Setzen wir $X_0^2 = M_1 N$ so folgt sofort aus (16') wenn wir rechts jetzt nur die Glieder mit $X_0 < g_r \leqslant X$ nehmen, daß

$$\sum_{X_0 < g_r \leqslant X} g_1^{1-n} \sum_n \leqslant c \frac{d(\Gamma)}{J} X^n \sum |L(a)|^2 \tag{24}$$

wo $c$ nur in $\lambda$ und $M_1$ abhängt. Daraus folgt wieder ein Siebverfahren wo jetzt die Anzahl der Menge $\mathfrak{p}$ Gitter $\Gamma_r$ welche ausgenommen werden zu ersetzen ist durch $\sum_{\mathfrak{p}} \frac{d}{g_r^n}$ und diese ist also $\leqslant c_1 \frac{X^n}{\tau Z}$.

Die zweite Bemerkung die wir machen wollen, ist folgende: Wir haben stets angenommen, daß die $\Gamma_1, \ldots, \Gamma_K$ die Eigenschaft haben sollen, daß kein $\beta_{j,r} \equiv \beta_{l,s} \pmod{\Gamma}$ sein soll (wenn sie nicht kongruent 0 mod $\Gamma$ sind). Wir können jetzt allgemein annehmen, daß es ein festes $k$ gibt, so daß höchstens $k-1$ solche $\beta_{j,r} \equiv \beta_{l,s} \pmod{\Gamma}$ sind. Dann können wir (5) anwenden und es ist stets $M_1$ durch $M(\Gamma, f, k)$ zu ersetzen und z.B. in (16) ist noch ein Faktor $k$ rechts hinzuzufügen.

### Literaturverzeichnis


[1] H. Davenport and H. Halberstam, *The values of a trigonometric polynomial at well spaced points*, Mathematica 13 (1966), S. 91–96.

[2] P. D. T. A. Elliott, *An inequalities of Large Sieve type*, Acta Arith. 18 (1971), S. 405–422.

[3] P. X. Gallagher, *The large sieve and probabilistic Galois theory*, in print.

[4] E. Hlawka, *Bemerkungen zum großen Sieb von Linnik*, Österr. Akad. Wiss. Math.-Natur. Kl. S.-B. II 178 (1970), S. 13–18.

[5] — *Ausfüllung und Überdeckung konvexer Körper durch konvexe Körper*, Monatsh. Math. 53 (1949), S. 81–131.

[6] M. Huxley, *The large sieve inequality for algebraic number fields*, Mathematica 15 (1968), S. 178–187.

[7] E.G. Lekkerkerker, *Geometry of Numbers*, Amsterdam–London 1969; Groningen 1969.

[8] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Berlin–Heidelberg–New York 1971.

[9] C. L. Siegel, *Über Gitterpunkte in konvexen Körpern und ein damit zusammenhängendes Extremalproblem*, Acta Math. 65 (1935), S. 307–323.

[10] H. Weyl, *On geometry of numbers*, Proc. London Math. Soc. (2) 47 (1942), S. 268–289.

[11] S. Uchiyama, *The maximal large sieve*, Hokkaido Mathematical Journal 1 (2) (1972), S. 118–126.


*Eingegangen 21. 4. 1973* (397)

ACTA ARITHMETICA
XXVII (1975)

# Correspondences in a finite field, I*

by

L. Carlitz (Durham, N.C.)

*To the memory of Yu. V. Linnik*

**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. It has been proved recently [1] 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 $n \geqslant 1$. By a *generalized polynomial* is meant a sum of monomials of the type

$$a_0 x^{e_1} a_1 x^{e_2} \ldots a_{k-1} x^{e_k} a_k,$$

where $a_i \in R$, $e_i > 0$ and $k \geqslant 1$ but arbitrary.

With every function from $\mathrm{GF}(q)$ into itself we may associate a set of numbers $a_1, \ldots, a_k \in F_q = \mathrm{GF}(q)$ and a partition ([3], [4], [5])

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

where

$$A_i \cap A_j = \emptyset \quad (i \neq j); \tag{1.2}$$

the sets $A_i$ are non-vacuous and

$$f(b_i) = a_i \quad (b_i \in A_i). \tag{1.3}$$

For example, for the function $f(x) = x^{q-1}$, we have $k = 2$, $a_1 = 0$, $a_2 = 1$,

$$A_1 = \{0\}, \quad A_2 = \{a \mid a \in F_q, a \neq 0\}.$$

* Supported in part by NSF grant GP-17031.

We shall generalize the above in the following way. Let

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

denote partitions of $F_q$. It will be assumed that

$$A_1, \dots, A_k;\ B_1, \dots, B_k \tag{1.5}$$

are non-vacuous; however $A_0, B_0$ are not restricted. It is not difficult to show that there exists a polynomial $f(x, y) \in F_q[x, y]$ with the following property:

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

We shall say that $f(x, y)$ characterizes the *correspondence* $\Gamma$ 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* with respect to the correspondence $\Gamma$ induced by (1.4) provided $h(x, y)$ satisfies the following condition:

$$h(a, b) \begin{cases} = 0 & (a \in A_j,\ b \in B_j,\ 1 \leqslant j \leqslant k), \\ \neq 0 & (\text{otherwise}). \end{cases} \tag{1.7}$$

Clearly, if $h(x, y)$ is admissible, then

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

satisfies (1.6).

It should be noted that in (1.7) the nonzero values taken on by $h(x, y)$ are quite arbitrary. More precisely, $h(a, b)$, in the lower line, may depend on the particular pair $a$, $b$ and not merely on the set in which they lie.

As an example, the polynomial

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

is admissible. We have $k = 2$,

$$A_0 = B_0 = \emptyset, \quad A_1 = B_1 = \{0\}, \quad A_2 = B_2 = F_q \setminus \{0\}.$$

As a second example, the polynomial

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

is also admissible. In this instance, $k = 1$,

$$A_0 = B_0 = \{0\}, \quad A_1 = B_1 = F_k \setminus \{0\}.$$

As a simple example of a polynomial that is not admissible (for any partitions (1.4)), we cite $h(x, y) = xy$.



A basic problem is to characterize and enumerate all admissible polynomials. This is clearly a difficult problem. Consider for example the case of correspondences of rank $k = q$. Then each of the sets $A_1, \dots, A_q$; $B_1, \dots, B_q$ consists of a single element, while $A_0, B_0$ are vacuous. An admissible polynomial is evidently $h(x, y) = y - \varphi(x)$, where $\varphi(x)$ denotes some *permutation* polynomial.

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

$$h(x, y) = f(x) - g(y) \tag{1.8}$$

is admissible. Conversely given an arbitrary correspondence of rank $\neq q-1$, we shall show that there exists an admissible polynomial of the form (1.8). For rank $q-1$, however, such an admissible form may not exist when $A_0 \neq \emptyset$, $B_0 \neq \emptyset$; this is indeed the only exceptional case.

The present paper may be considered an introduction to the study of correspondences. We shall, in particular, determine the number of correspondences in $F_q$. The number of correspondences of rank $k$ is equal to

$$k!\{S(q+1, k+1)\}^2, \tag{1.9}$$

where $S(q+1, k+1)$ is a Stirling number of the second kind. We also obtain a generating function for correspondence types which suggests a connection with partitions of bipartites (Theorem 7.2). A rather complicated generating function for the number of admissible polynomials is obtained (Theorem 7.3). However we are unable to find a simple characterization of admissible polynomials. We hope to return to these and related questions as well as certain generalizations in later papers.

**2. Preliminaries.** We shall require the following

LEMMA 2.1. *Let $A$ denote an arbitrary non-vacuous subset of $F_q$. The polynomial*

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

*satisfies*

$$L_A(a) = \begin{cases} 1 & (a \in A), \\ 0 & (a \notin A). \end{cases} \tag{2.2}$$

The proof is immediate.

Let

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

denote partitions of $F_q$, where

$$A_1, \dots, A_k;\ B_1, \dots, B_k$$

are non-vacuous, while $A_0, B_0$ are arbitrary.

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

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

Proof. Put

$$g(x, y) = \sum_{j=1}^{k} L_{A_j}(x) L_{B_j}(y),$$

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

$$g(a, b) = \begin{cases} 1 & (a \in A_j, b \in B_j, 1 \leqslant j \leqslant k), \\ 0 & (\text{otherwise}). \end{cases}$$

Hence the polynomial

$$f(x, y) = 1 - g(x, y)$$

satisfies (2.4).

We shall say that $f(x, y)$ characterizes the correspondence defined by the partitions (2.3). Also a polynomial $h(x, y) \in F_q[x, y]$ is admissible (with respect to the correspondence defined by the partitions (2.3)) provided that

$$h(x, y) \begin{cases} = 0 & (a \in A_j, b \in B_j, 1 \leqslant j \leqslant k), \\ \neq 0 & (\text{otherwise}). \end{cases} \tag{2.5}$$

We state a few properties of admissible polynomials that follow immediately from the definition. In the first place, if $h(x, y)$ is admissible (relative to (2.3)), then clearly

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

characterizes the correspondence.

If $h(x, y)$ is admissible and $g(x, y)$ never vanishes, then $h(x, y)g(x, y)$ is also admissible.

If $h(x, y)$ is admissible and $\varphi(x), \psi(y)$ are permutation polynomials such that each $A_j$ is carried into itself by $\varphi(x)$ and each $B_j$ is carried into itself by $\psi(y)$, then the polynomial

$$h_1(x, y) = h\big(\varphi(x), \psi(y)\big)$$

is also admissible.

If $h(x, y)$ is admissible and $\varphi(x)$ is a polynomial that vanishes only for $x = 0$, then the polynomial

$$h_1(x, y) = \varphi\big(h(x, y)\big)$$



is also admissible. In particular

$$h_1(x, y) = \big(h(x, y)\big)^r \quad (r = 1, 2, 3, \ldots)$$

is admissible.

It should be pointed out that we shall use the terms *function* and *polynomial* interchangeably. Thus, if $f(x), g(x)$ are polynomials, the statement $f(x) = g(x)$ is short for

$$f(x) \equiv g(x) \pmod{x^q - x}.$$

A similar remark applies to polynomials in several variables: the statement $f(x, y) = g(x, y)$ is short for

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

A convenient form for the polynomial characterizing a correspondence is given by the following theorem.

THEOREM 2.3. *Put*

$$\varphi_i(x) = \prod_{a \in A_i} (x - a), \qquad \psi_i(y) = \prod_{b \in B_i} (y - b), \tag{2.6}$$

*so that*

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

*Then*

$$f(x, y) = 1 - \sum_{j=1}^{k} \frac{x^q - x}{\varphi_j(x)} \frac{y^q - y}{\psi_j(y)} \varphi_j'(x) \psi_j'(x). \tag{2.8}$$

*Conversely, if* $\varphi_j(x), \psi_j(y), j = 0, 1, \ldots, k$ *are any polynomials satisfying* (2.7) *and*

$$\deg \varphi_j(x) > 0, \qquad \deg \psi_j(y) > 0 \quad (j = 1, 2, \ldots, k),$$

*then the partitions defined by* (2.6) *and* (2.3) *give a correspondence with characteristic polynomial* (2.8).

**3. Some examples.** It is helpful to look at some examples of both admissible and non-admissible polynomials.

(i) If $g(x)$ is an arbitrary polynomial, then $h(x, y) = g(x) - y$ is admissible. Let $c_1, \ldots, c_k$ denote the range of $g(x)$ and put

$$F_q = A_1 \cup A_2 \cup \ldots \cup A_k \quad \text{where} \quad A_j = \{a \mid f(a) = c_j\} \quad (j = 1, \ldots, k).$$

Then $A_0$ is vacuous, while

$$B_j = \{a_j\} \quad (j = 1, \ldots, k), \qquad B_0 = F_q \setminus \bigcup_{j=1}^{k} B_j.$$

(ii) The polynomial $h(x, y) = x^2 - y^2$ is admissible. This is obvious if $q$ is even. For $q$ odd the sets $A_j$, $B_j$ are given by

$$\begin{cases} A_1 = \{0\},\ A_2 = \{\pm 1\},\ \dots \\ B_1 = \{0\},\ B_2 = \{\pm 1\},\ \dots \\ A_0 = B_0 = \emptyset. \end{cases}$$

(iii) The polynomial $h(x, y) = xy$ is not admissible for any partitions (2.3). More generally, the polynomial $h(x, y) = x^r y^s$ $(r \geqslant 1, s \geqslant 1)$ is not admissible for any partitions (2.3).

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

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

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

These two examples have already been cited in the Introduction.

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

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

Let $g(a_1, b_1) = 0$ for some $a_1 \in A_1$, $b_1 \in B_1$ but $g(a, b) \neq 0$ otherwise. Then $h(x, y)g(x, y)$ is admissible for the same correspondence. More generally let $g(a, b) \neq 0$ except possibly when

$$a_j \in A_j, \quad b_j \in B_j, \quad j \in \{1, 2, \dots, k\}. \tag{3.2}$$

(viii) Let $h(x, y)$ be admissible for (3.1) and let $g(a, b)$ vanish only as in (3.2). Then the polynomials

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

run through all the admissible polynomials defining the given correspondence. However the polynomials (3.3) need not be distinct.

**4. Normal forms.** As is evident from the above examples, in general there are numerous admissible polynomials for a given correspondence. The following theorem describes a normal form that is usually available.

THEOREM 4.1. *Let the partitions*

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

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

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

*where $f(x) \in F_q(x)$, $g(y) \in F_q[y]$.*



Proof. Choose $k+2$ distinct numbers $a_0, a_0', a_1, \dots, a_k \in F_q$. Since $k < q-1$, this is clearly possible. Next construct the polynomials $f(x)$, $g(y)$ such that

$$f(c) = \begin{cases} a_0 & (c \in A_0), \\ a_j & (c \in A_j, 1 \leqslant j \leqslant k), \end{cases}$$

$$g(c) = \begin{cases} a_0' & (c \in B_0), \\ a_j & (c \in B_j, 1 \leqslant j \leqslant k). \end{cases}$$

Then clearly $h(x, y)$ as defined by (4.2) is admissible relative to the partitions (4.1).

THEOREM 4.2. *Let the partitions*

$$A_1, \dots, A_q;\ B_1, \dots, B_q \tag{4.3}$$

*define a correspondence $\Gamma$ (so that each of the sets contains a single element of $F_q$). Then there exists an admissible polynomial of the form*

$$h(x, y) = f(x) - g(y) \tag{4.4}$$

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

Proof. The elements of $F_q$ may be numbered so that

$$A_j = \{a_j\}, \quad B_j = \{b_j\} \quad (1 \leqslant j \leqslant q).$$

Let $c_1, c_2, \dots, c_q$ denote an arbitrary numbering of the elements of $F_q$. Define $f(x)$, $g(y)$ by means of

$$f(a_j) = c_j, \quad g(b_j) = c_j \quad (1 \leqslant j \leqslant q).$$

(Explicitly we have

$$f(x) = \sum_{j=1}^{q} c_j\{1 - (x - a_j)^{q-1}\},$$

$$g(y) = \sum_{j=1}^{q} c_j\{1 - (y - b_j)^{q-1}\}.)$$

Then clearly the polynomial $h(x, y)$ defined by (4.4) is admissible for the correspondence.

In particular if we take $c_j = b_j$ it is clear that $g(y) = y$ and (4.4) becomes

$$h(x, y) = f(x) - y. \tag{4.5}$$

Alternatively we may take $c_j = a_j$ and then we have

$$h(x, y) = x - g(y). \tag{4.6}$$

THEOREM 4.3. *Let the partitions*

$$A_0, A_1, \ldots, A_{q-1};\ B_0, B_1, \ldots, B_{q-1} \tag{4.7}$$

*define a correspondence $\Gamma$ of rank $q-1$. Then, if either $A_0$ or $B_0$ is vacuous, there exists an admissible polynomial of the form*

$$h(x, y) = f(x) - g(y). \tag{4.8}$$

Proof. 1. Assume $B_0$ vacuous, $A_0$ not vacuous. Number the elements of $F_q$:

$$F_q = \{a_0, a_1, \ldots, a_{q-1}\}.$$

Construct polynomials $f(x), g(y)$ such that

$$f(c) = \begin{cases} a_0 & (c \in A_0), \\ a_j & (c \in A_j,\ 1 \leqslant j \leqslant q-1), \end{cases}$$

$$g(c) = a_j \quad (c \in B_j,\ 1 \leqslant j \leqslant q-1).$$

Then $h(x, y)$ as defined by (4.8) is admissible for (4.7).

2. Let $A_0$ and $B_0$ both be vacuous. Let $a_1, \ldots, a_{q-1}$ denote $q-1$ distinct numbers of $F_q$. Construct polynomials $f(x), g(y)$ such that

$$\begin{cases} f(c) = a_j & (c \in A_j,\ 1 \leqslant j \leqslant q-1), \\ g(c) = a_j & (c \in B_j,\ 1 \leqslant j \leqslant q-1). \end{cases}$$

Then $h(x, y)$ as defined by (4.8) is admissible.

THEOREM 4.4. *Let $f(x), g(y)$ be arbitrary polynomials with coefficients in $F_q$. Then*

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

*is admissible for some correspondence in $F_q$.*

Proof. Let $A$ denote the range of $f(x)$ and $B$ the range of $g(y)$. Put

$$C = A \cap B = \{c_1, \ldots, c_k\}.$$

Define

$$A_j = \{a \mid f(a) = c_j\} \qquad (1 \leqslant j \leqslant k),$$

$$B_j = \{b \mid g(b) = c_j\} \qquad (1 \leqslant j \leqslant k),$$

$$A_0 = F_q \setminus \bigcup_{j=1}^{k} A_j, \quad B_0 = F_q \setminus \bigcup_{j=1}^{k} B_j.$$

Then clearly $h(x, y)$ is admissible for the correspondence defined by the partitions

$$A_0, A_1, \ldots, A_k;\ B_0, B_1, \ldots, B_k. \tag{4.9}$$



We may now state

THEOREM 4.5. *Given the correspondence defined by the partitions* (4.9). *An admissible polynomial of the form*

$$h(x, y) = f(x) - g(y) \tag{4.10}$$

*exists if and only if*

(i) $k \neq q-1$, *or*

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

Thus, for a given correspondence, there usually exists an admissible polynomial of the form (4.10). To illustrate the exceptional case put

$$F_q = \{a_0 = 0, a_1, a_2, \ldots, a_{q-1}\},$$

$$A_j = B_j = \{a_j\} \qquad (0 \leqslant j < q). \tag{4.11}$$

In this correspondence it is clear that every nonzero element of $F_q$ remains unchanged. By Theorem 2.3, we have

$$\begin{aligned} f(x, y) &= 1 - \sum_{j=1}^{q-1} \{1-(x-a_j)^{q-1}\}\{1-(y-a_j)^{q-1}\} \\ &= 1 - \sum_{a \in F_q, a \neq 0} \{1-(x-a)^{q-1}\}\{1-(y-a)^{q-1}\}. \end{aligned}$$

Since

$$\begin{aligned} &\sum_{a \in F_q} \{1-(x-a)^{q-1}\}\{1-(y-a)^{q-1}\} \\ &\quad = -\sum_a (x-a)^{q-1} - \sum_a (y-a)^{q-1} + \sum_a (x-a)^{q-1}(y-a)^{q-1} \\ &\quad = 1+1-(x-y)^{q-1}-1 = 1-(x-y)^{q-1}, \end{aligned}$$

it follows that

$$f(x, y) = (1-x^{q-1})(1-y^{q-1}) + (x-y)^{q-1}. \tag{4.12}$$

Hence we have the following supplement to Theorem 4.5.

THEOREM 4.6. *In the exceptional case of Theorem* 4.5, *that is, $k = q-1$, $A_0 \neq \emptyset$, $B_0 \neq \emptyset$, the characteristic polynomial is given by*

$$f(x, y) = \{1-\varphi^{q-1}(x)\}\{1-\psi^{q-1}(y)\} + \{\varphi(x) - \varphi(y)\}^{q-1}, \tag{4.13}$$

*where $\varphi(x), \psi(y)$ denote arbitrary permutation polynomials.*

In the normal form

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

the polynomials $f(x), g(y)$ are obviously not unique since we may add the same constant to each. However there are usually additional possibilities. This is clear, for example, from the proof of Theorem 4.2 since the numbers $c_1, c_2, \ldots, c_q$ can be permutated. Let $c_1, c_2, \ldots, c_q$ denote some fixed ordering and let $c_1', c_2', \ldots, c_q'$ denote a permutation of these numbers. As in the proof of Theorem 4.1, define $f(x), g(x)$ by means of

$$f(a_j) = c_j, \quad g(b_j) = c_j \quad (1 \leqslant j \leqslant q). \tag{4.14}$$

Also define $f'(x), g'(y)$ by means of

$$f'(a_j) = c_j', \quad g'(b_j) = c_j' \quad (1 \leqslant j \leqslant q). \tag{4.15}$$

Then clearly the polynomial

$$h'(x, y) = f'(x) - g'(y) \tag{4.16}$$

is admissible for the correspondence defined by (4.3). Moreover if $\varphi(x)$ is the permutation polynomial defined by

$$\varphi(c_j) = c_j' \quad (1 \leqslant j \leqslant k), \tag{4.17}$$

then we have

$$f'(x) = \varphi\big(f(x)\big), \quad g'(y) = \varphi\big(g(y)\big). \tag{4.18}$$

Conversely, given that $f(x) - g(y)$ and $f'(x) - g'(y)$ are admissible for (4.3), then (4.18) holds for some $\varphi$. We may state

THEOREM 4.7. *Let $f(x) - g(y)$ be admissible for the correspondence defined by*

$$A_1, \ldots, A_q; B_1, \ldots, B_q.$$

*Then all admissible polynomials of the form $f'(x) - g'(y)$ are given by* (4.18), *where $\varphi(x)$ is a permutation polynomial.*

Remark. For other correspondences this theorem does not yield all admissible polynomials of the prescribed form. Let $k_1 = k, k+1, k+2$ according as none, one or both of the sets $A_0, B_0$ are non-vacuous. If $k_1 = q$, Theorem 4.7 applies without change. If however $k_1 < q$, $\varphi(x)$ need not be a permutation but is any function that carries an ordered set of $k_1$ numbers into another such set.

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

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

where

$$|A_i| = m_i, \quad |B_i| = n_i \quad (i = 0, 1, \ldots, k). \tag{5.2}$$



Two polynomials $h_1(x, y), h_2(x, y)$ are *equivalent* provided they are admissible for some correspondence. Thus the totality of admissible polynomials breaks up into a number of equivalence classes. The following theorems are immediate.

THEOREM 5.1. *The number of equivalence classes of admissible polynomials over $F_q$ is equal to the number of correspondences in $F_q$.*

THEOREM 5.2. *Two admissible polynomials $h_1(x, y), h_2(x, y)$ are equivalent if and only if*

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

THEOREM 5.3. *Let $h_1(x, y), h_2(x, y)$ be equivalent admissible polynomials. Then there exist polynomials $g(x, y)$ that take on arbitrary values for*

$$a \in A_j, \quad b \in B_j \quad (j = 1, 2, \ldots, k)$$

*but are uniquely determined elsewhere and such that*

$$h_1(x, y) = g(x, y) h_2(x, y).$$

*The number of such $g(x, y)$ is equal to*

$$q^e, \quad e = \sum_{j=1}^{k} m_j n_j, \tag{5.3}$$

*where $m_j, n_j$ are defined by* (5.2).

We have observed in the Introduction that the nonzero values of an admissible polynomial are otherwise arbitrary. Hence we have

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

$$(q-1)^{e'}, \quad e' = q^2 - \sum_{j=1}^{k} m_j n_j. \tag{5.4}$$

The polynomial $f(x, y)$ defined by

$$f(a, b) = \begin{cases} 0 & (a \in A_j, \, b \in B_j, \; 1 \leqslant j \leqslant k), \\ 1 & (\text{otherwise}) \end{cases} \tag{5.5}$$

is said to *characterize* the correspondence defined by (5.1). It is evidently uniquely determined by the correspondence and may be called the characteristic polynomial of the correspondence.

THEOREM 5.5. *Let $f(x, y)$ denote the characteristic polynomial of the correspondence defined by* (5.1). *A polynomial $h(x, y)$ is admissible for the correspondence if and only if*

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

THEOREM 5.6. *If $h_1(x, y)$, $h_2(x, y)$ are equivalent admissible polynomials for some correspondence $\Gamma$, then*

$$h(x, y) = h_1(x, y)h_2(x, y) \tag{5.7}$$

*is also admissible and is in the same equivalence class. Thus the polynomials in a fixed equivalence class constitute a commutative group with respect to multiplication as defined by* (5.7); *the identity element is the characteristic polynomial.*

Theorem 4.7 suggests the following question. When are two admissible polynomials of the type $f(x)-g(y)$ equivalent? The question is answered first for the special case of correspondences of rank $q$. However by the remark following Theorem 4.7, the general case is covered by the following result.

THEOREM 5.7. *Given the correspondence $\Gamma$ defined by*

$$A_0, A_1, \dots, A_k;\ B_0, B_1, \dots, B_k. \tag{5.8}$$

*Let $k_1 = k$, $k+1$ or $k+2$ according as none, one or both of the sets are non-vacuous. Assume $k_1 \leqslant q$. Then two admissible polynomials $f(x)-g(y)$, $f'(x)-g'(y)$ are equivalent if and only if*

$$f'(x) = \varphi\big(f(x)\big), \quad g'(y) = \varphi\big(g(y)\big), \tag{5.9}$$

*where $\varphi(x)$ denotes any function that carries an ordered set of $k_1$ numbers into another such set.*

| 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 | $A_1 = B_1 = \{0\}$, $A_2 = B_2 = \{1\}$<br>$A_1 = B_2 = \{0\}$, $A_2 = B_1 = \{1\}$ | $x+y$<br>$x+y+1$ |



**6. Rank.** It is clear from the definition that the rank of a correspondence may take on any value between 0 and $q$, inclusive. We shall determine the number of correspondences of a given rank in the next section. We begin the present section by examining some special cases.

In the first place, for rank $k = 0$, it is clear that we have the unique correspondence defined by

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

We may state the following theorem.

THEOREM 6.1. *The admissible polynomials for the unique correspondence of rank 0 are the polynomials $h(x, y)$ that never vanish. The number of such polynomials is*

$$(q-1)^{q^2}. \tag{6.2}$$

*The characteristic polynomial for this correspondence is*

$$f(x, y) = 1. \tag{6.3}$$

Consider next the correspondence defined by

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

so that $k = 1$. It is evident from the proof of Theorem 2.2 that in this case the characteristic polynomial is $f(x, y) = 0$. We have therefore

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

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

*Hence this is also the only admissible polynomial for the correspondence.*

There are of course additional correspondences of rank 1. In general we have, for rank 1,

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

together with

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

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

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

In general the characteristic and admissible polynomials for these correspondences are not simple. However in certain cases simple results are obtained, for example, assume that

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

We find that the characteristic polynomial for (6.9) is (see example (v) of § 3)

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

The admissible polynomials for this correspondence are given by

$$c_0(1-x^{q-1})(1-y^{q-1})+(1-x^{q-1})\sum_{a\neq 0} c_a\{1-(y-a)^{q-1}\}+ \\ +(1-y^{q-1})\sum_{a\neq 0} c'_a\{1-(x-a)^{q-1}\}, \tag{6.11}$$

where $a$ runs through the nonzero elements of $F_q$ and $c_0$, $c_a$, $c'_a$ are arbitrary nonzero numbers of $F_q$. Thus the number of admissible polynomials is equal to

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

in agreement with (5.4).

Another special case of rank 1 that may be mentioned is

$$A_0 = B_0 = F_q\setminus\{0\}, \quad A_1 = B_1 = \{0\}. \tag{6.13}$$

We now have the characteristic polynomial

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

The admissible polynomials are given by

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

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

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

in agreement with (5.4).

We remark 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 an admissible polynomial for (6.13). By Theorem 4.5, an admissible polynomial of this kind, that is, $f(x)+g(y)$, cannot be found for $q=2$. However for $q=2^t$, $t>1$, let $\lambda$ denote any number of $F_q$ except 0 or 1. Then

$$(x^{q-1}+\lambda y^{q-1})^{q-1} = x^{q-1}+y^{q-1}+(\lambda+\lambda^2+\ldots+\lambda^{q-2})x^{q-1}y^{q-1}.$$

Since

$$\lambda+\lambda^2+\ldots+\lambda^{q-2} = \frac{\lambda-\lambda^{q-1}}{1-\lambda} = -1$$



we get

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

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

As for the correspondence defined by (6.9), it is easily verified, that for $q$ odd, the polynomial

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

is admissible. Indeed, since

$$(2-x^{q-1}-y^{q-1})^{q-1} = \sum_{r=0}^{q-1} 2^{q-r-1}(x^{q-1}+y^{q-1})^r \\ = 1+\sum_{r=1}^{q-1} 2^{q-r-1}\{x^{q-1}+y^{q-1}+(2^r-2)x^{q-1}y^{q-1}\},$$

we get for the characteristic polynomial

$$f(x,y) = 1-x^{q-1}y^{q-1}. \tag{6.17$'$}$$

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

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

Therefore, with the indicated choice of $\alpha$, $\beta$, the polynomial $1+\alpha x^{q-1}+\beta y^{q-1}$ is admissible for (6.9). This is again in agreement with Theorem 4.5.

It was stated in example (vi) of § 3 that the polynomial

$$h(x,y) = x^{q-1}-y^{q-1} \tag{6.18}$$

is admissible. In this case we have the correspondence of rank 2 defined by

$$A_0 = B_0 = \emptyset, \quad A_1 = B_1 = \{0\}, \quad A_2 = B_2 = F_q\setminus\{0\}. \tag{6.19}$$

The characteristic polynomial for (6.19) is

$$f(x,y) = x^{q-1}+y^{q-1}-2x^{q-1}y^{q-1}. \tag{6.20}$$

For rank $k=q$, we have $A_0 = B_0 = \emptyset$ and the correspondence is defined by

$$A_1, \ldots, A_q; B_1, \ldots, B_q, \tag{6.21}$$

where each of the sets contains a single element. As proved in Theorem 4.2 an admissible polynomial for this correspondence is furnished by

$$h(x, y) = \varphi(x) - \psi(y), \tag{6.22}$$

where $\varphi(x)$, $\psi(y)$ denote permutation polynomials. Of special interest is the case of the *identity* correspondence, that is,

$$A_i = B_i \quad (i = 1, 2, \ldots, q). \tag{6.23}$$

Clearly $x-y$ is admissible and the characteristic polynomial is

$$f(x, y) = (x-y)^{q-1}. \tag{6.24}$$

The general admissible polynomial is given by

$$h(x, y) = \sum_{a \neq b} c_{a,b}\{1-(x-a)^{q-1}\}\{1-(y-b)^{q-1}\}, \tag{6.25}$$

where the summation is over all $a, b \in F_q$, $a \neq b$ and the $c_{a,b}$ are arbitrary nonzero numbers of $F_q$. The number of admissible polynomials is evidently

$$(q-1)^{q^2-q} \tag{6.26}$$

in agreement with Theorem 5.4.

To get the number of correspondences (6.21) we first distribute the numbers of $F_q$ in the sets $A_1, \ldots, A_q$ in some arbitrary but fixed manner. Hence the number of correspondences is the number of ways of distributing the numbers of $F_q$ in the sets $B_1, \ldots, B_q$, that is, $q!$.

We have seen in § 4 that correspondences of rank $k = q-1$ with $A_0 \neq \emptyset, B_0 \neq \emptyset$ are exceptional in that admissible polynomials of the type $f(x)-g(y)$ do not exist. In particular if we put $F_q = \{a_0 = 0, a_1, a_2, \ldots, a_{q-1}\}$ and take

$$A_j = B_j = \{a_j\} \quad (0 \leqslant j < q), \tag{6.27}$$

we have seen that

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

is admissible. It is easily verified that $h(x, y)$ is indeed characteristic. The general admissible polynomial for (6.27) is given by

$$h(x, y) = c_{0,0}(1-x^{q-1})(1-y^{q-1}) + \sum_{\substack{i,j=0 \\ i \neq j}}^{q-1} c_{ij}\{1-(x-a_i)^{q-1}\}\{1-(y-a_i)^{q-1}\}, \tag{6.29}$$



where the $c_{ij}$ are arbitrary nonzero numbers of $F_q$. Thus the total number of admissible polynomials is

$$(q-1)^{q^2-q+1} \tag{6.30}$$

in agreement with (5.4).

Finally we remark that the polynomial

$$h(x, y) = (1-x^{q-1})y + x(1-y^{q-1}) \tag{6.31}$$

is admissible for the correspondence of rank 2 defined by (6.19).

**7. Enumerations.** As above we consider the partitions

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

and put

$$m_i = |A_i|, \quad n_i = |B_i| \quad (i = 0, 1, \ldots, k), \tag{7.2}$$

where

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

and

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

The set of integers

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

satisfying (7.3) and (7.4) are said to characterize a *correspondence type* of rank $k$.

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

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

where

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

Changing the notation, we put

$$\begin{cases} m = m_0 + \sum ie_{ij} & (m_0 \geqslant 0), \\ n = n_0 + \sum je_{ij} & (n_0 \geqslant 0), \\ k = \sum e_{ij}. \end{cases} \tag{7.8}$$

The $e_{ij}$ count the number of pairs $(A_s, B_t)$ with $|A_s| = i$, $|B_t| = j$.

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

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

and

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

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

We first construct a generating function for $N(m, n, k)$:

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

To begin with, it is evident that

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

We have

$$\sum_{i,j=1}^{\infty} \sum_{e_{ij}=0}^{\infty} \frac{x^{\Sigma i e_{ij}} y^{\Sigma j e_{ij}} z^{e_{ij}}}{\prod e_{ij}! (\prod i! \prod j!)^{e_{ij}}} = \exp \sum_{i,j=1}^{\infty} \frac{x^i y^j z}{i!\, j!} = \exp\{z(e^x - 1)(e^y - 1)\}.$$

It therefore follows that

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

We recall that

$$(e^x - 1)^k = k! \sum_{n=k}^{\infty} S(n, k) \frac{x^n}{n!}, \tag{7.13}$$

where

$$S(n, k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^{n-k} \binom{k}{j} j^n \tag{7.14}$$

denotes a Stirling number of the second kind. Thus, by (7.12),

$$\begin{aligned} F(x, y, z) &= e^{x+y} \sum_{k=0}^{\infty} \frac{z^k}{k!} (e^x - 1)^k (e^y - 1)^k \\ &= e^{x+y} \sum_{k=0}^{\infty} k!\, z^k \sum_{m,n=0}^{\infty} S(m, k) S(n, k) \frac{x^m y^n}{m!\, n!}. \end{aligned}$$



Comparing this with (7.11) we get

$$N(m, n, k) = \sum_{i=0}^{n} \sum_{j=0}^{n} \binom{m}{i} \binom{n}{j} S(i, k) S(j, k). \tag{7.15}$$

It follows from (7.13) that

$$\begin{aligned} k! \sum_{n=0}^{\infty} \frac{x^n}{n!} \sum_{j=0}^{n} \binom{n}{j} S(j, k) &= (e^x - 1)^{k+1} + (e^x - 1)^k \\ &= (k+1)! \sum_{n=k+1}^{\infty} S(n, k+1) \frac{x^n}{n!} + k! \sum_{n=k}^{\infty} S(n, k) \frac{x^n}{n!}, \end{aligned}$$

so that

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

by the familiar recurrence for Stirling numbers of the second kind. Hence (7.15) becomes

$$N(m, n, k) = k!\, S(m+1, k+1) S(n+1, k+1). \tag{7.16}$$

Thus the number of sets $A_i, B_j$ satisfying (7.6) and (7.8), with $k$ fixed, has been evaluated in terms of Stirling numbers of the second kind.

If we define

$$N(m, n) = \sum_{k} N(m, n, k), \tag{7.17}$$

so that $N(m, n)$ denotes the total number of sets $A_i, B_j$ satisfying (7.6) and (7.8), $k = 0, 1, 2, \ldots$, then we have

$$N(m, n) = \sum_{k=0}^{\min(m,n)} k!\, S(m+1, k+1) S(n+1, k). \tag{7.18}$$

It does not seem possible to 'sum' the series on the right of (7.18).

Turning next to $T(m, n, k)$, it is clear from (7.8) that

$$T(m, n, k) = \sum_{r=0}^{m} \sum_{s=0}^{n} T'(r, s, k), \tag{7.19}$$

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

$$r = \sum i e_{ij}, \quad s = \sum j e_{ij}, \quad k = \sum e_{ij}. \tag{7.20}$$

If we put

$$\begin{aligned} G(x, y, z) &= \sum_{m,n,k} T(m, n, k) x^m y^n z^k, \\ G'(x, y, z) &= \sum_{m,n,k} T'(m, n, k) x^m y^n z^k, \end{aligned} \tag{7.21}$$

it follows from (7.19) that

$$G(x,y,z) = (1-x)^{-1}(1-y)^{-1}G'(x,y,z). \tag{7.22}$$

By (7.20) we have

$$G'(x,y,z) = \sum_{i,j,e_{ij}} x^{\sum ie_{ij}} y^{\sum je_{ij}} z^{e_{ij}}.$$

For fixed $i, j$, we have

$$\sum_{e_{ij}} x^{ie_{ij}} y^{je_{ij}} z^{e_{ij}} = (1-x^iy^jz)^{-1}.$$

It follows that

$$G'(x,y,z) = \prod_{i,j=1}^{\infty} (1-x^iy^jz)^{-1} \tag{7.23}$$

and therefore, by (5.22),

$$G(x,y,z) = (1-x)^{-1}(1-y)^{-1} \prod_{i,j=1}^{\infty} (1-x^iy^jz)^{-1}. \tag{7.24}$$

By means of (7.23) we get an interesting combinatorial interpretation of $T'(m,n,k)$. Expanding each factor on the right of (7.23), it is clear that $T'(m,n,k)$ is the number of pairs of positive integers $(i_s, j_s)$ such that

$$\begin{cases} i_1+i_2+\dots+i_k = m, \\ j_1+j_2+\dots+j_n = n. \end{cases} \tag{7.25}$$

Another way of putting it is that $T'(m,n,k)$ is the number of partitions of the bipartite $(m,n)$ into $k$ positive parts. In view of (7.19), it is clear that $T(m,n,k)$ is equal to the number of pairs of positive integers $(i_s, j_s)$ such that

$$\begin{cases} i_1+i_2+\dots+i_k \leqslant m, \\ j_1+j_2+\dots+j_k \leqslant n. \end{cases} \tag{7.26}$$

Next put

$$T(m,n) = \sum_k T(m,n,k). \tag{7.27}$$

Then (7.24) becomes

$$\sum_{m,n=0}^{\infty} T(m,n)x^my^n = \prod_{i+j>0} (1-x^iy^j)^{-1}. \tag{7.28}$$



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

$$\begin{cases} i_1+i_2+i_3+\dots = m, \\ j_1+j_2+j_3+\dots = n, \end{cases} \tag{7.29}$$

or, if we prefer, the number of unrestricted partitions of the bipartite $(m,n)$.

For references to partitions of multipartite numbers see, for example, [2], [6], [7], [8], [9], [10].

We now apply the above results to the enumeration of correspondences and correspondence types. It suffices to take $m=n=q$. We may state the following theorems.

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 equal to*

$$\sum_{k=0}^{q} k!\{S(q+1,k+1)\}^2.$$

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

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

*Thus $T(q,q,k)$ is equal to the number of pairs of positive integers $(i_s, j_s)$ such that*

$$\begin{cases} i_1+i_2+\dots+i_k \leqslant q, \\ j_1+j_2+\dots+j_k \leqslant q. \end{cases}$$

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

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

*Thus $T(q,q)$ is equal to the number of pairs $(i_s, j_s)$, $i_s+j_s>0$, such that*

$$\begin{cases} i_1+i_2+i_3+\dots = q, \\ j_1+j_2+j_3+\dots = q. \end{cases}$$

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

$$N(m,n,k;\lambda) = \sum \frac{m!\,n!\,\lambda^{\sum ije_{ij}}}{m_0!\,n_0!\prod e_{ij}!(\prod i!\prod j!)^{e_{ij}}}, \tag{7.30}$$

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

$$F(x, y, z; \lambda) = \sum_{m,n,k=0}^{\infty} N(m, n, k; \lambda) \frac{x^m y^n}{m!\, n!} z^k. \tag{7.31}$$

Then, exactly as in the proof of (7.12), we have

$$F(x, y, z; \lambda) = e^{x+y} \exp\left\{ z \sum_{i,j=1}^{\infty} \frac{x^i y^j}{i!\, j!} \lambda^{ij} \right\}. \tag{7.32}$$

Put

$$\left( \sum_{i,j=1}^{\infty} \frac{x^i y^j}{i!\, j!} \lambda^{ij} \right)^k = k!\, k! \sum_{m,n=0}^{\infty} S(m, n, k; \lambda) \frac{x^m y^n}{m!\, n!}, \tag{7.33}$$

so that

$$S(m, n, k; 1) = S(m, k) S(n, k). \tag{7.34}$$

Clearly

$$N(m, n, k; \lambda) = k! \sum_{i=0}^{m} \sum_{j=0}^{n} \binom{m}{i} \binom{n}{j} S(i, j, k; \lambda). \tag{7.35}$$

Applying Theorem 5.4 we get

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

$$k!(q-1)^{q^2} \sum_{i,j=0}^{q} \binom{q}{i} \binom{q}{j} S\big(i, j, k; (q-1)^{-1}\big). \tag{7.36}$$

Unfortunately the $S(m, n, k; \lambda)$ are not easily computed. However we have

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

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

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

It follows from (7.36) that the number of admissible polynomials of rank 0 is $(q-1)^q$; the number of rank 1 is

$$\sum_{i,j=1}^{q} (q-1)^{q^2-ij}$$

in agreement with earlier results.



## References


[1] J. V. Brawley and L. Carlitz, *A characterization of the $n \times n$ matrices over a finite field*, Amer. Math. Monthly, 80 (1973), pp. 670–672. Addendum, ibidem p. 1041.

[2] L. Carlitz, *The expansion of certain products*, Proc. Amer. Math. Soc. 7 (1956), pp. 550–564.

[3] — *Invariant theory of equations in a finite field*, Trans. Amer. Math. Soc. 75 (1953), pp. 405–427.

[4] — *Invariant theory of systems of equations in a finite field*, J. Analyse Math. 3 (1953/54), pp. 382–413.

[5] S. R. Cavior, *Equivalence classes of functions over a finite field*, Acta Arith. 10 (1964), pp. 119–136.

[6] Basil Gordon, *Two theorems on multipartite partitions*, J. London Math. Soc. 38 (1963), pp. 459–463.

[7] P. M. MacMahon, *Combinatory Analysis*, vol. 2, Cambridge 1916.

[8] D. P. Roselle, *Coefficients associated with the expansion of certain products*, Proc. Amer. Math. Soc., to appear.

[9] E. M. Wright, *Partitions of multipartite numbers*, Proc. Amer. Math. Soc. 7 (1956), pp. 880–890.

[10] — *Partitions of multipartite numbers into a fixed number of parts*, Proc. London Math. Soc. 11 (1961), pp. 499–510.


*Received on 28. 5. 1973* (405)