Pacific Journal of Mathematics

SOLUTION OF LOOP EQUATIONS BY ADJUNCTION

RAFAEL ARTZY

Vol. 13, No. 2 April 1963

SOLUTION OF LOOP EQUATIONS BY ADJUNCTION

R. ARTZY

Solutions of integral equations over groups by means of adjunction of new elements have been studied by B. H. Neumann [3] and F. Levin [2]. Here an analogous question for loops will be dealt with, and the results will prove to be useful also for groups.

Let $(L, .)$ be a loop with neutral element e, x an indeterminate. Let w be a word whose letters are x and elements of L. Let n be the number of times that x appears in w. Form $f(x)$ from w by inserting parentheses between its letters so as to make it into a uniquely defined expression if juxtaposition means loop multiplication. The equation $f(x)=r$, r in L, will be called *an integral loop equation in x of degree n.*

An integral loop equation $f(x) = r$ is *monic* if $f(x)$ is a product of two factors both containing x. Every integral loop equation can be made monic by a finite number of left or right divisions by elements of L.

Not every integral loop equation has a solution as indicated by the monic example $x^2 = r$, $r \neq e$, L the four-group. Our aim is finding a loop E in which L is embedded and in which $f(x) = r$ has a solution. The loop E used here will be an extension loop [1] of L by $(C_n, +)$, the cyclic group of order n. The construction follows the

Extension Rule. The elements of E are ordered couples (c, a) where $c \in C_n$, $a \in L$. Equality of couples is componentwise. The multiplication in E is defined by $(c_1, a_1)(c_2, a_2) = (c_1 + c_2, a_1 a_2 \cdot h(c_1, c_2))$, where $h(c_1, c_2)$ is an element of L depending on c_1 and c_2, assuming the value e except in the case when $c_1 + c_2 = 0$ and $c_1 \neq 0$.

THEOREM 1. *A monic integral loop equation $f(x) = r$ of degree n over a loop L has a solution in an extension loop $E = (C_n, L)$ constructed according to the Extension Rule, with $f(e)h(c, n - c) = r$ whenever $c \neq 0$.*

Proof. If the element b of L is represented in E by $(0, b)$, L is mapped isomorphically into E. Let x be represented in E by $(1, e)$, where 1 is a generator of C_n. All elements of C_n will be written as integers. Then $f(x)$ can be constructed by stages. For every x entering into the successive multiplication one summand 1 appears in the first component. In the second component only the loop elements of $f(x)$ will appear as factors because x has the second component e. The h's

Received April 6, 1962.

do not enter the picture until the last step because they depend on the first components, and all multiplications but the last yield $h(c_1, c_2) = e$ in view of $0 \leqq c_1 + c_2 < n$. Thus, at first, the construction of the second component of $f(x)$ in E follows exactly the pattern of the successive multiplication which yielded $f(x)$, with the exception of the factor x. The result is, therefore, the same as though x had been replaced by e, namely $f(e)$. However, the last product, one of whose factors contains by definition at least one x, requires a factor $h(c, n-c)$, $0 < c < n$. Thus the final result is $(n, f(e)h(c, n - c)) = (0, r)$ and consequently $f(e)h(c, n - c) = r$, $c \neq 0$.

THEOREM 2. *An integral loop equation of degree n has in E at least $\varphi(n)$ solutions, φ being Euler's function. For each two of these solutions, x and y, there exists an automorphism of E carrying x into y and leaving L unchanged elementwise.*

Proof. Let again $x = (1, e)$. If k and n are relatively prime, (k, e) is another solution because $nk = 0$ and $h(m, q) = h(km, kq)$ since $m = 0$ or $\neq 0$ according to $km = 0$ or $\neq 0$. There are $\varphi(n)$ distinct k's with the properties $0 < k < n$ and $(k, n) = 1$. This proves the first part of the theorem. Now, $1 \to k$ is an automorphism of C_n preserving the 0-element and hence also the h's. The loop L is unaffected by these automorphisms, because they act only on the first components.

DEFINITION. An *abelian integral identity* over a loop L is an equation $u(w) = v(w')$, where (i) w and w' are words using the same set of elements of L, but not necessarily in the same order, (ii) $u(w)$ and $v(w')$ are formed from w and w', respectively, by inserting parentheses between the letters of the words so as to make them into uniquely defined expressions if juxtaposition means loop multiplication, (iii) the equality is preserved when the loop elements forming w and w' are replaced by arbitrary elements of L.

In general the validity of abelian integral identities in L, like associativity or the Moufang property, does not carry over into E. However, in the case of degree 2 we are able to obtain the following result.

THEOREM 3. *Let an integral equation of degree 2 over a loop L have the monic form $f(x) = r$. Every abelian integral identity valid in L will hold also in the extension loop E, constructed as in Theorem 1, provided $h(1, 1) = [f(e)]\backslash r$ lies in the center of L.*

Proof. The first component of the elements of E is 1 or 0. Moreover, $h(0, 1) = h(1, 0) = h(0, 0) = 1$; write $h(1, 1) = h$, for short. We have

then $h(p, q) = h^{pq}$, where pq is the product of p and q in $GF(2)$, and $h^0 = e$, $h^1 = h$. The addition in $C_2 = \{0, 1\}$ is the addition of $GF(2)$. The loop elements h^0 and h^1 multiply according to the rule $h^p h^q = h^{p+q}$, and, by the hypothesis of the theorem, they lie in the center of L.

Now, the abelian integral identity $u(w) = v(w')$ in E would surely be satisfied for the first components since they behave as elements of C_2, an abelian group. If in the second components the h's are disregarded, the abelian integral identity over E yields an exact replica of the same identity over L. But, as center elements of L, the h's appearing in u and v can indeed be pulled out and shifted to the right of each side. We denote the product of the h's of u by $h^{H(u)}$. In the degenerate case where u consists of one letter only, we define $H(u) = 0$. We have to prove for the second components that $u(w)h^{H(u)} = v(w')^{H(v)}$. Since $u(w) = v(w')$ it will be sufficient to prove $H(u) = H(v)$.

Let the first components of the elements of w be $p_1, \cdots, p_m$. We claim now that $H(u) = \sum_{i\ j=1, i<j}^{m} p_i p_j$, independent of the order of the p's, and that therefore $H(u) = H(v)$. For $m = 2$ we have trivially $H(u) = p_1 p_2$. For $m = 3$, $h^{H(u)} = h^{p_1 p_2} h^{(p_1+p_2)p_3} = h^{p_1 p_2 + p_1 p_3 + p_2 p_3}$. Suppose $H(u) = \sum_{i,j=1, i<j}^{m'} p_i p_j$ has been proved for every word length $m' < m$. If the last multiplication of $u(w)$ is $u'u''$, where u' is a product of $p_1, \cdots, p_k$ and u'' of $p_{k+1}, \cdots, p_m$, then the induction hypothesis yields $H(u') = \sum_{i\ j=1, i<j}^{k} p_i p_j$ and $H(u'') = \sum_{i,j=k+1, i<j}^{m} p_i p_j$. Then

$$\begin{aligned} H(u) &= H(u') + H(u'') + (p_1 + \cdots + p_k)(p_{k+1} + \cdots + p_m) \\ &= \sum_{i,j=1, i<j}^{k} p_i p_j + \sum_{i,j=k+1, i<j}^{m} p_i p_j \\ &\quad + (p_1 + \cdots + p_k)(p_{k+1} + \cdots + p_m) = \sum_{i,j=1, i<j}^{m} p_i p_j . \end{aligned}$$

This completes the proof.

COROLLARY. *The equation $xax = r$ over a group G has a solution in an extension group $E = (C_2, G)$ constructed as in Theorem* 1, *provided $a^{-1}r$ lies in the center of G. In particular the equation has always a solution in E if G is abelian.*

REFERENCES

1. R. H. Bruck, *Some results in the theory of linear non-associative algebras*, Trans. Amer. Math. Soc., **56** (1944), 141-199.

2. F. Levin, *Solution of equations over groups*, Bull. Amer. Math. Soc., **68** (1962), 603-604.

3. B. H. Neumann, *Adjunction of elements to groups*, J. London Math. Soc., **18** (1943), 12-20.

RUTGERS, THE STATE UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RALPH S. PHILLIPS
Stanford University
Stanford, California

J. DUGUNDJI
University of Southern California
Los Angeles 7, California

M. G. ARSOVE
University of Washington
Seattle 5, Washington

LOWELL J. PAIGE
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

E. F. BECKENBACH
T. M. CHERRY
D. DERRY
M. OHTSUKA
H. L. ROYDEN
E. SPANIER
E. G. STRAUS
F. WOLF

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY
UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY
CALIFORNIA RESEARCH CORPORATION
SPACE TECHNOLOGY LABORATORIES
NAVAL ORDNANCE TEST STATION

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is $18.00; single issues, $5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $8.00 per volume; single issues $2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics
Vol. 13, No. 2 April, 1963

Rafael Artzy, *Solution of loop equations by adjunction* 361
Earl Robert Berkson, *A characterization of scalar type operators on reflexive Banach spaces* 365
Mario Borelli, *Divisorial varieties* 375
Raj Chandra Bose, *Strongly regular graphs, partial geometries and partially balanced designs* 389
R. H. Bruck, *Finite nets. II. Uniqueness and imbedding* 421
L. Carlitz, *The inverse of the error function* 459
Robert Wayne Carroll, *Some degenerate Cauchy problems with operator coefficients* 471
Michael P. Drazin and Emilie Virginia Haynsworth, *A theorem on matrices of* 0*'s and* 1*'s* 487
Lawrence Carl Eggan and Eugene A. Maier, *On complex approximation* 497
James Michael Gardner Fell, *Weak containment and Kronecker products of group representations* 503
Paul Chase Fife, *Schauder estimates under incomplete Hölder continuity assumptions* 511
Shaul Foguel, *Powers of a contraction in Hilbert space* 551
Neal Eugene Foland, *The structure of the orbits and their limit sets in continuous flows* 563
Frank John Forelli, Jr., *Analytic measures* 571
Robert William Gilmer, Jr., *On a classical theorem of Noether in ideal theory* 579
P. R. Halmos and Jack E. McLaughlin, *Partial isometries* 585
Albert Emerson Hurd, *Maximum modulus algebras and local approximation in* C^n 597
James Patrick Jans, *Module classes of finite type* 603
Betty Kvarda, *On densities of sets of lattice points* 611
H. Larcher, *A geometric characterization for a class of discontinuous groups of linear fractional transformations* 617
John W. Moon and Leo Moser, *Simple paths on polyhedra* 629
T. S. Motzkin and Ernst Gabor Straus, *Representation of a point of a set as sum of transforms of boundary points* 633
Rajakularaman Ponnuswami Pakshirajan, *An analogue of Kolmogorov's three-series theorem for abstract random variables* 639
Robert Ralph Phelps, *Čebyšev subspaces of finite codimension in* $C(X)$ 647
James Dolan Reid, *On subgroups of an Abelian group maximal disjoint from a given subgroup* 657
William T. Reid, *Riccati matrix differential equations and non-oscillation criteria for associated linear differential systems* 665
Georg Johann Rieger, *Some theorems on prime ideals in algebraic number fields* . . . 687
Gene Fuerst Rose and Joseph Silbert Ullian, *Approximations of functions on the integers* 693
F. J. Sansone, *Combinatorial functions and regressive isols* 703
Leo Sario, *On locally meromorphic functions with single-valued moduli* 709
Takayuki Tamura, *Semigroups and their subsemigroup lattices* 725
Pui-kei Wong, *Existence and asymptotic behavior of proper solutions of a class of second-order nonlinear differential equations* 737
Fawzi Mohamad Yaqub, *Free extensions of Boolean algebras* 761