic polynomial is the identity element of the group.

Let the partitions

$$A_0, A_1, \dots, A_k; \quad B_0, B_1, \dots, B_k; \quad C_0, C_1, \dots, C_k \tag{12.2}$$

define the (1, 1, 1) correspondence Γ. Also let

$$A_0, A_1, \dots, A_k; \quad B_0, B_1, \dots, B_k \tag{12.3}$$

and

$$B_0, B_1, \dots, B_k; \quad C_0, C_1, \dots, C_k \tag{12.4}$$

define the (1, 1) correspondences Γ_1 and Γ_2, respectively. The following theorem relates the characteristic polynomials of Γ, Γ_1, Γ_2.

THEOREM 12.1. *Let $f(x, y, z)$, $f_1(x, y)$, $f_2(y, z)$ denote the characteristic polynomials of Γ, Γ_1, Γ_2, respectively. Then*

$$f(x,y,z) = f_1(x,y) + f_2(y,z) - f_1(x,y)f_2(y,z). \tag{12.5}$$

THEOREM 12.2. *With the notation of Theorem 12.1, let $h(x, y, z)$ denote any admissible polynomial for Γ. Then there exist $h_1(x, y)$, $h_2(y, z)$, admissible polynomials for Γ_1, Γ_2, respectively, such that*

$$h(x,y,z) = h_1(x,y) + h_2(y,z) - h_1(x,y)h_2(y,z).$$

THEOREM 12.3. *The number of admissible polynomials for the correspondence defined by (12.2) is equal to*

$$(q-1)^e, \qquad e = q^3 - \sum_{i=1}^{k} |A_i|\cdot|B_i|\cdot|C_i|.$$

Two admissible pairs of polynomials are equivalent if they are admissible for the same correspondence.

THEOREM 12.4. *Given the (1, 1, 1) correspondence of augmented rank $k_1 \leqslant q$, two admissible pairs*

$$\phi(x) - \psi(y), \quad \psi(y) - \omega(z); \quad \phi_1(x) - \psi_1(y), \quad \psi_1(y) - \omega_1(z)$$

are equivalent if and only if

$$\phi_1(x) = f(\phi(x)), \quad \psi_1(y) = f(\psi(y)), \quad \omega_1(z) = f(\omega(z)),$$

where f is any function that is one-to-one when it is restricted to each of the images of ϕ, ψ, ω.

We remark that there are 32 admissible polynomials for $q = 2$.

B. (m, n) correspondences. We give only the following two results.

THEOREM 12.5. *The number of admissible polynomials for the (m, n) correspondences defined by*

$$F_q^m = A_0 \cup A_1 \cup \cdots \cup A_k, \qquad F_q^n = B_0 \cup B_1 \cup \cdots \cup B_k$$

is equal to

$$(q-1)^e, \qquad e = q^{m+n} - \sum_{i=1}^{k} |A_i|\cdot|B_i|.$$

THEOREM 12.6. *Given the (m, n) correspondence of augmented rank $k_1 \leqslant q$, two admissible polynomials $\phi(x) - \psi(y)$, $\phi_1(y) - \psi_1(y)$ are equivalent if and only if $\phi_1(\mathrm{x}) = f(\phi(\mathrm{x}))$, $\psi_1(\mathrm{y}) = f(\psi(\mathrm{y}))$, where f denotes any function that is one-to-one when it is restricted to each of the images of ϕ and ψ.*

We remark that there are 96 admissible (2, 1) polynomials for $q = 2$. For the tabulation, inclusing the corresponding partitions, see [**3**, §5].

13. Rank. A. (1, 1, 1) correspondences. The unique (1, 1, 1) correspondence of rank 0 is defined by $A_0 = B_0 = C_0 = F_q$. It has the characteristic polynomial $f(x, y, z) = 1$. The admissible polynomials are the $h(x, y, z)$ that never vanish; the number of such polynomials is $(q - 1)^{q^3}$.

The characteristic polynomial of the rank 1 correspondence defined by $A_1 = B_1 = C_1 = F_q$ is $f(x, y, z) = 0$; this is also the only admissible polynomial. The correspondence defined by

$$A_0 = B_0 = C_0 = \{0\}, \quad A_1 = B_1 = C_1 = F_q \setminus \{0\} \tag{13.1}$$

is of rank 1 and has characteristic polynomial $f(x, y, z) = 1 - x^{q-1}y^{q-1}z^{q-1}$. The number of admissible polynomials $3q^2 - 3q + 1$.

Another special case of rank 1 in a sense dual to (13.1) is

$$A_0 = B_0 = C_0 = F_q \setminus \{0\}, \quad A_1 = B_1 = C_1 = \{0\}. \tag{13.2}$$

It has characteristic polynomial

$$f(x, y, z) = 1 - (1 - x^{q-1})(1 - y^{q-1})(1 - z^{q-1}).$$

There are $(q - 1)^{q^3 - 1}$ admissible polynomials. In particular, $h(x, y, z) = x^{q-1} + y^{q-1} + z^{q-1}$ is admissible provided $(q, 3) = 1$. For $q = 3^t$, $t > 1$, it can be shown that

$$h(x, y, z) = x^{q-1} + \lambda y^{q-1} + \lambda^2 z^{q-1},$$

where $\lambda \in F_q \setminus F_3$, is admissible.

Similarly, for (13.1), $h(x, y, z) = 3 - x^{q-1} - y^{q-1} - z^{q-1}$ is admissible provided $(q, 3) = 1$. For $q = 3^t$, $t > 1$,

$$h(x, y, z) = 1 - \alpha x^{q-1} - \alpha y^{q-1} - (1 + \alpha) z^{q-1},$$

where $\alpha \in F_q \setminus F_3$, is admissible.

As an example of a rank 2 correspondence, we take

$$A_1 = B_1 = C_1 = \{0\}, \quad A_2 = B_2 = C_2 = F_q \setminus \{0\}. \tag{13.3}$$

The characteristic polynomial is

$$f(x, y, z) = x^{q-1} + y^{q-1} + z^{q-1} - y^{q-1}z^{q-1} - z^{q-1}x^{q-1} - x^{q-1}y^{q-1}.$$

For $q > 2$, the polynomial $h(x, y, z) = \alpha x^{q-1} + \beta y^{q-1} + \gamma z^{q-1}$, where $\alpha + \beta + \gamma = 0$, $\alpha\beta\gamma \neq 0$, is admissible.

The last few examples suggest that it would be of interest to determine those (1, 1, 1) correspondences that have admissible polynomials of the form

$$\phi(x) + \psi(y) + \omega(z). \tag{13.4}$$

B. (m, n) correspondences. For rank 1 we have generally the partitions

$$A_0, A_1; \quad B_0, B_1, \tag{13.5}$$

where $\alpha_i = |A_i|$, $\beta_i = |B_i|$, $\alpha_1 > 0$, $\beta_1 > 0$, $\alpha_0 + \alpha_1 = q^m$, $\beta_0 + \beta_1 = q^n$. Thus the number of correspondences is

$$\sum_{\alpha_1=1}^{q^m} \sum_{\beta_1=1}^{q^n} \binom{q^m}{1}\binom{q^n}{1} = (2^{q^m} - 1)(2^{q^n} - 1).$$

In particular, for $m = 2$, $n = 1$, the correspondence defined by $A_0 = \{(0, 0)\}$, $B_0 = \{0\}$, $A_1 = F_q^2 \setminus \{(0, 0)\}$, $B_1 = F_q \setminus \{0\}$ has the characteristic polynomial $1 - (x_1^{q-1} + x_2^{q-1} - x_1^{q-1}x_2^{q-1})y^{q-1}$. The correspondence defined by $A_0 = F_q^2 \setminus \{(0, 0)\}$, $B_0 = F_q \setminus \{0\}$, $A_1 = \{(0, 0)\}$, $B_1 = \{0\}$ has the characteristic polynomial $1 - (1 - x_1^{q-1})(1 - x_2^{q-1})(1 - y^{q-1})$. As for (13.2), the polynomial $x_1^{q-1} + x_2^{q-1} + y^{q-1}$ is admissible provided $(q, 3) = 1$. The case $q = 3^t$, $t > 1$, can be handled as for (13.2).

For (2, 1) correspondences of rank q, consider

$$A_1, \ldots, A_q; \quad B_1, \ldots, B_q, \tag{13.6}$$

where $A_i = \{(a_i, b_i - a_i)\}$, $B_i = \{b_i\}$ $(1 \leqslant i \leqslant q)$ and $F_q = b_1, \ldots, b_q$. An admissible polynomial is evidently $x_1 + x_2 - y$ and therefore

$$(x_1 + x_2 - y)^{q-1}$$

is characteristic.

14. Enumeration (compare §7 above). A. $(m_1, \ldots, m_r)$ correspondences. The general correspondence of rank k is defined by

$$F_q^{m_i} = A_{i0} \cup A_{i1} \cup \cdots \cup A_{ik} \qquad (1 \leqslant i \leqslant r), \tag{14.1}$$

together with

$$\begin{aligned} &\alpha_{ij} = |A_{ij}| \qquad (1 \leqslant i \leqslant r; 0 \leqslant j \leqslant k), \\ &\alpha_{i0} \geqslant 0, \quad \alpha_{ij} > 0 \qquad (1 \leqslant j \leqslant k), \end{aligned} \tag{14.2}$$

and

$$q^{m_i} = \sum_{j=0}^{k} \alpha_{ij} \qquad (1 \leqslant i \leqslant r). \tag{14.3}$$

The set of integers (α_{ij}) $(1 \leqslant i \leqslant r;\ 0 \leqslant j \leqslant k)$ satisfying (14.2) and (14.3) is said to characterize a *correspondence type*. Let $T(q^{m_1}, \ldots, q^{m_r}, k)$ denote the number of correspondence types of rank k. Also let $T(q^{m_1}, \ldots, q^{m_r})$ denote the total number of correspondence types.

THEOREM 14.1. *We have*

$$\begin{aligned} &\sum_{n_1, \ldots, n_r=0}^{\infty} \sum_{k} T(n_1, \ldots, n_r, k) x_1^{n_1} \cdots x_r^{n_r} z^k \\ &= (1 - x_1)^{-1} \cdots (1 - x_r)^{-1} \prod_{i_1, \ldots, i_r=1}^{\infty} (1 - x_1^{i_1} \cdots x_r^{i_r} z)^{-1}. \end{aligned} \tag{14.4}$$

Thus $T(q^{m_1}, \ldots, q^{m_r}, k)$ is equal to the number of rectangular arrays of positive integers (α_{ij}) $(1 \leqslant i \leqslant r;\ 1 \leqslant j \leqslant k)$ such that

$$\sum_{j=1}^{k} \alpha_{ij} \leqslant q^{m_i} \qquad (1 \leqslant i \leqslant r).$$

THEOREM 14.2. *We have*

$$\sum_{n_1,\dots,n_r=0}^{\infty} T(n_1,\dots,n_r)x_1^{n_1}\cdots x_r^{n_r} \tag{14.5}$$
$$= (1-x_1)^{-1}\cdots(1-x_r)^{-1}\prod_{i_1,\dots,i_r=1}^{\infty}\left(1-x_i^{i_1}\cdots x_r^{i_r}\right)^{-1}.$$

THEOREM 14.3. *The number of* $(m_1,\dots,m_r)$ *correspondences of rank* k *is equal to*

$$(k!)^{r-1}S(q^{m_1}+1,k+1)\cdots S(q^{m_r}+1,k+1),$$

where $S(n+1,k+1)$ *denotes a Stirling number of the second kind.*

THEOREM 14.4. *The number of* $(m_1,\dots,m_r)$*-admissible polynomials of rank* k *is equal to*

$$(k!)^{r-1}(q-1)^{m_1+\cdots+m_r}\sum_{i_1,\dots,i_r}\binom{q^{m_1}}{i_1}\cdots\binom{q^{m_r}}{i_r}S\left(i_1,\dots,i_r,k;(q-1)^{-1}\right),$$

where

$$(k!)^{r-1}\sum_{n_1,\dots,n_r=k}^{\infty}S(n_1,\dots,n_r,k;\lambda)\frac{x_1^{n_1}\cdots x_r^{n_r}}{n_1!\cdots n_r!}$$
$$=\left\{\sum_{n_1,\dots,n_r=1}^{\infty}\frac{x_1^{n_1}\cdots x_r^{n_r}}{n_1!\cdots n_r!}\lambda^{n_1\cdots n_r}\right\}^k.$$

REFERENCES

1. J. V. Brawley and L. Carlitz, *A characterization of the n × n matrices over a finite field*, Amer. Math. Monthly **80** (1973), 670–672; addendum, ibid., p. 1041. MR **47** #5046; **49** #355.

2. L. Carlitz, *Correspondences in a finite field*. I, Acta Arith. **27** (1975), 101–123. MR **51** #8083.

3. ———, *Correspondences in a finite field*. II, Indiana Univ. Math. J. **24** (1974/75), 785–811. MR **51** #8084.

4. ———, *The expansion of certain products*, Proc. Amer. Math. Soc. **7** (1956), 558–564. MR **19**, 29.

5. ———, *Invariantive theory of equations in a finite field*, Trans. Amer. Math. Soc. **75** (1953), 405–427. MR **15**, 291.

6. ———, *Invariant theory of systems of equations in a finite field*, J. Analyse Math. **3** (1954), 382–413. MR **16**, 115.

7. S. R. Cavior, *Equivalence classes of functions over a finite field*, Acta. Arith. **10** (1964/65), 119–136. MR **29** #1203.

8. ———, *Equivalence classes of sets of polynomials over a finite field*, J. Reine Angew. Math. **225** (1967), 191–202. MR **34** #4260.

9. L. E. Dickson, *General theory of modular invariants*, Trans. Amer. Math. Soc. **10** (1909), 123–158.

10. ———, *Linear groups*: *With an exposition of Galois field theory*, reprint, Dover, New York, 1958. MR **21** #3488.

11. Basil Gordon, *Two theorems on multipartite partitions*, J. London Math. Soc. **38** (1963), 459–464. MR **28** #1187.

12. P. M. MacMahon, *Combinatorial analysis*, vol. 2, Cambridge Univ. Press, Cambridge, 1916.

13. Gary L. Mullen, *Equivalence classes of polymonials over a finite field*, Acta Arith. **31** (1976), 353–358.

14. L. Rédei and T. Szele, *Algebraischzahlentheoretische Betrachtungen über Ringe*. I, Acta Math. **79** (1947), 291–320. MR **9**, 407.

15. D. P. Roselle, *Coefficients associated with the expansion of certain products*, Proc. Amer. Math. Soc. **45** (1974), 144–150. MR **49** #7152.

16. H. Werner, *Produkte von Kongruenzklassengeometrien universeller Algebren*, Math. Z. **121** (1971), 111–140. MR **43** #7396.

17. E. M. Wright, *Partitions of multi-partite numbers*, Proc. Amer. Math. Soc. **7** (1956), 880–890. MR **18**, 793.

18. ______ , *Partition of multipartite numbers into a fixed number of parts*, Proc. London Math. Soc. (3) **11** (1961), 499–510. MR **24** #A2573.

DEPARTMENT OF MATHEMATICS, DUKE UNIVERSITY, DURHAM, NORTH CAROLINA 27706