Novi Sad J. Math.
Vol. 43, No. 1, 2013, 59-71

ON A SUM FORM FUNCTIONAL EQUATION AND ITS RELEVANCE IN INFORMATION THEORY AND CRYPTANALYSIS

Prem Nath[1] **and Dhiraj Kumar Singh**[2]

Abstract. The general solutions of a sum form functional equation containing two unknown mappings have been obtained. The importance of these solutions in information theory and cryptanalysis has also been discussed.

AMS Mathematics Subject Classification (2010): 39B22, 39B52

Key words and phrases: The entropies of degree α, additive mapping, multiplicative mapping, concentration measure of order α

1. Introduction

For $n = 1, 2, 3, \ldots$; let

$$\Gamma_n = \left\{ (x_1, \ldots, x_n) : 0 \leq x_i \leq 1, i = 1, \ldots, n; \sum_{i=1}^{n} x_i = 1 \right\}$$

denote the set of all n-component complete discrete probability distributions with nonnegative elements. Throughout the sequel; $\mathbb{R}$ will denote the set of all real numbers; $I = \{x \in \mathbb{R} : 0 \leq x \leq 1\} = [0, 1]$, the unit closed interval and $\Delta = \{(x, y)\colon\ 0 \leq x \leq 1, 0 \leq y \leq 1, 0 \leq x + y \leq 1\}$, the unit closed triangle.

The main objective of this paper is to study the functional equation

$$\text{(FE1)} \qquad \sum_{i=1}^{n} \sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + \sum_{i=1}^{n} f(p_i) \sum_{j=1}^{m} g(q_j)$$

in which $f : I \to \mathbb{R}$, $g : I \to \mathbb{R}$ are mappings, $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$, and $n \geq 3$, $m \geq 3$ are arbitrary but fixed integers.

To begin with, we mention some situations which motivate us to study (FE1).

(I) The functional equation

$$(1.1) \quad \sum_{i=1}^{n} \sum_{j=1}^{m} G(p_i q_j) = \sum_{i=1}^{n} G(p_i) + \sum_{j=1}^{m} G(q_j) + \lambda \sum_{i=1}^{n} G(p_i) \sum_{j=1}^{m} G(q_j)$$

[1]Department of Mathematics, University of Delhi, Delhi 110007, India,
e-mail: pnathmaths@gmail.com
[2]Department of Mathematics, Zakir Husain Delhi College (University of Delhi), Jawaharlal Nehru Marg, Delhi 110002, India, e-mail: dksingh@maths.du.ac.in, dhiraj426@rediffmail.com

with $G : I \to \mathbb{R}$ a mapping, $0 \neq \lambda \in \mathbb{R}$ a fixed parameter, $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$; $n \geq 3$, $m \geq 3$ being fixed integers, is useful in characterizing the nonadditive entropies

$$H_n^\alpha(p_1, \ldots, p_n) = (1 - 2^{1-\alpha})^{-1} \left(1 - \sum_{i=1}^{n} p_i^\alpha\right) \tag{1.2}$$

where $H_n^\alpha : \Gamma_n \to \mathbb{R}$, $n = 1, 2, \ldots$ are mappings, $0 < \alpha \in \mathbb{R}$, $\alpha \neq 1$, $0^\alpha := 0$ and $1^\alpha := 1$. The nonadditive entropies H_n^α, $n = 1, 2, 3, \ldots$; defined above, are due to Havrda and Charvat [3] and arise when $\lambda = 2^{1-\alpha} - 1$ in (1.1) with $0 < \alpha \in \mathbb{R}$, $\alpha \neq 1$, $0^\alpha := 0$ and $1^\alpha := 1$.

Losonczi and Maksa [4] defined a mapping $g : I \to \mathbb{R}$ as

$$g(x) = \lambda G(x) + x \tag{1.3}$$

for all $x \in I$. With the aid of (1.3), (1.1) reduces to the multiplicative type functional equation

$$\sum_{i=1}^{n} \sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) \tag{1.4}$$

which is included in (FE1) when $\sum_{i=1}^{n} f(p_i) = 0$ for all $(p_1, \ldots, p_n) \in \Gamma_n$, $n \geq 3$ a fixed integer. Now, we point out the importance of the functional equation (1.4) in cryptanalysis.

For any probability distribution $(p_1, \ldots, p_n) \in \Gamma_n$, Harremoës and Topsøe [2] defined the index of coincidence $IC(p_1, \ldots, p_n)$ as

$$IC(p_1, \ldots, p_n) = \sum_{i=1}^{n} p_i^2 \,. \tag{1.5}$$

Obviously, $IC(p_1, \ldots, p_n)$ is a symmetric function of $p_1, \ldots, p_n$. If we define $M_2 : I \to \mathbb{R}$ as $M_2(p) = p^2$ for all $p \in I$, then it is clear that $IC(p_1, \ldots, p_n) = \sum_{i=1}^{n} M_2(p_i)$, and it can be easily seen that M_2 satisfies equation (1.4) for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$, $n \geq 1$, $m \geq 1$ being integers. The quantity $\sum_{i=1}^{n} p_i^2$ is the probability of getting "two of a kind" in two independent trials governed by the distribution $(p_1, \ldots, p_n) \in \Gamma_n$ and is useful in cryptanalysis (see Stinson [6], pp-33). It can be easily seen that $IC(p_1, \ldots, p_n) \leq 1$ with equality if and only if $p_i = 1$ for exactly one i, $1 \leq i \leq n$. The concentration measure $CM(p_1, \ldots, p_n)$ of $(p_1, \ldots, p_n) \in \Gamma_n$ is defined as (see Harremoës and Topsøe [2])

$$CM(p_1, \ldots, p_n) = 1 - IC(p_1, \ldots, p_n) \,.$$

Clearly, $CM(p_1, \ldots, p_n)$ is also a symmetric function of $p_1, \ldots, p_n$. Moreover,

$$CM(p_1, \ldots, p_n) = 1 - \sum_{i=1}^{n} p_i^2 \,. \tag{1.6}$$

It can be easily verified that

$$H_n^2(p_1, \ldots, p_n) = 2CM(p_1, \ldots, p_n)\,.$$

This shows that the concentration measure $CM(p_1, \ldots, p_n)$ is very closely related to the nonadditive entropy $H_n^2(p_1, \ldots, p_n)$ given by (1.2) when $\alpha = 2$.

As a generalization of (1.5), Harremöes and Topsøe [2] also defined the index of coincidence of order α, $\alpha \in \mathbb{R}$ and $\alpha > 1$, of the probability distribution $(p_1, \ldots, p_n) \in \Gamma_n$ as

$$IC_\alpha(p_1, \ldots, p_n) = \sum_{i=1}^{n} p_i^\alpha \tag{1.7}$$

with $0^\alpha := 0$. Here, too, obviously $IC_\alpha(p_1, \ldots, p_n)$ is a symmetric function of probabilities. Let us define the functions $M_\alpha : I \to \mathbb{R}$, $\alpha > 0$ as $M_\alpha(p) = p^\alpha$ for all $p \in I$. Then $IC_\alpha(p_1, \ldots, p_n) = \sum\limits_{i=1}^{n} M_\alpha(p_i)$, $\alpha > 1$, and it is easily seen that this function M_α also satisfies equation (1.4) for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$, $n \geq 1$, $m \geq 1$ being integers. Since $\sum\limits_{i=1}^{n} p_i^\alpha \leq 1$ as $\alpha > 1$, one may define the concentration measure of order α, $\alpha > 1$, of the probability distribution $(p_1, \ldots, p_n) \in \Gamma_n$ as

$$CM_\alpha(p_1, \ldots, p_n) = 1 - IC_\alpha(p_1, \ldots, p_n)\,.$$

Clearly, $CM_\alpha(p_1, \ldots, p_n)$ is also a symmetric function of $p_1, \ldots, p_n$. Moreover, for $\alpha > 1$,

$$CM_\alpha(p_1, \ldots, p_n) = (1 - 2^{1-\alpha}) H_n^\alpha(p_1, \ldots, p_n)\,.$$

We would like to mention that in (1.7), we may allow the values of α which satisfy $0 < \alpha < 1$. Then we can consider the functions M_α with $0 < \alpha < 1$ also and the functions M_α, $\alpha > 0$, satisfy the functional equation (1.4) for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$, $n \geq 1$, $m \geq 1$ being integers. If the probability distribution $(p_1, \ldots, p_n)$ has at least two positive elements, then $\sum\limits_{i=1}^{n} p_i^\alpha > 1$ when $0 < \alpha < 1$ and it is not possible to define $CM_\alpha(p_1, \ldots, p_n)$ in this case.

(II) Let $n \geq 3$, $m \geq 3$ be fixed integers. Suppose $g : I \to \mathbb{R}$ is a mapping such that the difference

$$\sum_{i=1}^{n} \sum_{j=1}^{m} g(p_i q_j) - \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) \tag{1.8}$$

is nonzero for at least one pair (P, Q) of probability distribution $(p_1, \ldots, p_n) = P \in \Gamma_n$ and $(q_1, \ldots, q_m) = Q \in \Gamma_m$. In such a situation, one may ask the following question: Does there exist a mapping $f : I \to \mathbb{R}$ such that the difference (1.8) equals $\sum\limits_{i=1}^{n} f(p_i) \sum\limits_{j=1}^{m} g(q_j)$ or $\sum\limits_{j=1}^{m} f(q_j) \sum\limits_{i=1}^{n} g(p_i)$ for all $(p_1, \ldots, p_n) = P \in$

Γ_n, $(q_1, \ldots, q_m) = Q \in \Gamma_m$? In the former case, we get the functional equation (FE1) whereas in the latter case, we have the functional equation

$$\text{(FE2)} \qquad \sum_{i=1}^{n} \sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + \sum_{j=1}^{m} f(q_j) \sum_{i=1}^{n} g(p_i) \,.$$

Such situations do exist. Below we give two examples:

Example 1.1. Consider $g : I \to \mathbb{R}$, $f : I \to \mathbb{R}$ defined as

$$g(x) = \frac{2}{3}\, x^2 \quad \text{and} \quad f(x) = \frac{1}{3}\, x^2 \qquad \text{for all} \ \ x \in I \,.$$

Example 1.2. Define $g : I \to \mathbb{R}$ and $f : I \to \mathbb{R}$ as

$$g(x) = f(x) = \frac{1}{2}\, x \qquad \text{for all} \ \ x \in I \,.$$

The details are omitted.

We shall deal only with (FE1). The equation (FE2) can be dealt similarly.

2. Some preliminary results

In this section we mention some definitions and results needed to develop further results in this paper.

A mapping $a : I \to \mathbb{R}$ is said to be additive on I if the equation $a(x + y) = a(x) + a(y)$ holds for all $(x, y) \in \Delta$. A mapping $A : \mathbb{R} \to \mathbb{R}$ is said to be additive on $\mathbb{R}$ if the equation $A(x + y) = A(x) + A(y)$ holds for all $x \in \mathbb{R}$, $y \in \mathbb{R}$. It is known [1] that if $a : I \to \mathbb{R}$ is additive on I, then it has a unique additive extension $A : \mathbb{R} \to \mathbb{R}$ in the sense that A is additive on $\mathbb{R}$ and $A(x) = a(x)$ for all $x \in I$.

Result 2.1 ([4])**.** Let $f : I \to \mathbb{R}$ be a mapping which satisfies the equation $\sum\limits_{i=1}^{n} f(p_i) = c$ for all $(p_1, \ldots, p_n) \in \Gamma_n$, $n \geq 3$ a fixed integer and c a given real constant. Then, there exists an additive mapping $b : \mathbb{R} \to \mathbb{R}$ such that $f(p) = b(p) - \dfrac{1}{n} b(1) + \dfrac{c}{n}$ for all $p \in I$.

Definition 2.2. A mapping $M : I \to \mathbb{R}$ is said to be multiplicative on I if $M(0) = 0$, $M(1) = 1$ and $M(pq) = M(p)M(q)$ for all $p \in]0, 1[$, $q \in]0, 1[$, where $]0, 1[= \{x \in \mathbb{R} : 0 < x < 1\}$.

Result 2.3 ([4])**.** Let $n \geq 3$, $m \geq 3$ be fixed integers. Suppose a mapping $g : I \to \mathbb{R}$ satisfies equation (1.4) for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$. Then any general solution g of (1.4), for all $p \in I$, is of the form

$$\text{(2.1)} \qquad g(p) = a(p) + g(0)$$

subject to the condition

$$\text{(2.2)} \qquad a(1) + nmg(0) = [a(1) + ng(0)][a(1) + mg(0)]$$

where $a : \mathbb{R} \to \mathbb{R}$ is an additive mapping or

$$g(p) = M(p) - A(p) \tag{2.3}$$

where $A : \mathbb{R} \to \mathbb{R}$ is an additive mapping such that $A(1) = 0$ and $M : I \to \mathbb{R}$ is a mapping which is multiplicative in the sense of Definition 2.2.

3. On the functional equation (FE1)

The main result of this paper is the following:

Theorem 3.1. *Let $n \geq 3$, $m \geq 3$ be fixed integers and $g : I \to \mathbb{R}$, $f : I \to \mathbb{R}$ be mappings which satisfy the functional equation* (FE1) *for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$. Then, any general solution (g, f) of* (FE1) *is of the form (for all $p \in I$)*

$$(S_1) \quad \begin{cases} \text{(i)} & g(p) \textit{ as in } (2.1) \textit{ subject to the condition } (2.2) \\ \text{(ii)} & f(p) = b(p) - \dfrac{1}{n} b(1) \end{cases}$$

or

$$(S_2) \quad \begin{cases} \text{(i)} & g(p) = M(p) - A(p), \quad A(1) = 0 \\ \text{(ii)} & f(p) = b(p) - \dfrac{1}{n} b(1) \end{cases}$$

or

$$(S_3) \quad \begin{cases} \text{(i)} & g(p) \textit{ as in } (2.1) \textit{ subject to the condition with} \\ \text{(ia)} & a(1) + nmg(0) = [a(1) + mg(0)]^2, \qquad g(0) \neq 0 \\ \text{(ii)} & f(p) = b(p) - \dfrac{1}{n} b(1) + \dfrac{1}{n}(m-n)g(0), \quad g(0) \neq 0 \end{cases}$$

or

$$(S_4) \quad \begin{cases} \text{(i)} & g(p) = a(p), \quad a(1) = 0 \\ \text{(ii)} & f \textit{ arbitrary} \end{cases}$$

or

$$(S_5) \quad \begin{cases} \text{(i)} & g(p) = a(p) + g(0), \qquad a(1) = -\,nmg(0),\ g(0) \neq 0 \\ \text{(ii)} & f(p) = b(p) - \dfrac{1}{n} b(1) + (m-1)g(0), \qquad g(0) \neq 0 \end{cases}$$

or

$$(S_6) \quad \begin{cases} \text{(i)} & g(p) = a(p) + g(0) \quad \textit{with} \\ \text{(ia)} & a(1) + nmg(0) = \left(\dfrac{d+1}{d}\right)[a(1) + mg(0)]^2, \quad d \notin \{0, -1\} \\ \text{(ii)} & f(p) = \dfrac{1}{d} a(p) + B(p) + f(0), \qquad d \notin \{0, -1\} \end{cases}$$

or

$$(S_7)\quad \begin{cases} \text{(i)} \quad g(p) = \dfrac{d}{d+1}[M(p) - A_1(p)], \quad A_1(1) = 0,\ d \notin \{0, -1\} \\ \\ \text{(ii)} \quad f(p) = \dfrac{1}{d+1}[M(p) - A_1(p)] + B(p) + f(0), \quad d \notin \{0, -1\} \end{cases}$$

where $a : \mathbb{R} \to \mathbb{R}$, $b : \mathbb{R} \to \mathbb{R}$, $A : \mathbb{R} \to \mathbb{R}$, $B : \mathbb{R} \to \mathbb{R}$, $A_1 : \mathbb{R} \to \mathbb{R}$ *are additive mappings such that*

$$(3.1)\quad B(1) = \left(\frac{d+1}{d}\right)(m-n)g(0) - nf(0) + \frac{n}{d}g(0), \quad d \notin \{0, -1\}$$

and $M : I \to \mathbb{R}$ *is a mapping which is multiplicative in the sense of Definition 2.2.*

To prove Theorem 3.1, we need to prove the following:

Lemma 3.2. *Let* $n \geq 3$, $m \geq 3$ *be fixed integers and* $g : I \to \mathbb{R}$ *be a mapping which satisfies the functional equation*

$$\text{(FE3)} \qquad \sum_{i=1}^{n}\sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + (m-n)g(0) \sum_{j=1}^{m} g(q_j)$$

for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$. *If* $g(0) \neq 0$, *then any general solution* g *of* (FE3) *is only of the form* (i) *in* (S_3) *with* S_3(ia) *where* $a : \mathbb{R} \to \mathbb{R}$ *is an additive mapping.*

Proof. Since $n \geq 3$, $m \geq 3$ are fixed integers and $g(0) \neq 0$, it follows that $m(n-1)g(0) \neq 0$. Also, if we put $p_1 = 1, p_2 = \ldots = p_n = 0$ in (FE3), we obtain the equation

$$(3.2) \qquad [g(1) + (m-1)g(0) - 1] \sum_{j=1}^{m} g(q_j) = m(n-1)g(0)$$

for all $(q_1, \ldots, q_m) \in \Gamma_m$. So, $[g(1) + (m-1)g(0) - 1] \neq 0$. Now (3.2) can be written in the form

$$\sum_{j=1}^{m} g(q_j) = m(n-1)g(0)[g(1) + (m-1)g(0) - 1]^{-1}$$

valid for all $(q_1, \ldots, q_m) \in \Gamma_m$. By Result 2.1, there exists an additive mapping $a : \mathbb{R} \to \mathbb{R}$ such that

$$(3.3)\quad g(p) = a(p) - \frac{1}{m}a(1) + (n-1)g(0)[g(1) + (m-1)g(0) - 1]^{-1}$$

for all $p \in I$. Consequently, (3.3) reduces to (S_3)(i). In order that (S_3)(i) be a solution of (FE3), the condition S_3(ia) should be satisfied. $\square$

Proof of Theorem 3.1. We divide the discussion into two cases:

Case 1. $\sum_{i=1}^{n} f(p_i)$ vanishes identically on Γ_n.

This means that $\sum_{i=1}^{n} f(p_i) = 0$ for all $(p_1, \ldots, p_n) \in \Gamma_n$, $n \geq 3$ a fixed integer. By Result 2.1, there exists a mapping $b : \mathbb{R} \to \mathbb{R}$ such that $f(p) = b(p) - \frac{1}{n} b(1)$ for all $p \in I$. Substituting $\sum_{i=1}^{n} f(p_i) = 0$ in (FE1), equation (1.4) follows. Making use of Result 2.3, we obtain solutions (S_1) and (S_2).

Case 2. $\sum_{i=1}^{n} f(p_i)$ does not vanish identically on Γ_n.

Let us write (FE1) in the form

$$\sum_{j=1}^{m} \left\{ \sum_{i=1}^{n} g(p_i q_j) - g(q_j) \sum_{i=1}^{n} g(p_i) - g(q_j) \sum_{i=1}^{n} f(p_i) \right\} = 0\,.$$

By Result 2.1, there exists a mapping $\overline{A} : \Gamma_n \times \mathbb{R} \to \mathbb{R}$, additive in the second variable, such that

$$\begin{aligned} \sum_{i=1}^{n} g(p_i q) - g(q) \sum_{i=1}^{n} g(p_i) - g(q) \sum_{i=1}^{n} f(p_i) \\ = \overline{A}(p_1, \ldots, p_n; q) - \frac{1}{m} \overline{A}(p_1, \ldots, p_n; 1) \end{aligned} \tag{3.4}$$

which holds for all $(p_1, \ldots, p_n) \in \Gamma_n$ and $q \in I$. The substitution $q = 0$ in (3.4) and the use of $\overline{A}(p_1, \ldots, p_n; 0) = 0$ gives

$$\overline{A}(p_1, \ldots, p_n; 1) = m g(0) \left[\sum_{i=1}^{n} g(p_i) + \sum_{i=1}^{n} f(p_i) - n \right]. \tag{3.5}$$

From (3.4) and (3.5), the equation

$$\begin{aligned} \sum_{i=1}^{n} g(p_i q) - g(q) \sum_{i=1}^{n} g(p_i) - g(q) \sum_{i=1}^{n} f(p_i) \\ = \overline{A}(p_1, \ldots, p_n; q) + g(0) \left[n - \sum_{i=1}^{n} g(p_i) - \sum_{i=1}^{n} f(p_i) \right] \end{aligned} \tag{3.6}$$

follows. Let $(r_1, \ldots, r_n) \in \Gamma_n$ be any probability distribution. Putting $q = r_t$, $t = 1, \ldots, n$ in (3.6), adding the resulting n equations, using the additivity of $\overline{A}$ in the second variable and equation (3.5), we obtain the equation

(3.7)

$$\begin{aligned} \sum_{i=1}^{n} \sum_{t=1}^{n} g(p_i r_t) - \sum_{t=1}^{n} g(r_t) \sum_{i=1}^{n} g(p_i) + n(m-n) g(0) \\ = \sum_{t=1}^{n} g(r_t) \sum_{i=1}^{n} f(p_i) + (m-n) g(0) \sum_{i=1}^{n} g(p_i) + (m-n) g(0) \sum_{i=1}^{n} f(p_i). \end{aligned}$$

The left-hand side of (3.7) is symmetric in r_t and p_i, $t = 1, \ldots, n$; $i = 1, \ldots, n$. So, should be the right-hand side of (3.7). This fact gives rise to the symmetric equation

$$(3.8)\qquad \left[\sum_{t=1}^{n} g(r_t) + (m-n)g(0)\right]\left[\sum_{i=1}^{n} f(p_i) - (m-n)g(0)\right] = \left[\sum_{i=1}^{n} g(p_i) + (m-n)g(0)\right]\left[\sum_{t=1}^{n} f(r_t) - (m-n)g(0)\right].$$

Case 2.1. $\sum_{i=1}^{n} f(p_i) - (m-n)g(0)$ vanishes identically on Γ_n.

This means that the equation $\sum_{i=1}^{n} f(p_i) = (m-n)g(0)$ holds for all $(p_1, \ldots, p_n) \in \Gamma_n$, $n \geq 3$, $m \geq 3$ being fixed integers. But $\sum_{i=1}^{n} f(p_i)$ does not vanish identically on Γ_n. Hence, there exists a probability distribution $(\overline{p}_1, \ldots, \overline{p}_n) \in \Gamma_n$ such that $\sum_{i=1}^{n} f(\overline{p}_i) \neq 0$. But $\sum_{i=1}^{n} f(\overline{p}_i) = (m-n)g(0)$. Hence $(m-n)g(0) \neq 0$ from which it follows that $g(0) \neq 0$. Thus, indeed, we have

$$(3.9)\qquad \sum_{i=1}^{n} f(p_i) = (m-n)g(0), \quad g(0) \neq 0$$

for all $(p_1, \ldots, p_n) \in \Gamma_n$. By applying Result 2.1 to this equation, we obtain S_3(ii) in which $b : \mathbb{R} \to \mathbb{R}$ is additive. Also, from (FE1) and (3.9), equation (FE3) follows with $g(0) \neq 0$. So, by Lemma 3.2, (S_3)(i) also follows. Thus, we have obtained the solution (S_3) of (FE1).

Case 2.2. $\sum_{i=1}^{n} f(p_i) - (m-n)g(0)$ does not vanish identically on Γ_n.

In this case, there exists a probability distribution $(p_1^*, \ldots, p_n^*) \in \Gamma_n$ such that

$$(3.10)\qquad \left[\sum_{i=1}^{n} f(p_i^*) - (m-n)g(0)\right] \neq 0\,.$$

Setting $p_i = p_i^*$, $i = 1, \ldots, n$ in (3.8) and making use of (3.10), we obtain the equation

$$(3.11)\qquad \sum_{t=1}^{n} g(r_t) = d\left[\sum_{t=1}^{n} f(r_t) - (m-n)g(0)\right] - (m-n)g(0)$$

where

$$(3.12)\qquad d = \left[\sum_{i=1}^{n} f(p_i^*) - (m-n)g(0)\right]^{-1}\left[\sum_{i=1}^{n} g(p_i^*) + (m-n)g(0)\right].$$

Case 2.2.1. $d = 0$.

In this case, (3.11) reduces to the equation

$$\sum_{t=1}^{n} g(r_t) = -(m-n)g(0) \tag{3.13}$$

valid for all $(r_1, \ldots, r_n) \in \Gamma_n$, $n \geq 3$, $m \geq 3$ being fixed integers. Choosing $r_1 = 1$, $r_2 = \ldots = r_n = 0$ in (3.13), it follows that $g(1) + (m-1)g(0) = 0$. Now, choosing $p_1 = 1$, $p_2 = \ldots = p_n = 0$; $q_1 = 1$, $q_2 = \ldots = q_m = 0$ in (FE1) and using $g(1) + (m-1)g(0) = 0$, it follows that $m(n-1)g(0) = 0$. Hence $g(0) = 0$ and $g(1) = 0$. Consequently, (3.13) gives the equation $\sum_{t=1}^{n} g(r_t) = 0$ valid for all $(r_1, \ldots, r_n) \in \Gamma_n$. By Result 2.1, S_4(i) follows, in which $a : \mathbb{R} \to \mathbb{R}$ is an additive mapping with $a(1) = 0$ as $g(0) = 0 = g(1)$. Making use of (S_4)(i) in (FE1), it follows that, indeed, f is an arbitrary real-valued mapping, that is, (S_4)(ii) also holds. Thus, we have obtained the solution (S_4) of (FE1).

Case 2.2.2. $d \neq 0$.

In this case, let us write (3.11) in the form

$$\sum_{t=1}^{n} \left[f(r_t) - \frac{1}{d} g(r_t) \right] = \left(1 + \frac{1}{d}\right)(m-n)g(0)$$

valid for all $(r_1, \ldots, r_n) \in \Gamma_n$. By Result 2.1, there exists an additive mapping $B : \mathbb{R} \to \mathbb{R}$ such that

$$f(p) - \frac{1}{d} g(p) = B(p) - \frac{1}{n} B(1) + \frac{1}{n}\left(1 + \frac{1}{d}\right)(m-n)g(0) \tag{3.14}$$

for all $p \in I$. Also, from (FE1) and (3.14), the functional equation

$$\sum_{i=1}^{n}\sum_{j=1}^{m} g(p_i q_j) = \left(1 + \frac{1}{d}\right)\sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + \left(1 + \frac{1}{d}\right) \times (m-n)g(0) \sum_{j=1}^{m} g(q_j) \tag{FE4}$$

follows.

Case 2.2.2.1. $0 \neq d = -1$.

In this case, (FE4) reduces to the functional equation $\sum_{i=1}^{n}\sum_{j=1}^{m} g(p_i q_j) = 0$ which, for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$, $n \geq 3$, $m \geq 3$ fixed integers, has a solution g of the form $g(p) = a(p) + g(0)$ with $a(1) = -nmg(0)$, $a : \mathbb{R} \to \mathbb{R}$ being an additive mapping. But we must have $g(0) \neq 0$ because if $g(0) = 0$, then $a(1) = 0$ and then, as in Case 2.2.1, the solution (S_4) will follow again. So, (S_5)(i) holds. Making use of this form of g in (3.14) (with $d = -1$), we obtain $f(p) = -a(p) + B(p) - g(0) - \frac{1}{n} B(1)$ for all $p \in I$. Consequently, (S_5)(ii) follows by defining $b : \mathbb{R} \to \mathbb{R}$ as $b(x) = -a(x) + B(x)$ for all $x \in \mathbb{R}$ with $B(1) = -n[f(0) + g(0)]$. Thus, we have obtained the solution (S_5).

Case 2.2.2.2. $0 \neq d \neq -1$.

In this case, $\left(1 + \frac{1}{d}\right) \neq 0$. Put $p = 0$ in (3.14) and use $B(0) = 0$. We obtain (3.1). Define a mapping $h : I \to \mathbb{R}$ as

$$h(p) = \left(1 + \frac{1}{d}\right) g(p) \tag{3.15}$$

for all $p \in I$. Then, (FE4) reduces to the functional equation

$$\sum_{i=1}^{n}\sum_{j=1}^{m} h(p_i q_j) = \sum_{i=1}^{n} h(p_i) \sum_{j=1}^{m} h(q_j) + (m-n)h(0) \sum_{j=1}^{m} h(q_j) \tag{FE5}$$

valid for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$, $n \geq 3$, $m \geq 3$ being fixed integers. Note that (FE5) resembles (FE3) but $h \neq g$.

If $g(0) \neq 0$, then $h(0) \neq 0$. In this case, making use of Lemma 3.2, we have

$$h(p) = b_1(p) + h(0), \quad h(0) \neq 0 \tag{3.16}$$

where $b_1 : \mathbb{R} \to \mathbb{R}$ is an additive mapping with

$$b_1(1) + nm\, h(0) = [b_1(1) + m\, h(0)]^2 . \tag{3.17}$$

From (3.15), (3.16) and (3.17); (S_6)((i), (ia)) follows by defining an additive mapping $a : \mathbb{R} \to \mathbb{R}$ as $a(x) = \frac{d}{d+1} b_1(x)$ for all $x \in \mathbb{R}$ and $d \notin \{0, -1\}$. From (3.14) (with $0 \neq d \neq -1$) and (S_6)(i); (S_6)(ii) follows. Thus, we have obtained (S_6).

If $g(0) = 0$, then $h(0) = 0$. In this case, functional equation (FE5) reduces to the functional equation

$$\sum_{i=1}^{n}\sum_{j=1}^{m} h(p_i q_j) = \sum_{i=1}^{n} h(p_i) \sum_{j=1}^{m} h(q_j), \quad (h(0) = 0).$$

Making use of Result 2.3, it follows that h is of the form

$$h(p) = b_1(p) \quad \text{with} \quad [b_1(1)]^2 = b_1(1)$$

where $b_1 : \mathbb{R} \to \mathbb{R}$ is an additive mapping or

$$h(p) = M(p) - A_1(p)$$

where $M : I \to \mathbb{R}$ and $A_1 : \mathbb{R} \to \mathbb{R}$ are as described in Result 2.3. In the former case, the solution of (FE1) which we get is included in (S_6) when $g(0) = 0$. In the latter case, we get the new solution (S_7). □

4. Discussion

In this section we discuss the importance of various solutions of (FE1), and also mention some related functional equations.

1. In the both solutions (S_1) and (S_2), $\sum_{i=1}^{n} f(p_i) = 0$ for all $(p_1, \ldots, p_n) \in \Gamma_n$. Using this fact in (FE1), the functional equation (1.4) follows, whose importance in information theory has already been pointed out in Section 1.

2. From (S_3)(ii), it is easy to see that $\sum_{i=1}^{n} f(p_i) = (m-n)g(0)$, $g(0) \neq 0$. Consequently, the equation (FE1) reduces to (FE3) with $g(0) \neq 0$. Whatsoever be the choice of the additive mapping $a : \mathbb{R} \to \mathbb{R}$, the both summands $\sum_{i=1}^{n} g(p_i)$ and $\sum_{j=1}^{m} g(q_j)$ are independent of the probabilities. So, the solution (S_3) does not seem to be of any importance from information-theoretic point of view but it is of importance from the point of view of functional equations because it gives rise to the functional equation (FE3) though only when $g(0) \neq 0$.

Nath and Singh [5] came across the functional equation

$$\text{(FE6)} \qquad \sum_{i=1}^{n}\sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + (m-n)g(0) \sum_{j=1}^{m} g(q_j) + m(n-1)g(0)$$

in which $g : I \to \mathbb{R}$ is a mapping; $n \geq 3$, $m \geq 3$ are fixed integers and $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$. The functional equation (FE3) is, indeed, a 'shortened form' of (FE6) obtained from it by omitting the last term $m(n-1)g(0)$ appearing on its right hand side.

3. In S_4(ii), f is any arbitrary real-valued mapping. So, f can be chosen the way we like. One important choice of f is $f(p) = p^\alpha$ for all $p \in I$, $\alpha > 0$, $\alpha \neq 1$ being a fixed real power such that $0^\alpha := 0$, $1^\alpha := 1$. In this case, (FE1) reduces to the functional equation

$$\text{(FE7)} \qquad \sum_{i=1}^{n}\sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + \sum_{i=1}^{n} p_i^\alpha \sum_{j=1}^{m} g(q_j)$$

in which $g : I \to \mathbb{R}$ is a mapping, $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$; $n \geq 3$, $m \geq 3$ being fixed integers. In our subsequent work we will present all solutions of (FE7) for $n \geq 3$, $m \geq 3$ being fixed integers and $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$.

4. From (FE1) and S_5(ii), the functional equation

$$\text{(FE8)} \qquad \sum_{i=1}^{n}\sum_{j=1}^{m} g(p_i q_j) = \sum_{i=1}^{n} g(p_i) \sum_{j=1}^{m} g(q_j) + n(m-1)g(0) \sum_{j=1}^{m} g(q_j)$$

follows. Its general solutions for all $(p_1, \ldots, p_n) \in \Gamma_n$, $(q_1, \ldots, q_m) \in \Gamma_m$ and $n \geq 3$, $m \geq 3$ being fixed integers will be presented elsewhere.

5. In solution (S_6), the summands $\sum_{i=1}^{n} f(p_i)$ and $\sum_{i=1}^{n} g(p_i)$ are independent of the probabilities $p_1, \ldots, p_n$. So, the solution (S_6) does not seem to be of any relevance in information theory.

6. In solution (S_7), the summands are

$$\sum_{i=1}^{n} g(p_i) = \frac{d}{d+1} \left[\sum_{i=1}^{n} M(p_i) - 1 \right] + \frac{d}{d+1}$$

and

$$\sum_{i=1}^{n} f(p_i) = \frac{1}{d+1} \left[\sum_{i=1}^{n} M(p_i) - 1 \right] + \frac{1}{d+1} .$$

From the point of view of information theory and cryptanalysis, it is desirable to choose the mapping $M : I \to \mathbb{R}$ defined as $M(p) = p^\alpha$, $0 \le p \le 1$, $\alpha \in \mathbb{R}$, $\alpha > 0$, $\alpha \ne 1$, $0^\alpha := 0$ and $1^\alpha := 1$. Then, we get

$$\sum_{i=1}^{n} g(p_i) = \frac{d}{d+1} [2^{1-\alpha} - 1] H_n^\alpha(p_1, \ldots, p_n) + \frac{d}{d+1}$$

and

$$\sum_{i=1}^{n} f(p_i) = \frac{1}{d+1} [2^{1-\alpha} - 1] H_n^\alpha(p_1, \ldots, p_n) + \frac{1}{d+1} .$$

In particular, if $\alpha > 1$, then

$$\sum_{i=1}^{n} g(p_i) = -\frac{d}{d+1} CM_\alpha(p_1, \ldots, p_n) + \frac{d}{d+1}$$

and

$$\sum_{i=1}^{n} f(p_i) = -\frac{1}{d+1} CM_\alpha(p_1, \ldots, p_n) + \frac{1}{d+1}$$

where $CM_\alpha(p_1, \ldots, p_n)$ denotes the concentration measure of order α, $\alpha > 1$.

Thus, we see that the mappings g and f, appearing in (FE1), are related to non-additive entropy of degree α and concentration measure of order α.

References

[1] Daróczy, Z., Losonczi, L., Über die Erweiterung der auf einer Punktmenge additiven Funktionen. Publ. Math. (Debrecen) 14 (1967), 239–245.

[2] Harremoës, P., Topsøe, F., Inequalities between entropy and index of coincidence derived from information diagrams. IEEE Transaction on Information Theory 47 (7) (2001), 2944–2960.

[3] Havrda, J., Charvát, F., Quantification method of classification process. Concept of structural α-entropy. Kybernetika (Prague) 3 (1967), 30–35.

[4] Losonczi, L., Maksa, Gy., On some functional equations of the information theory. Acta Math. Acad. Sci. Hung. 39 (1982), 73–82.

[5] Nath, P., Singh, D.K., On a multiplicative type sum form functional equation and its role in information theory. Applications of Mathematics 51 (5) (2006), 495–516.

[6] Stinson, D.R., Cryptography: theory and practice. Boca Raton, FL: CRC 1995.

Received by the editors November 14, 2011