ANNALES
POLONICI MATHEMATICI
XXXVII (1980)

The solution of a system of quadratic functional equations

by J. A. LESTER (Waterloo)

Abstract. For a set G with binary operation $*$, and an algebraically closed field F, the solution of the system of quadratic functional equations

$$g_k(\alpha * \beta) = \sum_{i,j=1}^{N} \Gamma_k^{ij} g_i(\alpha) g_j(\beta)$$

satisfied by the N functions $g_k\colon G \to F$, is determined in terms of additive and multiplicative functions from G to F, under certain assumptions on F, G, and the $\Gamma_k^{ij} \in F$.

1. Introduction. We consider the system of N quadratic functional equations given by

$$g_k(\alpha * \beta) = \sum_{i,j=1}^{N} \Gamma_k^{ij} g_i(\alpha) g_j(\beta). \tag{1.1}$$

The domain of $g_1, \ldots, g_N$ is a set G upon which is defined the operation $*$, while the range is an algebraically closed field F ($\Gamma_k^{ij} \in F$).

Equation (1.1) has been studied extensively under various hypotheses on $(G, *)$, F and the functions g_k: for examples and further references see [1], [3]–[7]. In this note, we shall assume the following:

I. $\Gamma_k^{ij} = \Gamma_k^{ji}$.

II. $\sum_{k=1}^{N} \Gamma_k^{ij} \Gamma_h^{km} = \sum_{k=1}^{N} \Gamma_k^{im} \Gamma_h^{kj}$.

III. There exist $e_1, \ldots, e_N \in F$ such that

$$\sum_{i=1}^{N} \Gamma_k^{ij} e_i = \delta_k^j.$$

IV. F has characteristic 0 or $\geqslant N$.

V. The operation $*$ has identity θ, and all $\alpha \in G$ have inverses.

Assumptions I, II and III are not completely arbitrary, being consequences of the following (see [6]):

LEMMA 1.1. *If* (1.1) *has a solution consisting of linearly independent functions, then*

(i) *if* $*$ *is commutative,* I *holds,*

(ii) *if* $*$ *is associative,* II *holds,*

(iii) *if* $*$ *has identity* θ, III *holds.*

Proof. Let $\bar{g}_1, \ldots, \bar{g}_k$ be the linearly independent solution. Then, if $*$ is commutative

$$\begin{aligned} 0 &= \bar{g}(\alpha*\beta) - \bar{g}(\beta*\alpha), \qquad \alpha, \beta \in G, \\ &= \sum_{i,j=1}^{N} \Gamma_k^{ij} \bar{g}_i(\alpha)\bar{g}_j(\beta) - \sum_{i,j=1}^{N} \Gamma_k^{ij} \bar{g}_i(\beta)\bar{g}_j(\alpha) \\ &= \sum_{i,j=1}^{N} [(\Gamma_k^{ij} - \Gamma_k^{ji})\bar{g}_i(\alpha)]\bar{g}_j(\beta). \end{aligned}$$

Two applications of linear independence give I; the proofs of (ii) and (iii) are similar (in (iii), $e_k = \bar{g}_k(\theta)$). □

We could consequently replace I, II, III and V by the assumptions that (1.1) has a linearly independent solution and that $(G, *)$ is an abelian group. However, as we shall see later, for some G and F, (1.1) has only linearly dependent solutions.

Equation (1.1) and its solution may be stated in a somewhat more algebraic form. Let $(F^N, +,)$ denote the vector space of N-tuples over F, and define multiplication on F^N as follows: for $a = (a_1, \ldots, a_N)$, $b = (b_1, \ldots, b_N) \in F^N$,

$$(a \circ b)_k = \sum_{i,j=1}^{N} \Gamma_k^{ij} a_i b_j .$$

We may thus consider each N-tuple of F^N to be the components of elements of an algebra $(\tilde{F}, +, \circ,)$, and the Γ_k^{ij}'s to be the multiplication constants of $\tilde{F}$, all with respect to some given basis. From assumptions I, II and III, $\tilde{F}$ is commutative, associative, and has an identity with components $(e_1, \ldots, e_N)$, which we denote by e. The functions $g_1, \ldots, g_N$ may now be considered as components of a mapping $g: G \to \tilde{F}$ satisfying

$$g(\alpha*\beta) = g(\alpha) \circ g(\beta). \tag{1.2}$$

The main result of this note is the solution of this equation:

THEOREM. (i) *There is no loss in generality in assuming that* $(\tilde{F}, +, \circ)$ *is a local ring (i.e. that it has a unique maximal ideal).*

(ii) *If* $(\tilde{F}, +, \circ)$ *is a local ring, then the general solution of* (1.2) *is given by*

$$g(\alpha) = \pi(\alpha)\exp[a(\alpha)],$$

where

(a) $\pi\colon G \to F$ *is multiplicative, i.e.*

$$\pi(\alpha * \beta) = \pi(\alpha)\pi(\beta),$$

(b) $a\colon G \to \tilde{F}$ *is additive, i.e.*

$$a(\alpha * \beta) = a(\alpha) + a(\beta),$$

(c) *for all* $\alpha \in G$, $a(\alpha)$ *is nilpotent, i.e.* $[a(\alpha)]^k = 0$ *for some positive integer* $k \leqslant N$ (*and hence the sum*

$$\exp[a(\alpha)] = \sum_{k=0}^{\infty} \frac{1}{k!}[a(\alpha)]^k$$

is actually finite).

Note. 1° In Section 3, it will be shown that V may be replaced by the assumption that $\pi(\alpha) \neq 0$ for all $\alpha \in G$.

2° In Section 2, the set of nilpotents of $\tilde{F}$ is shown to be a $(N-1)$-dimensional sub-algebra of $\tilde{F}$. Thus with respect to some basis (not necessarily the original one) the mapping $a\colon G \to \tilde{F}$ has as components $(a_1, \ldots, a_{N-1}, 0)$, where $a_1, \ldots, a_{N-1}$ are additive functions from G to F. This solution is therefore an improvement over that in [6], where the solution to (1.1) is expressed in terms of an $N \times N$ matrix A of additive functions from G to F satisfying $A(\alpha)A(\beta) = A(\beta)A(\alpha)$ for all $\alpha, \beta \in G$, the characterization of which is itself an unsolved problem.

2. Decomposition of elements of $\tilde{F}$. Much of the algebra used in this section can be found in [2]. The author is indebted to a referee for considerable condensation and modernization of the following discussion.

Since $(\tilde{F}, +, \circ,)$ is finite dimensional, $(\tilde{F}, +, \circ)$ is an Artinian ring, and thus may be decomposed into a finite direct sum of local Artinian rings. Then g may be decomposed into a corresponding sum of mappings, each satisfying (1.2), which proves part (i) of the theorem. We assumo from now on that $(\tilde{F}, +, \circ)$ is local.

The unique maximal ideal $\tilde{N}$ of $(\tilde{F}, +, \circ)$ is its radical, and so consists of all the nilpotents of $(\tilde{F}, +, \circ)$. The algebra $(\tilde{F}, +, \circ,)$ may be decomposed as $\tilde{F} = \tilde{H} + \tilde{N}$, where $\tilde{H}$ is a subalgebra of $\tilde{F}$ isomorphic to $\tilde{F}/\tilde{N}$, and $\tilde{H} \cap \tilde{N} = \{0\}$. But since F is algebraically closed and $\tilde{N}$ is a maximal ideal, $\tilde{F}/\tilde{N}$ is a field isomorphic to F, and so the subalgebra $\tilde{H}$ consists of all F-multiples of e. Then any $x \in \tilde{F}$ has a unique decomposition of the form $x = \lambda(x)e + n$ for some $n \in \tilde{N}$ and $\lambda(x) \in F$.

It is clear that the subalgebra $(\tilde{N}, +, \circ,)$ has dimension $N-1$ and that $\lambda(x) = 0$ iff $x \in \tilde{N}$. We now derive some further properties of the function $\lambda\colon \tilde{F} \to F$.

LEMMA 2.1. *For all* $x, y \in \tilde{F}$, $a, b \in F$

(i) $\lambda(x \circ y) = \lambda(x)\lambda(y)$,

(ii) $\lambda(ax+by) = a\lambda(x)+b\lambda(y)$,

(iii) $\lambda(e) = 1$.

Proof. We prove (i) only; the proof of (ii) is similar, and that of (iii) trivial. There exist $n, m, k \in \tilde{N}$ so that $x = \lambda(x)e+n$, $y = \lambda(y)e+m$, and $x \circ y = \lambda(x \circ y)e+k$. Consequently, $x \circ y = \lambda(x)\lambda(y)e+\lambda(y)n+\lambda(x)m+$ $+m \circ n$, and so $[\lambda(x \circ y)-\lambda(x)\lambda(y)]e = \lambda(x)m+\lambda(y)n+m \circ n-k \in \tilde{N}$, which yields (i). □

We note that since $(\tilde{F}, +, \circ)$ is a local ring, its only idempotents are 0 and e. Also, since any $n \in \tilde{N}$ satisfies $n^k = 0$ for some integer k, the minimum polynomial $m(t)$ of n must divide t^k. Thus $m(t) = t^r$ for some integer r. Since $r \leqslant N$, it follows that $n^r = 0$ for some integer r *no greater than* N.

3. Solution of equation (1.2). We first note that (1.2) has the trivial solution $g(\alpha) = 0$ for all $\alpha \in G$, which is of the required form with $\pi(\alpha) = 0$ for all $\alpha \in G$. We exclude this case from further consideration.

Define the mapping $\pi: G \to F$ by $\pi(\alpha) = \lambda[g(\alpha)]$. Then from Lemma 2.1, (i) and equation (1.2), π is multiplicative, i.e. $\pi(\alpha * \beta)$ $= \pi(\alpha)\pi(\beta)$.

Equation (1.2) shows that $g(\theta)$ is idempotent; thus either $g(\theta) = 0$ or $g(\theta) = e$. If $g(\theta) = 0$, then $g(\beta) = g(\theta) \circ g(\beta) = 0$ for all $\beta \in G$, which is the case we have excluded from consideration. Hence $g(\theta) = e$, and so for any $\alpha \in G$, $\pi(\alpha)\pi(\alpha^{-1}) = \pi(\theta) = \lambda[g(\theta)] = \lambda(e) = 1$. Thus $\pi(\alpha) \neq 0$ for all $\alpha \in G$.

Note. Since this last statement is the only consequence of V we need, we may replace V by the assumption that $\pi(\alpha) \neq 0$ for any $\alpha \in G$.

For any $\alpha \in G$, define $b(\alpha) = [\pi(\alpha)]^{-1}[g(\alpha)-\lambda\{g(\alpha)\}e]$; then

$$g(\alpha) = \pi(\alpha)[e+b(\alpha)] \tag{3.1}$$

and $b(\alpha) \in \tilde{N}$. The sum

$$a(\alpha) = \ln[e+b(\alpha)] = \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k}[b(\alpha)]^k$$

is well defined (for $k \geqslant N$, $[b(\alpha)]^k = 0$, and since F has characteristic 0 or $\geqslant N$, we may divide by all $k < N$). Also, $a(\alpha) \in \tilde{N}$, and the sum

$$\exp[a(\alpha)] = \sum_{k=0}^{\infty} \frac{1}{k!}[a(\alpha)]^k$$

is also well defined (for $k \geqslant N$, $[a(\alpha)]^k = 0$, and because F has characteristic 0 or $\geqslant N$, we may divide by all $k < N$, and hence by $k!$ for $k < N$).

But $\exp[a(a)] = \exp[\ln(e+b(a))] = e+b(a)$, which, together with equation (3.1), implies that

$$g(a) = \pi(a)\exp[a(a)].$$

It is easily verified that $a\colon G \to \tilde{N}$ is additive. Conversely, if $\pi\colon G \to F$ is any multiplicative function, and $a\colon G \to \tilde{N}$ is any additive function, then $g\colon G \to \tilde{F}$, defined by (3.1) is a solution of (1.2).

Finally, we give an example of a set $(G, *)$ and a field F for which (1.1) has no linearly independent solution. Assume $N \geqslant 2$, $(G, *)$ is finite with k elements, and F is a field of characteristic $> k$. For any fixed $a \in G$, some two of $a, 2a = a*a, \ldots, (k+1)a$ are equal, i.e. $pa = qa$ for some $0 < q < p \leqslant k+1$, and hence, if $f\colon G \to \tilde{F}$ is any additive function, $pf(a) = qf(a)$. But $0 < p-q \leqslant k$, and $(p-q)f(a) = 0$, so since F has characteristic $> k$, $f(a) = 0$. Thus the only additive function from G to $\tilde{F}$ is the zero function, and the only solutions of (1.2) are (subject to I–V) $g(a) = 0$ for all $a \in G$ and $g(a) = \pi(a)e$, both of which are linearly dependent.

References

[1] J. Aczél, *Lectures on functional equations and their applications*, Academic Press, 1966.

[2] M. F. Atiyah and I. G. MacDonald, *Introduction to commutative algebra*, Addison-Wesley, 1966.

[3] D. Z. Djoković, *A theorem on semigroups of linear operators*, Publications de l'Institut Mathématique de Beograd, Nouvelle Série 3 (17) (1963), p. 129–130.

[4] M. Kuczma and A. Zajtz, *Quelques remarques sur l'équation fonctionnelle matricielle de Cauchy*, Colloq. Math. 18 (1967), p. 159–168.

[5] J. A. Lester, *A canonical form for a system of quadratic functional equations*, ibidem 35 (1976), p. 105.

[6] M. A. McKiernan, *General solution of quadratic functional equations*, Aequationes Math. (to appear) (see Short Communications 14, issue 3).

[7] — *Measurable solutions of quadratic functional equations*, Colloq. Math. 35 (1976), p. 97.

UNIVERSITY OF WATERLOO

Reçu par la Rédaction le 5. 2. 1976