MTA Számítástechnikai és Automatizálási Kutató Intézete, **Közlemények 25/1982**

THE SOLUTION OF HOSSZÚ-EQUATION OVER FINITE FIELDS*

János Bagyinszki

University of Gödöllő

1. PRELIMINARIES

M. Hosszú [H-67] considered the functional equation

$$f(x+y-xy)+f(xy)=f(x)+f(y) \tag{1.1}$$

with real variables x,y,f and solved it under the assumption that $f: \mathbb{R} \to \mathbb{R}$ is a differentiable function on the set $\mathbb{R}$ of real numbers. Several authors investigated equation (1.1). There have been two directions of generalization.

Weakening of the conditions for the function $f: \mathbb{R} \to \mathbb{R}$ was the first direction of generalizations; e.g. requiring the continuity at certain points [S-68.a] or, supposing integrability [D-69], [S-68.b]. Let us consider the well-known Jensen-equation

$$f\left(\frac{x+y}{2}\right)=f(x)+f(y) \tag{1.2}$$

and the Cauchy-equation

$$f(x+y)=f(x)+f(y) \tag{1.3}.$$

The equivalence of equations (1.1) and (1.2), and of equations (1.1) and (1.3) - has been proved for the sets

---

* Presented at the Kolloquium "Diskrete Mathematik und Anvendungen in der Mathematischen Kybernetik", Rostock, 30.3.1981-3.4.1981.

$\{f \mid f: \mathbb{R} \to \mathbb{R}\}$, $\{f \mid f: \mathbb{C} \to \mathbb{C}\}$ in the papers [S-68.b], [B-70], [D-71] and [V-69] ($\mathbb{C}$ denotes the field of complex numbers).

Some generalizations of the equation (1.1) and its solutions have been given in the papers [F-69], [L-72] and [L-74].

The definition and solution of the equation (1.1) over an algebraic structure (different from the field of real or complex numbers) is the second direction of generalizations. By the end of this section F,R,e,G denotes a field, a commutative ring with identity, identity of the field or ring and an Abelian group, respectively. In Świątak's paper [S-71] it has been shown that: if F is a field, whose characteristic is not 2 or 3, G is an Abelian group without 2-torsion and for every fixed $g \in G$ there is a homomorphism $\chi: F^{+} \to G$ such that $\chi(e)=g$, then equation (1.1) is equivalent to equation

$$2f(x+y)=f(2x)+f(2y) \tag{1.2'}$$

for functions $f: F \to G$. Aczél noticed [S-71] that Balnuša's proof for functions $f: \mathbb{C} \to \mathbb{C}$ is also valid for functions $f: F \to F$, if F is a quadratic closed field with certain additional conditions. In Davison's paper [D-74.a] functions of the type $f: R \to G$ have been investigated, where R is one of the three rings Z (rational integers), $Z/_{kZ}$ (integers mod k) and Q (the field of rational numbers). In case of $|F| \geq 5$, the equivalence of equation (1.1) and the equation

$$f(x+y)+f(0)=f(x)+f(y) \tag{1.3'}$$

has been proved in [D-74.b] for functions $f: F \to G$. Finally, if R is additively generated by their units and there exists a unit element $u \in R$ such that $e-u$ and $e-u-u^{-1}$ are units, then the equations (1.1) and (1.3') are equivalent for functions $f: R \to G$ if and only if, the equations (1.1) and (1.3') are equivalent for the functions $f': R/_{2R} \to G$.

2. RESULTS

We prove that, over a finite field, the class of generalized Hosszú-functions and the class of quasi-linear functions of $|F|$-valued logic are the same (in connection to our earlier results [B-D-76], [B-79], see also [R-77]). This fact refute a statement of [D-R-80], which asserts that for $|F|\leq 4$ there exists a Hosszú-function which is not a solution of the equation (1.3'). Our proof is entirely different from the proof of [D-74.b]; it is less complicated but it is valid only for a restricted domain. However, our proof is valid for n-ary functions, too. To the present knowledge of the author, the generalized Hosszú-functions have been introduced first in this paper.

For finite fields we solve a problem of H.Świątak and remark that we can extend the proofs to fields of characteristic p. Some of the proofs can be extended to more general classes of functions, $\{f \mid f:R\to G\}$. However, in this paper, the statement is restricted to finite fields. To formulate our theorems we need some defintions.

Let $R=\langle R;+,\cdot\rangle$ and $R'=\langle R';\oplus,\odot\rangle$ be commutative rings with identity, denote $G=\langle G;\boxplus\rangle$ and N an Abelian group and the set of non-negative integers, respectively. For a function $f:R^n\to G$ $(n\in N)$ we define the Hosszú-operator with the identity

$$H_{\tilde{x},\tilde{y}}\tilde{f}=f(\tilde{x}+\tilde{y}-\tilde{x}\tilde{y}) \boxplus f(\tilde{x}\tilde{y}) \boxminus f(\tilde{x}) \boxminus f(\tilde{y}), \qquad \text{where}$$

$\tilde{x}=(x_1,\ldots,x_n)$, $\tilde{x}+\tilde{y}=(x_1+y_1,\ldots,x_n+y_n)$, $\tilde{x}\cdot\tilde{y}=(x_1y_1,\ldots,x_ny_n)$.
We call the equation

$$H_{\tilde{x}\tilde{y}}\tilde{f}=0 \tag{2.1}$$

and their solutions (generalized) Hosszú-equation, and (generalized) Hosszú-functions, respectively.

It is easy to see that the following two lemmas hold:

Lemma 1: (1) The constant functions are Hosszú-functions.

(2) For every pair of functions (f_1,f_2) of the type $R^n \to G$ and every numbers $n_1,n_2 \in N$, the equality $H(n_1 f_1 \boxplus n_2 f_2)=n_1 \cdot Hf_1 \boxplus n_2 \cdot Hf_2$ is an identity.

Lemma 2: For every pair of functions (f_1,f_2) of the type $R^n \to R'$ and every constants $c_1,c_2 \in R'$, the equality $H(c_1 \odot f_1 \oplus c_2 \odot f_2)=c_1 \odot Hf_1 \oplus c_2 \odot Hf_2$ is an identity.

Further on, let $q=p^\alpha$, where p is a prime, $\alpha \geq 1$ integer, $F_q=GF(q)$.

Theorem 1: The function $f:F_q \to F_q$ is a Hosszú-function if and only if, f is a polynomial function of the form:

$$f(x)=\sum_{i=0}^{\alpha-1} a_i x^{p^i} + a_\alpha . \qquad (2.2)$$

Sketch of the proof: The functions of the form (2.2) are solutions of the equation (2.1) by the lemmas 1. and 2., because the identity $(a+b)^{p^i} = a^{p^i} + b^{p^i}$ holds for rings of characteristic p. We have an indirect proof for the necessity of the condition (2.2) using the automorphism-group of F_q. We mention that this method could also be applied to fields of characteristic p.

Using this theorem and lemmas we have.

Theorem 2: The function $f:F_q^n \to F_q$ is a Hosszú-function if and only if, f is a polynomial function of the form

$$f(\tilde{x})=\sum_{j=1}^{n} \sum_{i=1}^{\alpha-1} a_{ij} x_j^{p^i} + a_\alpha . \qquad (2.3)$$

The next theorem solves a problem of Świątak (P.2. in [S-71]) if f is a function of the type $f:F_q \to F_q$. The theorem is formulated for unary functions and finite fields, but it can be extended to n-ary functions and fields of characteristic p in a similar way as it could be done to theorem 1.

Theorem 3: Let $P_i(x,y)+Q_i(x,y)=T(x,y)$, $i=1,2$ and $P_1 \neq P_2$ be two partitions of a polynom $T(x,y)$ over F_q. Assume that for every elements $u,v \in F_q^*$ the system of equations $P_1(x,y)=u$, $Q_1(x,y)=v$ has a solution (x,y). Then the function f is a solution of the equation

$$f(P_1(x,y))+f(Q_1(x,y))=f(P_2(x,y))+f(Q_2(x,y)) \qquad (2.4)$$

if and only if, f is a polynomial function of the form (2.2).

Remark: The sets A_q of functions $f:F\to F$ with $|F|\leq 4$ which are not a solution of equation (1.3'):

$$A_2=\emptyset,\ A_3=\{f(x)=a_o+a_1x+a_2x^2 \mid a_2\neq 0\} \text{ and}$$

$$A_4=\{f(x)=b_o+b_1x+b_2x^2+x^3\}.$$

It is easy to see that no elements of A_q $(q=3,4)$ are solutions of equation (1.1).

R E F E R E N C E S

A-66 Aczél, J., Lectures on Functional Equations and Their Applications, A.P., 1966.

H-67 Hosszú, M., $f(x+y-xy)+f(xy)=f(x)+f(y)$ (unpublished) Colloquium of Functional Equations, Zakopane, 1967.

S.68.a Świątak, H., On the functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Mat. Vesnik 5 (20), (1968), 177-182.

S-68.b Świątak, H., Remarks on the functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Aequationes Math., 1, (1968), 239-241.

D-69 Daróczy, Z., Über die Funktonalgleichung $f(xy)+f(x+y-xy)=f(x)+f(y)$, Publ. Math. Debrecen, 16, (1969), 129-132.

V-69 Vincze, E., 17. Bemerkung zum Vortrag von Herrn prof. Fenyő. Aequationes Math. 2 (1969), 374.

F-69 Fenyő, I., On the general solution of a functional equations in the domain of distributions, Aequationes Math., 3 (1969), 236-246.

B-70 Blanuša, D., The functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Aequationes Math., 5, (1970), 63-67.

D-71 Daróczy, Z., On the general solution of the functional equation $f(x+y-xy)+f(xy)=f(x)+f(y)$, Aequationes Math., 6, (1971), 130-132.

S-71 Świątak, H., A proof of the equivalence of the equation $f(x+y-xy)+f(xy)=f(x)+f(y)$ and Jensen's equation Aequationes Math., 6, (1971), 24-29.

L-72 Lajkó, K., Über die allgemeinen Lösungen der Funktionalgleihung F(x)+F(y)-F(xy)=H(x+y-xy), Publ. Math. (Debrecen) 19, (1972), 219-223.

L-74 Lajkó, K., Applications of extensions of additive functions, Aequationes Math. 11, (1974), 68-76.

D-74.a Davison, T.M.K., On the functional equation f(m+n-mn)+f(mn)=f(m)+f(n), Aequationes Math., 10, (1974), 206-211.

D-74.b Davison, T.M.K., The complete solution of Hosszú's functional equation over a field, Aequationes Math., 11, (1974), 273-276.

B-D-76 Bagyinszki, J. and Demetrovics, J., The structure of linear classes in prime valued logics (Hungarian) MTA-SzTAKI Közlemények, 16/1976, 25-52.

R-77 Rosenberg, I.G., Completeness properties of multiple--valued logic algebras, in "Computer Science and Multiple-valued Logic" (Ed, D.D. Rine) North Holland, 1977, 144-186.

B-79 Bagyinszki, J., Teh lattice of closed classes of linear functions over a finite ring of square--free order, Dept. of Math. Karl Marx Univ. of Economics, Bp. 1979-2., 1-21.

D-R-80 Davison, T.M.K. and Redlin, L., Hosszú's functional equation over rings generated by their units Aequationes Math., 20, (1980), 318-320.

ÖSSZEFOGLALÁS

Az irodalomban szereplő Hosszú-egyenletet általánositjuk többváltozós függvényekre, s az általánositott Hosszú-egyenletet megoldjuk véges testek fölött értelmezett függvényekre. A megoldásokat általánositott Hosszú-függvényeknek nevezzük.

Megmutatjuk, hogy véges testek fölött az általánositott Hosszú-függvények osztálya azonos a k-értékü logikai kvázi-lineáris függvényeinek osztályával (1. és 2. tétel).

Eredményeink megcáfolják Davison egy állitását.

Véges testek esetére megoldjuk Świątak egy problémáját, más irányba jelentősen általánositva a Hosszú-egyenletet (3. tétel).

Megjegyezzük, hogy a bizonyitások átvihetők p-karakterisztikáju testekre.

Р Е З Ю М Е

Бадински Янош

Уравнение, названное в литературе о М. Госсу, расширяется на функции со многими переменными и решается в случае функций, определенных над конечными полями. Решения называются обобщенными функциями Госсу.

Показывает, что над конечными полями класс обобщенных функций Госсу совпадает с классом квази-линейных функций к-значной логики. /Теоремы 1. и 2./

Эти результаты отрицают одно утверждение Дависона. Решается одна проблема Швиатака в случае конечных полей. При этом дается другое обобщение уравнения Госсу. /Теорема 3./

Заметим, что метод доказательств можно применить и в случае полей характеристикой р.