ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS

NOVA SERIES TOM. XXIX.

SECTIO MATHEMATICAE

REDIGIT

MÁTYÁS FERENC

EGER, 2002

REMARKS ON UNIFORM DENSITY OF SETS OF INTEGERS

Zuzana Gáliková & Béla László (Nitra, Slovakia)
Tibor Šalát (Bratislava, Slovakia)

Dedicated to the memory of Professor Péter Kiss

Abstract. The concept of the uniform density is introduced in papers [1], [2]. Some properties of this concept are studied in this paper. It is proved here that the uniform density has the Darboux property.

AMS Classification Number: 11B05

Keywords: asymptotic density, uniform density, almost convergence, Darboux property

Introduction

Let $A \subseteq N = \{1,2,3,\dots\}$ and $m,n \in N$, $m < n$. Denote by $A(m,n)$ the cardinality of the set $A \cap [m,n]$. The numbers

$$\underline{d}(A) = \varliminf_{n\to\infty} \frac{A(1,n)}{n}, \qquad \bar{d}(A) = \varlimsup_{n\to\infty} \frac{A(1,n)}{n}$$

are called the lower and the upper asymptotic density of the set A. If there exists

$$d(A) = \lim_{n\to\infty} \frac{A(1,n)}{n}$$

then it is called the asymptotic density of A.

According to [1], [2] we set

$$\alpha_s = \min_{t\geq 0} A(t+1,t+s), \qquad \alpha^s = \max_{t\geq 0} A(t+1,t+s).$$

Then there exist

$$\underline{u}(A) = \lim_{s\to\infty} \frac{\alpha_s}{s}, \qquad \bar{u}(A) = \lim_{s\to\infty} \frac{\alpha^s}{s}$$

and they are called the lower and the upper uniform density of A, respectively.

It is obvious that for every $A \subseteq N$

$$\underline{u}(A) \le \underline{d}(A) \le \bar{d}(A) \le \bar{u}(A).$$

Hence if $u(A)$ exists then $d(A)$ exists as well and $u(A) = d(A)$. The converse is not true. For example put

$$A = \bigcup_{k=1}^{\infty} \left\{10^k + 1, 10^k + 2, \dots, 10^k + k\right\}.$$

Then $d(A) = 0$, but $\underline{u}(A) = 0$, $\bar{u}(A) = 1$.

Note that the numbers α_s and α^s can be replaced by the numbers β_s and β^s, respectively, where

$$\beta_s = \varliminf_{t \to \infty} A(t+1, t+s), \quad \beta^s = \varlimsup_{t \to \infty} A(t+1, t+s)$$

(cf. [1], [2]).

In this paper we introduce some elementary remarks, observations on the concept of the uniform density and prove that this density has the Darboux property.

1. Uniform density $u(A)$ and $\lim_{s\to\infty} \frac{A(t+1,t+s)}{s}$ (uniformly with respect to $t \ge 0$)

We introduce the following observation.

Theorem 1.1. *If there exists*

$$\lim_{s \to \infty} \frac{A(t+1, t+s)}{s} = L \tag{1}$$

uniformly with respect to $t \ge 0$, then there exists $u(A)$ and $u(A) = L$.

Proof. Let $\varepsilon > 0$. By the assumption there exists an $s_0 = s_0(\varepsilon) \in N$ such that for each $s > s_0$ and each $t \ge 0$ we have

$$(L - \varepsilon)s < A(t+1, t+s) < (L + \varepsilon)s.$$

By the definition of the numbers β_s, β^s we get from this for $s > s_0$

$$L - \varepsilon \le \frac{\beta_s}{s} \le \frac{\beta^s}{s} \le L + \varepsilon.$$

If $s \to \infty$ we get

$$L - \varepsilon \le \underline{u}(A) \le \bar{u}(A) \le L + \varepsilon.$$

Since $\varepsilon > 0$ is an arbitrary positive number, we get $u(A) = L$.

The foregoing theorem can be conversed.

Theorem 1.2. *If there exists $u(A)$ then*

$$\lim_{s\to\infty} \frac{A(t+1, t+s)}{s} = u(A)$$

uniformly with respect to $t \ge 0$.

Proof. Put $u(A) = L$. Since

$$L = \lim_{p\to\infty} \frac{\alpha_p}{p} = \lim_{p\to\infty} \frac{\alpha^p}{p}$$

for every $\varepsilon > 0$, there exists a p_0 such that for each $p > p_0$ we have

$$(L - \varepsilon)p < \alpha_p \le \alpha^p < (L + \varepsilon)p.$$

So we get

$$(L - \varepsilon)p < \min_{t\ge 0} A(t+1, t+p) \le \max_{t\ge 0} A(t+1, t+p) < (L + \varepsilon)p.$$

By the definition of $A(t+1, t+p)$ we get from this

$$\left| \frac{A(t+1, t+p)}{p} - L \right| \le \varepsilon$$

for each $p > p_0$ and each $t \ge 0$. Hence

$$\lim_{p\to\infty} \frac{A(t+1, t+p)}{p} = L \quad (= u(A))$$

uniformly with respect to $t \ge 0$.

2. Uniform density and almost convergence

The concept of almost convergence was introduced in [5] (see also [10], p. 60). A sequence $(x_n)_1^\infty$ of real numbers almost converges to L if

$$\lim_{p\to\infty} \frac{x_{n+1} + x_{n+2} + \cdots + x_{n+p}}{p} = L$$

uniformly with respect to $n \geq 0$. If $(x_n)_1^\infty$ almost converges to L, we write

$$F - \lim x_n = L.$$

One can conjecture that there is a relationship between the uniform density of a set $A \subseteq N$ and the characteristic function χ_A of this set ($\chi_A(n) = 1$ if $n \in A$, $\chi_A(n) = 0$ if $n \in N \setminus A$).

Theorem 2.1. *Let $A \subseteq N$. Then $u(A) = v$ if and only if $F - \lim \chi_A(n) = v$.*

Proof. Let $t \geq 0$, $s \in N$. By the definition of the sequence $(\chi_A(n))_1^\infty$ we see that

$$\frac{A(t+1, t+s)}{s} = \frac{\chi_A(t+1) + \chi_A(t+2) + \cdots + \chi_A(t+s) - t}{s}.$$

The assertion follows from this equality by Theorem 1.1 and 1.2.

3. Another way for defining the uniform density of sets

If $A = \{a_1 < a_2 < \cdots < a_n < \cdots\} \subseteq N$ is an infinite set then it is well–known that

$$\underline{d}(A) = \varliminf_{n \to \infty} \frac{n}{a_n}, \quad \bar{d}(A) = \varlimsup_{n \to \infty} \frac{n}{a_n}$$

and

$$d(A) = \lim_{n \to \infty} \frac{n}{a_n}$$

(if $d(A)$ exists) (cf. [8], p. 247). A similar result can be stated also for the uniform density.

Theorem 3.1. *Let $A = \{a_1 < a_2 < \cdots < a_n < \cdots\} \subseteq N$ be an infinite set. Then $u(A) = L$ if and only if*

$$\lim_{p \to \infty} \frac{p}{a_{k+p} - a_{k+1}} = L \tag{2}$$

uniformly with respect to $k \geq 0$.

Proof. 1. Let $u(A) = L$. Consider that for $p \geq 2$

$$\frac{p}{a_{k+p} - a_{k+1}} = \frac{A(a_{k+1}, a_{k+p})}{a_{k+p} - a_{k+1}}.$$

By Theorem 1.2 (see (1)) the right-hand side converges by $p \to \infty$ (uniformly with respect to $k \geq 0$) to $u(A) = L$. Hence (2) holds.

2. Suppose that (2) holds (uniformly with respect to $k \geq 0$). By Theorem 1.1 it suffices to prove that

$$\lim_{p \to \infty} \frac{A(t+1, t+p)}{p} = L$$

uniformly with respect to $t \geq 0$.

We shall show it. Suppose in the first place that $t \geq a_1$. Then there exist $k, s \in N$ such that

$$a_k < t+1 \leq a_{k+1} < \cdots < a_{k+s} \leq t+p < a_{k+s+1}.$$

Then $A(t+1, t+p)$ equals to s and so

$$\frac{A(t+1,t+p)}{p} = \frac{s}{p}.$$

Further on the basis of choice of the numbers k, s we get

$$a_{k+s} - a_{k+1} \leq p-1 < a_{k+s+1} - a_k.$$

Therefore

$$\frac{s}{a_{k+s+1} - a_k + 1} < \frac{A(t+1,t+p)}{p} < \frac{s}{a_{k+s} - a_{k+1}}.$$

But $-a_k + 1 \leq -a_{k-1}$, so that

$$\begin{aligned}\frac{s}{a_{k+s+1} - a_k + 1} &\geq \frac{s}{a_{k+s+1} - a_{k-1}} = \frac{s+3}{a_{k+s+1} - a_{k-1}} \frac{s}{s+3} \\ &= \frac{s+3}{a_{k+s+1} - a_{k-1}} \left(1 - \frac{3}{s+3}\right).\end{aligned}$$

So we get wholly

$$\frac{s+3}{a_{k+s+1} - a_{k-1}} \left(1 - \frac{3}{s+3}\right) < \frac{A(t+1,t+p)}{p} < \frac{s}{a_{k+s} - a_{k+1}}. \tag{3}$$

Let $\gamma > 0$. Then by assumption (see (2)) there exists a v_0 such that for each $v > v_0$ we have

$$-\gamma < \frac{v}{a_{k+v} - a_{k+1}} - L < \gamma \tag{4}$$

for all $k \geq 0$.

Using (4) we get from (3)

$$\frac{s+3}{a_{k+s+1} - a_{k-1}} - L - \frac{3}{a_{k+s+1} - a_{k-1}} < \frac{A(t+1,t+p)}{p} - L < \frac{s}{a_{k+s} - a_{k+1}} - L. \tag{5}$$

Let $s > v_0$. Then by (4) the right-hand side of (5) is less than γ. On the left–hand side we get

$$\frac{s+3}{a_{k+s+1} - a_{k-1}} - L > -\gamma.$$

Further

$$\frac{-3}{a_{k+s+1}-a_{k-1}} \geq \frac{-3}{s+2},$$

since

$$a_{k+s+1}-a_{k-1} = (a_k - a_{k-1}) + (a_{k+1}-a_k) + \cdots + (a_{k+s+1}-a_{k+s})$$

and each summand on the right-hand side is ≥ 1.

Hence for every $t \geq a_1$ we get from (5) $(s > v_0)$

$$-\gamma - \frac{3}{s+2} < \frac{A(t+1,t+p)}{p} - L < \gamma \tag{6}$$

From this

$$\lim_{p\to\infty} \frac{A(t+1,t+p)}{p} = L$$

uniformly with respect to $t \geq a_1$.

It remains the case if $0 \leq t < a_1$. Since there is only a finite number of such t's, it suffices to show that for each fixed t, $0 \leq t < a_1$, we have

$$\lim_{p\to\infty} \frac{A(t+1,t+p)}{p} = L. \tag{7}$$

If t is fixed, $0 \leq t < a_1$ and p is sufficiently large we can determine a k such that $a_k \leq t+p < a_{k+1}$. Then

$$0 \leq t < a_1 < a_2 < \cdots < a_k \leq t+p < a_{k+1}$$

and

$$A(t+1,t+p) = A(t+1,a_1) + A(a_2,a_k). \tag{8}$$

From this

$$p < a_{k+1}, \quad p > a_k - a_1 \tag{8'}$$

and so from (8), (8′) we obtain

$$\begin{aligned} \frac{A(t+1,a_1)}{p} + \frac{A(a_2,a_{k+1})-1}{a_{k+1}} &\leq \frac{A(t+1,t+p)}{p} \\ &\leq \frac{A(t+1,a_1)}{p} + \frac{k-1}{a_k - a_1}. \end{aligned} \tag{9}$$

Obviously we have $A(t+1, a_1) \le a_1$ and so

$$\frac{A(t+1, a_1)}{p} = o(1) \quad (p \to \infty).$$

We arrange the left-hand side of (9). We get

$$\frac{A(a_2, a_{k+1}) - 1}{a_{k+1}} = -\frac{1}{a_{k+1}} + \frac{k}{a_{k+1} - a_2} \frac{a_{k+1} - a_2}{a_{k+1}} = o(1) + \frac{k}{a_{k+1} - a_2}$$

(if $p \to \infty$ then $k \to \infty$, as well).

Wholly we have

$$\frac{k}{a_{k+1} - a_2} + o(1) \le \frac{A(t+1, t+p)}{p} \le \frac{k-1}{a_k - a_1} + o(1).$$

If $p \to \infty$, then $k \to \infty$ and by assumption (cf (2)) the terms

$$\frac{k-1}{a_k - a_1} - L, \qquad \frac{k}{a_{k+1} - a_2} - L$$

converge to zero. But then (9) yields

$$\lim_{p \to \infty} \frac{A(t+1, t+p)}{p} = L$$

uniformly with respect to $t \ge 0$. So $u(A) = L$.

The following theorem is a simple consequence of Theorem 3.1

Theorem 3.2. *Let $A = \{a_1 < a_2 < \cdots\} \subseteq N$ be a lacunary set, i.e.*

$$\lim_{n \to \infty} (a_{n+1} - a_n) = +\infty. \tag{10}$$

Then $u(A) = 0$.

Proof. Let $\varepsilon > 0$. Choose $M \in N$ such that $M^{-1} < \varepsilon$. By the assumption there exists an n_0 such that for each $n > n_0$ we get $a_{n+1} - a_n > M$.

Let $k > n_0$, $s \in N$, $s > 1$. Then

$$a_{k+s} - a_{k+1} = (a_{k+2} - a_{k+1}) + (a_{k+3} - a_{k+2}) + \cdots + (a_{k+s} - a_{k+s-1}) > (s-1)M$$

and so

$$\frac{s}{a_{k+s} - a_{k+1}} < \frac{s}{(s-1)M} < 2\varepsilon.$$

Hence for each $k > n_0$ and $s \geq 2$ we have

$$\frac{s}{a_{k+s} - a_{k+1}} < 2\varepsilon.$$

If $0 \leq k \leq n_0$, k is fixed, then

$$\lim_{s\to\infty} \frac{s}{a_{k+s} - a_{k+1}} = 0, \tag{11}$$

since, for sufficiently large s

$$\begin{aligned} a_{k+s} - a_{k+1} &= [(a_{k+2} - a_{k+1}) + \cdots + (a_{n_0+1} - a_{n_0})] \\ &\quad + [(a_{n_0+2} - a_{n_0+1}) + \cdots + (a_{k+s} - a_{k+s-1})] > M(k + s - n_0 - 1) \\ &\geq M(s - (n_0 + 1)). \end{aligned}$$

There exists only a finite number of k's with $0 \leq k \leq n_0$, so we see that (11) holds uniformly with respect to k, $0 \leq k \leq n_0$. So we get wholly

$$\lim_{s\to\infty} \frac{s}{a_{k+s} - a_{k+1}} = 0$$

uniformly with respect to $k \geq 0$. So according to Theorem 3.1, $u(A) = 0$.

Remark. The assumption (10) in Theorem 3.2 cannot be replaced by the weaker assumption

$$\overline{\lim_{n\to\infty}} (a_{n+1} - a_n) = +\infty. \tag{10'}$$

This can be shown by the following example:

$$A = \bigcup_{k=1}^{\infty} \{k! + 1, k! + 2, \ldots, k! + k\} = \{a_1 < a_2 < \cdots < a_n < \cdots\}.$$

Here we have $\underline{u}(A) = 0$, $\bar{u}(A) = 1$ and (10′) is satisfied.

Example 3.1 Let $\alpha \in R$, $\alpha > 1$. Put $a_k = [k\alpha]$, $(k = 1, 2, \ldots)$, where $[v]$ denotes the integer part of v. We show that the uniform density of the set A is $\frac{1}{\alpha}$. This follows from Theorem 3.1, since

$$\lim_{p\to\infty} \frac{p}{a_{k+p} - a_{k+1}} = \frac{1}{\alpha}$$

uniformly with respect to $k \geq 0$. This uniform convergence can be shown by a simple calculation which gives the estimates ($p \geq 2$)

$$\frac{p}{(p-1)\alpha+1} \leq \frac{p}{a_{k+p}-a_{k+1}} \leq \frac{p}{(p-1)\alpha-1}.$$

4. Darboux property of the uniform density

For every $A \subseteq N$ having the uniform density the number $u(A)$ belongs to $[0,1]$. The natural question arises whether also conversely for every $t \in [0,1]$ there is a set $A \subseteq N$ such that $u(A)=t$. The answer to this question is positive.

Theorem 4.1.
If $t \in [0,1]$ then there is a set $A \subseteq N$ with $u(A)=t$.

Proof. We can already suppose that $0 < t < 1$. Construct the set

$$A = \left\{ \left[\frac{1}{t}\right], \left[\frac{2}{t}\right], \ldots, \left[\frac{k}{t}\right], \ldots \right\} = \{a_1 < a_2 < \cdots\}.$$

Put $a_k = [\frac{k}{t}]$ $(k=1,2,\ldots)$ and set in Example 3.1 $\alpha = \frac{1}{t} > 1$. So we get

$$\lim_{p\to\infty} \frac{p}{a_{k+p}-a_{k+1}} = \frac{1}{\alpha} = t$$

uniformly with respect to $k \geq 0$. The assertion follows by Theorem 3.1.

Let v be a non-negative set function defined on a class $S \subseteq 2^N$. The function v is said to have the Darboux property provided that if $v(A) > 0$ for $A \in S$ and $0 < t < v(A)$, then there is a set $B \subseteq A$, $B \in S$ such that $v(B)=t$ (cf. [6], [7], [9]).

Theorem 4.2. *The uniform density has the Darboux property.*

Proof. Let $u(A) = \delta > 0$,

$$A = \{a_1 < a_2 < \cdots < a_k < \cdots\}$$

and $0 < t < \delta$. Construct the set

$$B = \{b_1 < b_2 < \cdots < b_k < \cdots\}$$

in such a way that we set

$$b_k = a_{[k\frac{\delta}{t}]} \quad (k=1,2,\ldots).$$

Put $n_k = [k\frac{\delta}{t}]$ $(k = 1, 2, \ldots)$. Then $n_1 < n_2 < \cdots < n_k < \cdots$,

$$B = \{a_{n_1} < a_{n_2} < \cdots < a_{n_k} < \cdots\}, \quad B \subseteq A.$$

We prove that $u(B) = t$.

By Theorem 3.1 it suffices to show that

$$\lim_{p\to\infty} \frac{p}{b_{m+p} - b_{m+1}} = t \tag{12}$$

uniformly with respect to $m \geq 0$.

We have $(p > 1)$

$$\frac{p}{b_{m+p} - b_{m+1}} = \frac{p}{a_{n_{m+p}} - a_{n_{m+1}}}.$$

By a simple arrangement we get

$$\frac{p}{b_{m+p} - b_{m+1}} = \frac{n_{m+p} - n_{m+1} + 1}{a_{n_{m+p}} - a_{n_{m+1}}} \frac{p}{n_{m+p} - n_{m+1} + 1}. \tag{13}$$

A simple estimation gives

$$(p-1)\frac{\delta}{t} - 1 < n_{m+p} - n_{m+1} < (p-1)\frac{\delta}{t} + 1.$$

Using this in (13) we get

$$\lim_{p\to\infty} \frac{p}{n_{m+p} - n_{m+1} + 1} = \frac{t}{\delta} \tag{14}$$

uniformly with respect to $m \geq 0$.

Further by assumption

$$\lim_{p\to\infty} \frac{p}{a_{s+p} - a_{s+1}} = \delta$$

uniformly with respect to $s \geq 0$ (Theorem 3.1).

So we get

$$\lim_{p\to\infty} \frac{n_{m+p} - n_{m+1} + 1}{a_{n_{m+p}} - a_{n_{m+1}}} = \delta \tag{15}$$

uniformly with respect to $m \geq 0$ since the sequence

$$\left(\frac{n_{m+p} - n_{m+1} + 1}{a_{n_{m+p}} - a_{n_{m+1}}}\right)_{p=2}^{\infty}$$

is a subsequence of the sequence

$$\left(\frac{p}{a_{s+p} - a_{s+1}}\right)_{p=1}^{\infty}.$$

By (13), (14), (15) we get (12) uniformly with respect to $m \geq 0$.

References

[1] Brown, T. C. and Freedman, A. R., Arithmetic progressions in lacunary sets, *Rocky Mountains J. Math* **17** (1987), 587–596.

[2] Brown, T. C. and Freedman, A. R., The uniform density of sets of integers and Fermat's Last Theorem, *C. R. Math. Rep. Acad. Sci. Canada* **XII** (1990), 1–6.

[3] Grekos, G., Šalát, T. and Tomanová, J., Gaps and densities, (to appear).

[4] Gerkos, G. and Volkmann, B., On densities and gaps, *J. Number Theory* **26** (1987), 129–148.

[5] Lorentz, G., A contribution to the theory of divergent sequences, *Acta Math.* **80** (1848), 167–190.

[6] Marcus, S., Atomic measures and Darboux property, *Rev. Math. Pures et Appl.,* **VII** (1962), 327–332.

[7] Marcus, S., On the Darboux property for atomic measures and for series with positive terms, *Rev. Roum. Math. Pures et Appl.,* **XI** (1966), 647–652.

[8] Niven, I. and Zuckerman, H. S., An Introduction to the Theory of Numbers, John Wiley, New York, London, Sydney, 1967.

[9] Olejçek, V., Darboux property of finitely additive measure on δ–ring, *Math. Slov.* **27** (1977), 195–201.

[10] Petersen, G. M., Regular Matrix Transformations, Mc Graw-Hill, London, New York, Toronto, Sydney, 1966.

Zuzana Gáliková and
Béla László
Constantine Philosopher University
Department of Algebra and Number Theory
Tr. A. Hlinku 1
949 74 Nitra
Slovakia
E-mail: katc@ukf.sk

Tibor Šalát
Department of Algebra
and Number Theory
Mlynská dolina
842 15 Bratislava
Slovakia

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 15–34*

ON THE CUBE MODEL OF THREE-DIMENSIONAL EUCLIDEAN SPACE

I. Szalay (Szeged, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. In [4] the open interval $\underline{R}=]-1,1[$ with the sub-addition $\oplus$ and sub-multiplication $\odot$ was considered as a compressed model of the field of real numbers $(R,+,\cdot)$. Considering the points of the open cube $\underline{R}^3=\{X=(x_1,x_2,x_3):\ x_1,x_2,x_3\in\underline{R}\}$ we give the concepts of sub-line and sub-plane and construct a bounded model of the three dimensional Euclidean geometry which is isomorphic with the familiar model R^3.

Preliminary

The first exact formulation of classical Euclidean geometry was given by Hilbert. Nowadays, Hilbert's axiom-system is well-known. (For example, see [2], pp. 172, 102, 31, 326, 135–136, 187, 351, 77, 326, 25, 45 and 405.) It is a very comfortable model, the three-dimensional Descartes coordinate-system R^3 is a real vector space with a canonical inner product. It is used in the secondary and higher schools, in general. Another model, given by Fjodoroff (see [2] p. 117), is less-known. Its speciality is that it is able to interpret the points of R^3 in a given basic plane by a point (lying on the basic plane) together with a directed circle. Both mentioned models, are boundless.

Our cube model, being an (open) cube in R^3, is bounded. Its speciality is that it is able to show the "end of line" or the "meeting of parallel lines" and so on. On the other hand, the elements of this model are less spectacular in a traditional sense. "Line" may be a screwed curve which does not lie in any traditional plane. The form "ball" depends on not only its "radius" but the place of its "centre", too.

The importence of the cube model is in the methodology of teacher training. Seeing that the axioms are not trivial helps to understand the role of parallelism in the history of mathematics: Namely, the axiom of parallelism was the only axiom which seemed to be provable by the other axioms.

The cube model is based on the ordered field of compressed real numbers situated on the open interval]-1, 1[denoted by $\underline{R}$. Introducing the sub-addition $\oplus$ and sub-multiplication $\odot$, the ordered field $(\underline{R},\oplus,\odot)$ is isomorphic with the ordered field $(R,+,\cdot)$. The points of open cube $\underline{R}^3=\{X=(x_1,x_2,x_3):\ x_1,x_2,x_3\in\underline{R}\}$ give the points of the cube model.

Introduction

Having the compression function $u \in R \mapsto \operatorname{th} u \in]-1, 1[$ ([1], I. 7.54–7.58) we say that the compressed of u is given by the equation

$$\underbracket{u} = \operatorname{th} u, \quad u \in R. \tag{0.1}$$

Hence, we have that the compresseds of real numbers are just on the open interval $\underbracket{R} =]-1, 1[$. Considering the compression function as an isomorphism between the fields $(R, +, \cdot)$ and $(\underbracket{R}, \oplus, \odot)$ we define the sub-addition and sub-multiplication by the identities

$$\underbracket{u} \oplus \underbracket{v} := \underbracket{u + v}, \quad u, v \in R \tag{0.2}$$

and

$$\underbracket{u} \odot \underbracket{v} := \underbracket{u \cdot v}, \quad u, v \in R, \tag{0.3}$$

respectively. If $x = \underbracket{u}$ and $y = \underbracket{v}$, then (0,1), (0,2) and (0,3) yield the relations

$$x \oplus y = \frac{x + y}{1 + xy}, \quad x, y \in \underbracket{R} \tag{0.4}$$

and

$$x \odot y = \operatorname{th}((\operatorname{ar\,th} x)(\operatorname{ar\,th} y)), \quad x, y \in \underbracket{R}. \tag{0.5}$$

Moreover, we can use the identities

$$\underbracket{u} \ominus \underbracket{v} := \underbracket{u - v}, \quad u, v \in R \tag{0.6}$$

$$\underbracket{u} \mathbin{\bigcirc\kern-0.62em:\kern0.3em} \underbracket{v} := \underbracket{u : v}, \quad u, v \in R, \quad v \neq 0 \tag{0.7}$$

or

$$x \ominus y = \frac{x - y}{1 - xy}, \quad x, y \in \underbracket{R} \tag{0.8}$$

and

$$x \mathbin{\bigcirc\kern-0.62em:\kern0.3em} y = \operatorname{th}\left(\frac{\operatorname{ar\,th} x}{\operatorname{ar\,th} y}\right), \quad x, y \in \underbracket{R}, y \neq 0, \tag{0.9}$$

where the operations $\ominus$ and $\odot$ are called sub-subtraction and sub-division, respectively.

The inverse of compression is explosion defined by the equation

$$\overset{\sqcup}{x} = \operatorname{ar\,th} x, \quad x \in \underset{\sqcup}{R} \tag{0.10}$$

and $\overset{\sqcup}{x}$ is called the exploded of x. Clearly, by (0.1) and (0.10) we have the identities

$$x = \underset{\sqcup}{(\overset{\sqcup}{x})}, \quad x \in \underset{\sqcup}{R} \tag{0.11}$$

and

$$u = \overset{\sqcup}{(\underset{\sqcup}{u})}, \quad u \in R. \tag{0.12}$$

1. Operations on $\underset{\sqcup}{R}^3$

Having the familiar three dimensional Euclidean vector-space R^3 with the traditional operations (addition, multiplication by scalar, inner product) as well as the concepts of norm and metric, we give their isomorphic concepts for $\underset{\sqcup}{R}^3$ which is the set of points $X = (x_1, x_2, x_3)$ such that $x_1, x_2, x_3 \in \underset{\sqcup}{R}$. Clearly, $\underset{\sqcup}{R}^3$ forms an open cube in R^3. Considering the vectors $X = (x_1, x_2, x_3)$ and $Y = (y_1, y_2, y_3)$ from $\underset{\sqcup}{R}^3$ we define sub-addition as

$$X \oplus Y = (x_1 \oplus y_1, x_2 \oplus y_2, x_3 \oplus y_3), \tag{1.1}$$

sub-multiplication by scalar $c \in \underset{\sqcup}{R}$ as

$$c \odot X = (c \odot x_1, c \odot x_2, c \odot x_3) \tag{1.2}$$

and sub-inner product as

$$X \odot Y = (x_1 \odot y_1) \oplus (x_2 \odot y_2) \oplus (x_3 \odot y_3). \tag{1.3}$$

Introducing the exploded of the point $X = (x_1, x_2, x_3)$ as

$$\overset{\sqcup}{X} = (\overset{\sqcup}{x_1}, \overset{\sqcup}{x_2}, \overset{\sqcup}{x_3}), \quad X \in \underset{\sqcup}{R}^3 \tag{1.4}$$

and the compressed of the point $U = (u_1, u_2, u_3)$ as

$$\lfloor U \rfloor = (\lfloor u_1 \rfloor, \lfloor u_2 \rfloor, \lfloor u_3 \rfloor), \quad U \in R^3 \tag{1.5}$$

we have the identities

$$X = \lfloor (\overset{\sqcup}{X}) \rfloor, \quad X \in \lfloor R \rfloor^3 \tag{1.6}$$

and

$$U = \overset{\sqcup}{(\lfloor U \rfloor)}, \quad U \in R^3. \tag{1.7}$$

Using (0.11), (0.2), (1.5) and (1.4), the identity (1.1) yields

$$X \oplus Y = \lfloor \overset{\sqcup}{X} + \overset{\sqcup}{Y} \rfloor, \quad X, Y \in \lfloor R \rfloor^3. \tag{1.8}$$

Moreover, by (0.11), (0.3), (1.4) the identity (1.2) yields

$$c \odot X = \lfloor \overset{\sqcup}{c} \cdot \overset{\sqcup}{X} \rfloor, \quad c \in \lfloor R \rfloor \quad \text{and} \quad X \in \lfloor R \rfloor^3. \tag{1.9}$$

Considering the operations (1.1) and (1.2) we have the following

Theorem 1.10. $\lfloor R \rfloor^3$ *is a real vector space with the sub-addition* (1.1) *and scalar sub-multiplication* (1.2). *In detail, we have the following identities:*

$$X \oplus Y = Y \oplus X, \quad X, Y \in \lfloor R \rfloor^3, \tag{1.11}$$

$$(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z), \quad X, Y, Z \in \lfloor R \rfloor^3, \tag{1.12}$$

$$X \oplus o = X, \quad \text{where} \quad X \in \lfloor R \rfloor^3 \quad \text{arbitrary and} \quad o = (0, 0, 0), \tag{1.13}$$

$$X \oplus (-X) = o, \quad \text{where} \quad -X \text{ is the familiar additive inverse of } \quad x \in \lfloor R \rfloor^3. \tag{1.14}$$

Moreover, the identities

$$\lfloor 1 \rfloor \odot X = X, \quad X \in \lfloor R \rfloor^3, \tag{1.15}$$

(1.16) $$c \odot (X \oplus Y) = (c \odot X) \oplus (c \odot Y), \quad c \in \underbracket{R}, \ X, Y \in \underbracket{R}^3,$$

(1.17) $$(c_1 \oplus c_2) \odot X = (c_1 \odot X) \oplus (c_2 \odot X), \quad c_1, c_2 \in \underbracket{R}, \ x \in \underbracket{R}^3,$$

(1.18) $$(c_1 \odot c_2) \odot X = c_1 \odot (c_2 \odot X), \quad c_1, c_2 \in \underbracket{R} \ X \in \underbracket{R}^3,$$

also hold.

Remark 1.19. By Theorem 1.10 we say that $\underbracket{R}^3$ is a sub-linear space with the operations (1.1) and (1.2).

Using (0.11), (0.3), (0.2) and (1.4) the identity (1.3) yields

(1.20) $$X \odot Y = \underbracket{\overset{\sqcup}{X} \cdot \overset{\sqcup}{Y}}, \quad X, Y \in \underbracket{R}^3,$$

where "·" means the familiar inner product (of vectors $\overset{\sqcup}{X}$ and $\overset{\sqcup}{Y}$) in R^3.

For the sub-inner product we have

Theorem 1.21. $\underbracket{R}^3$ *in a Euclidean vector space with the sub-inner product defined by* (1.3) *such that the sub-inner product has the following properties*

(1.22) $$X \odot Y = Y \odot X, \quad X, Y \in \underbracket{R}^3,$$

(1.23) $$(X \oplus Y) \odot Z = (X \odot Z) \oplus (Y \odot Z), \quad X, Y, Z \in \underbracket{R}^3$$

(1.24) $$(c \odot X) \odot Y = c \odot (X \odot Y), \quad c \in \underbracket{R}, \quad X, Y \in \underbracket{R}^3$$

and for any $X \in \underbracket{R}^3$ *the inequality*

(1.25) $$X \odot X \geq 0 \quad \textit{holds such that} \quad X \odot X = 0 \quad \textit{if and only if} \quad X = 0.$$

Remark 1.26. By Theorem 1.21 we say that $\underbracket{R}^3$ is a sub-euclidean space with the sub-inner product (1.3).

In [4] the concept of sub-function was defined for one variable (see [4], (0.8) and (0.9)). Hence, we have the sub-square root function

$$\text{sub}\sqrt{x} = \underset{\sqcup}{\sqrt{\overset{\sqcup}{x}}}, \quad x \in [0,1). \tag{1.27}$$

Having the property (1.25) and using the sub-square root function we can define the sub-norm as follows:

$$\|X\|_{\underset{\sqcup}{R}^3} = \text{sub}\sqrt{X \odot X}, \quad x \in \underset{\sqcup}{R}^3. \tag{1.28}$$

Using (1.27), (1.20) and (0.12) the definition (1.28) yields

$$\|X\|_{\underset{\sqcup}{R}^3} = \underset{\sqcup}{\|\overset{\sqcup}{X}\|_{R^3}}, \quad x \in \underset{\sqcup}{R}^3, \tag{1.29}$$

where $\|\cdot\|_{R^3}$ means the familiar norm of vectors.

Remark 1.30. Applying the familiar Cauchy's inequality by (1.20), (0.1), (0.3) and (1.29) we have the inequality

$$|X \odot Y| \leq \|X\|_{\underset{\sqcup}{R}^3} \odot \|Y\|_{\underset{\sqcup}{R}^3}, \quad X, Y, \in \underset{\sqcup}{R}^3.$$

Corollary 1.31. *The sub-norm has the following properties*

$$\|X\|_{\underset{\sqcup}{R}^3} \geq 0, \ (X \in \underset{\sqcup}{R}^3) \textit{ such that} \|X\|_{\underset{\sqcup}{R}^3} = 0 \textit{ if and only if } X = 0, \tag{1.32}$$

$$\|c \odot X\|_{\underset{\sqcup}{R}^3} = |c| \odot \|X\|_{\underset{\sqcup}{R}^3}, \quad c \in \underset{\sqcup}{R}, \quad X \in \underset{\sqcup}{R}^3 \tag{1.33}$$

and

$$\|X \oplus Y\|_{\underset{\sqcup}{R}^3} \leq \|X\|_{\underset{\sqcup}{R}^3} \oplus \|Y\|_{\underset{\sqcup}{R}^3}, \quad X, Y \in \underset{\sqcup}{R}^3. \tag{1.34}$$

Remark 1.35. By Corollary 1.31 we say that $\underset{\sqcup}{R}^3$ is a sub-normed space with the sub-norm (1.28).

Finally, we define the sub-distance of elements of $\underset{\sqcup}{R}^3$ as follows

$$d_{\underset{\sqcup}{R}^3}(X,Y) = \|X \ominus Y\|_{\underset{\sqcup}{R}^3}, \quad X, Y \in \underset{\sqcup}{R}^3, \tag{1.36}$$

where the sub-subtraction of vectors is defined by

$$X \ominus Y = X \oplus (-Y). \tag{1.37}$$

Using (1.29), (1.37), (1.8), (1.7), (1.4) and (0.10) the definition (1.36) yields

$$d_{\lfloor R \rfloor^3}(X, Y) = \lfloor d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Y}) \rfloor, \quad X, Y \in \lfloor R \rfloor^3, \tag{1.38}$$

where d_{R^3} is the familiar distance of the points of R^3.

Corollary 1.39. *The sub-distance has the following properties*

$$d_{\lfloor R \rfloor^3}(X, Y) = d_{\lfloor R \rfloor^3}(Y, X), \quad X, Y \in \lfloor R \rfloor^3, \tag{1.40}$$

$$d_{\lfloor R \rfloor^3}(X, Y) \geq 0 \quad \textit{such that} \quad d_{\lfloor R \rfloor^3}(X, Y) = 0 \quad \textit{if and only if} \tag{1.41}$$

$$X = Y, \quad X, Y \in \lfloor R \rfloor^3$$

and

$$d_{\lfloor R \rfloor^3}(X, Y) \leq d_{\lfloor R \rfloor^3}(X, Z) \oplus d_{\lfloor R \rfloor^3}(Z, Y), \quad X, Y, Z \in \lfloor R \rfloor^3. \tag{1.42}$$

Remark 1.43. By Corollary 1.39 we say that $\lfloor R \rfloor^3$ is a sub-metrical space with the sub-distance (1.36).

2. On the geometry of $\lfloor R \rfloor^3$

Our starting point is the Euclidean geometry of R^3 with its points, lines and planes based on the axioms formulated by Hilbert. Now we construct the cube-model of the classical Euclidean geometry. The points of the model will be the points of R^3. Considering a line ℓ in R^3 its compressed will be the set of compressed points of ℓ denoted by $\lfloor \ell \rfloor$. Considering a plane s in R^3 its compressed will be the set of compressed points of s denoted by $\lfloor s \rfloor$. The set $\lambda = \lfloor \ell \rfloor$ is called *sub-line* and the set $\sigma = \lfloor s \rfloor$ is called *sub-plane*. Clearly, $\lambda \subset \lfloor R \rfloor^3$ and $\sigma \subset \lfloor R \rfloor^3$. Moreover, the exploded of a sub-line is a line and the exploded of a sub-plane is a plane, that is $\overset{\sqcup}{\lambda} = \ell$ and $\overset{\sqcup}{\sigma} = s$.

By the axioms of the euclidean geometry of R^3 we have the properties of the geometry of $\underset{\sqcup}{R}^3$.

Denoting by $\mathbf{L}$ the set of lines of R^3, by $\mathbf{P}$ the set of planes of R^3, $(R^3, \mathbf{L}, \mathbf{P})$ is a so-called incidence geometry (see [3]). Considering $\underset{\sqcup}{\mathbf{L}} = \{\underset{\sqcup}{\ell} \colon \ell \in \mathbf{L}\}$ and $\underset{\sqcup}{\mathbf{P}} = \{\underset{\sqcup}{s} \colon s \in \mathbf{P}\}$, $(\underset{\sqcup}{R}^3, \underset{\sqcup}{\mathbf{L}}, \underset{\sqcup}{\mathbf{P}})$ is also an incidence geometry. Now we give the properties of "incidence".

Property 2.1. If X and Y are distinct points of $\underset{\sqcup}{R}^3$ then there exists a sub-line λ that contains both X and Y

Property 2.2. There is only one λ such that $X \in \lambda$ and $Y \in \lambda$.

Property 2.3. Any sub-line has at least two points. There exist at least three points not all in one sub-line.

Property 2.4. If X, Y and Z not are in the same sub-line then there exists a sub-plane σ such that X, Y and Z are in σ. Any sub-plane has a point at least.

Property 2.5. If X, Y and Z are different non sub-collinear points, there is exactly one sub-plane containing them.

Property 2.6. If two points lie in a sub-line, then the line containing them lies in the plane.

Property 2.7. If two sub-planes have a joint point then they have another joint point, too.

Property 2.8. There exists at least four points such that they are not on the same sub-plane.

We will say that the *point Z is between the points X and Y on the sub-line λ if $\overset{\sqcup}{Z}$ is between $\overset{\sqcup}{X}$ and $\overset{\sqcup}{Y}$ on the line $\overset{\sqcup}{\lambda}$*. The concept of "between" has the following properties:

Property 2.9. If Z is between X and Y then X, Y and Z are three different points of a sub-line and Z is between Y and X.

Property 2.10. For any arbitrary point X and Y there exists at least one point Z lying on the sub-line determined by X and Y such that Z is between X and Y.

Property 2.11. For any three points of a sub-line there is only one between the other two.

Property 2.12. (Pasch-type property.) If X, Y and Z are not in the same sub-line and λ is a sub-line of the sub-plane determined by the points X, Y and Z such that λ has not points X, Y or Z but it has a joint point with the sub-segment XY of the sub-line determined by X and Y then λ has a joint point with one of the sub-segmentes XZ or YZ of the sub-lines determined by X and Z or Y and Z, respectively.

We will say that *two sets in $\underset{\sqcup}{R}^3$ are sub-congruent if their explodeds are congruent in the familiar sense.* Let two half-lines be given with the same starting point W and let be U and V their inner points. Let us consider the familiar convex angle $\measuredangle\, UWV$. Compressing this angle we obtain the sub-angle sub $\measuredangle\, \lfloor U \rfloor \lfloor W \rfloor \lfloor V \rfloor$ (or sub-angle sub $\measuredangle\, XZY$ where $X = \lfloor U \rfloor$, $Y = \lfloor V \rfloor$ and $Z = \lfloor W \rfloor$) with the peak-point $\lfloor W \rfloor$ and bordered by the sub-half-lines determined by the points $\lfloor W \rfloor$, $\lfloor U \rfloor$ and $\lfloor W \rfloor$, $\lfloor V \rfloor$. The concept of "sub-congruence" and "sub-angle" have the following properties

Property 2.13. On a given sub-half-line there always exists at least one sub-segment such that one of its end-points is the starting point of the sub-half-line and this sub-segment is sub-congruent with an earlier given sub-segment.

Property 2.14. If both sub-segments p_1 and p_2 are sub-congruent with the sub-segments p_3 then p_1 and p_2 are sub-congruent.

Property 2.15. If sub-segment p_1 is sub-congruent with sub-segment q_1 and p_2 is sub-congruent with q_2 then $p_1 \cup p_2$ is sub-congruent with $q_1 \cup q_2$.

Property 2.16. On a given side of a sub-half-lines there exists only one sub-angle which is sub congruent with a given sub-angle. Each sub angle is sub-congruent with itself.

Property 2.17. Let us consider two sub-triangles. If two sides and sub-angles enclosed by these sides are sub-congruent in the sub-triangles mentioned above then they have another sub-congruent sub-angles.

We say that *the sub-lines λ_1 and λ_2 are sub-parallel if their explodeds $\overset{\sqcup}{\lambda_1}$ and $\overset{\sqcup}{\lambda_2}$ are parallel lines in the familiar sense.* Now we have

Property 2.18. If a sub-line λ_1 and a point X are given such that X is off λ_1 then there exists only one sub-line λ_2 through X that is sub-parallel to λ_1.

Finally, we mention two properties for continuity.

Property 2.19. (Archimedes-type property.) If a point X_1 is between the points X and Y on a sub-line then there are points X_2 $X_3, \ldots, X_n$ such that the sub-segments $X_{i-1}X_i$; $(i = 2, 3, \ldots, n)$ are sub-congruent with sub-segment XX_1 and Y is between points X and X_n.

Property 2.20. (Cantor-type property.) If $\{X_nY_n\}_{n=1}^{\infty}$ is a sequence of sub-segments lying on a sub-line λ such that for any $n = 1, 2, 3, \ldots$, $X_{n+1}Y_{n+1} \subset X_nY_n$ then there exists at least one point Z of λ such that Z belongs to each X_n Y_n.

To measure the sub-segments and sub-angles we can use the principle of isomorphic expressed by the identities (1.8), (1.9) and (1.20). If the sub-segment p has the end-points X and Y then its sub-measure can be defined as follows:

$$\text{sub meas}\, p = \lfloor \text{meas}\ \overset{\sqcup}{p} \rfloor, \tag{2.21}$$

where meas $\overset{\sqcup}{p}$ is understood in the traditional sense. Considering that $\overset{\sqcup}{p}$ is a segment bordered by $\overset{\sqcup}{X}$ and $\overset{\sqcup}{Y}$ we have that

$$\text{meas}\ \overset{\sqcup}{p} = D_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Y}).$$

Hence, by (2.21) and (1.38) we have

$$\text{sub meas}\, p = d_{\underset{\sqcup}{R}^3}(X,Y), \tag{2.22}$$

which is the *sub-distance* of X and Y.

Similarly, to measure sub-angles we write

$$\text{sub meas sub} \measuredangle XZY = \underbrace{\text{meas} \measuredangle \overset{\sqcup}{X} \overset{\sqcup}{Z} \overset{\sqcup}{Y}} \tag{2.23}$$

where meas $\measuredangle \overset{\sqcup}{X} \overset{\sqcup}{Z} \overset{\sqcup}{Y}$ is understood in the traditional sense. Using the concept of sub-function again, we obtain that

$$\text{sub arc}\cos x = \underbrace{\text{arc}\cos \overset{\sqcup}{x}}, \quad x \in [-\underset{\sqcup}{1}, \underset{\sqcup}{1}]. \tag{2.24}$$

Moreover, we have the following

Theorem 2.25. *If X, Y and Z are given points of $\underset{\sqcup}{R}^3$ such that $X \neq Z$ and $Y \neq Z$ then*

$$\begin{aligned} &\text{sub meas sub} \measuredangle XZY \\ &= \text{sub arc}\cos(((X \ominus Z) \odot (Y \ominus Z)) \bigodot (d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z))). \end{aligned} \tag{2.26}$$

3. Examples for special subsets of $\underset{\sqcup}{R}^3$

Example 3.1. First, we show that the equation

$$X = B \oplus (\tau \odot M), \quad \tau \in \underset{\sqcup}{R} \tag{3.2}$$

where B, M are given points of $\underset{\sqcup}{R}^3$ with the condition

$$\|M\|_{\underset{\sqcup}{R}^3} = \underset{\sqcup}{1} \tag{3.3}$$

represents a sub-line. Really, using (1.8), (1.7) and (1.9) the equation (3.2) yields the equation

$$\overset{\sqcup}{X} = \overset{\sqcup}{B} + t\, \overset{\sqcup}{M}, \quad t = \overset{\sqcup}{\tau} \in R \tag{3.4}$$

which represents a line. Moreovoer, by (1.29) and (0.12) the condition (3.3) means that

$$\| \overset{\sqcup}{M} \|_{R^3} = 1 \tag{3.5}$$

holds. Writing that $B = (b_1, b_2, b_3)$ and $M = (m_1, m_2, m_3)$, the equation (3.2) is equivalent to the equation-system

$$\begin{aligned} x_1 &= b_1 \oplus (\tau \odot m_1) \\ x_2 &= b_2 \oplus (\tau \odot m_2)\,, \qquad \tau \in \underset{\sqcup}{R} \\ x_3 &= b_3 \oplus (\tau \odot m_3) \end{aligned}$$

which considering (0.4) and (0.5) can be written in the following form

$$\begin{aligned} x_1 &= \frac{b_1 + \mathrm{th}((\mathrm{ar\,th}\,\tau)(\mathrm{ar\,th}\,m_1))}{1 + b_2\,\mathrm{th}((\mathrm{ar\,th}\,\tau)(\mathrm{ar\,th}\,m_1))} \\ x_2 &= \frac{b_2 + \mathrm{th}((\mathrm{ar\,th}\,\tau)(\mathrm{ar\,th}\,m_2))}{1 + b_2\,\mathrm{th}((\mathrm{ar\,th}\,\tau)(\mathrm{ar\,th}\,m_2))}, \qquad (-1 < \tau < 1) \\ x_3 &= \frac{b_3 + \mathrm{th}((\mathrm{ar\,th}\,\tau)(\mathrm{ar\,th}\,m_3))}{1 + b_3\,\mathrm{th}((\mathrm{ar\,th}\,\tau)(\mathrm{ar\,th}\,m_3))}. \end{aligned} \tag{3.6}$$

In the special case $B = \left(0, 0, \frac{1}{2}\right)$ and $M = \left(\mathrm{th}\,\frac{1}{\sqrt{6}}, \mathrm{th}\,\frac{1}{\sqrt{6}}, \mathrm{th}\,\frac{2}{\sqrt{6}}\right)$ then (3.6) is

$$\begin{aligned} x_1 &= \mathrm{th}\left(\frac{1}{\sqrt{6}}\,\mathrm{ar\,th}\,\tau\right) \\ x_2 &= \mathrm{th}\left(\frac{1}{\sqrt{6}}\,\mathrm{ar\,th}\,\tau\right), \qquad -1 < \tau < 1 \\ x_3 &= \frac{1 + 2\,\mathrm{th}\left(\frac{2}{\sqrt{6}}\,\mathrm{ar\,th}\,\tau\right)}{2 + \mathrm{th}\left(\frac{2}{\sqrt{6}}\,\mathrm{ar\,th}\,\tau\right)} \end{aligned} \tag{3.7}$$

and the sub-line is shown in the following figure:

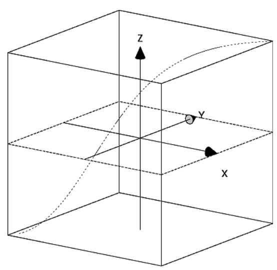

Fig. 3.8

Example 3.9. The sub-line given by the equation-system (3.7) (see Fig. 3.8) and the sub-line given by the equation-system

$$\begin{aligned} x_1 &= \operatorname{th}\left(\frac{1}{\sqrt{6}} \operatorname{ar\,th} \tau\right) \\ x_2 &= \operatorname{th}\left(\frac{1}{\sqrt{6}} \operatorname{ar\,th} \tau\right), \quad -1 < \tau < 1 \\ x_3 &= \operatorname{th}\left(\frac{2}{\sqrt{6}} \operatorname{ar\,th} \tau\right) \end{aligned} \tag{3.10}$$

are sub-parallel and their graphs are shown in the following figure:

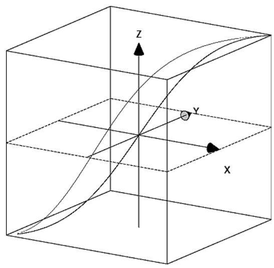

Fig. 3.11

Example 3.12. The sub-line given by the equation system (3.7) (see Fig. 3.8) and the sub-line given by the equation-system

$$\begin{aligned} x_1 &= \operatorname{th}\left(\frac{1}{\sqrt{6}} \operatorname{ar\,th} \tau\right) \\ x_2 &= -\operatorname{th}\left(\frac{1}{\sqrt{6}} \operatorname{ar\,th} \tau\right), \quad -1 < \tau < 1 \\ x_3 &= \frac{1 + 2\operatorname{th}\left(\frac{2}{\sqrt{6}} \operatorname{ar\,th} \tau\right)}{2 + \operatorname{th}\left(\frac{2}{\sqrt{6}} \operatorname{ar\,th} \tau\right)} \end{aligned} \tag{3.13}$$

has the joint point $B = \left(0, 0, \frac{1}{2}\right)$. Their graphs are shown in the following figure:

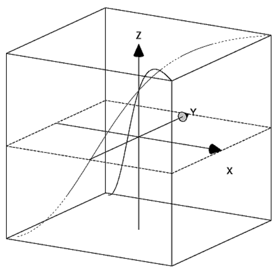

Fig. 3.14

Example 3.15. The sub-lines given by (3.10) (see Fig. 3.11) and (3.13) (see Fig. 3.14) have neither a joint point nor a joint sub-plane. They can be seen in the following figure

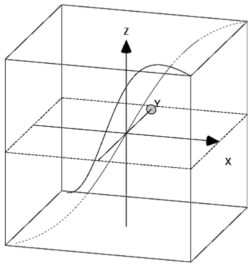

Fig. 3.16

Example 3.17. The equation

$$z = x \oplus y \oplus \frac{1}{2}, \quad x, y \in \underline{R} \tag{3.18}$$

represents a sub-plane. Really, by (0.11) and (0.2) the computation

$$\overset{\sqcup}{z} = \overline{x \oplus y \oplus \tfrac{1}{2}} = \overline{\underline{(\overset{\sqcup}{x})} \oplus \underline{(\overset{\sqcup}{y})}} \oplus \underline{(\overline{(\tfrac{1}{2})})} = \overline{\underline{\overset{\sqcup}{x} + \overset{\sqcup}{y}} \oplus \underline{(\overline{(\tfrac{1}{2})})}}$$
$$= \overline{(\underline{\overset{\sqcup}{x} + \overset{\sqcup}{y} + \overline{(\tfrac{1}{2})}})} = \overset{\sqcup}{x} + \overset{\sqcup}{y} + \overline{(\tfrac{1}{2})}$$

shows that if (x, y, z) satisfies (3.18) then the points $(\overset{\sqcup}{x}, \overset{\sqcup}{y}, \overset{\sqcup}{z})$ form a plane. By (0.4) the equation (3.18) is equivalent to the

$$z = \frac{xy + 2x + 2y + 1}{2xy + x + y + 2}, \quad -1 < x, y < 1, \tag{3.19}$$

so we have the surface of a sub-plane

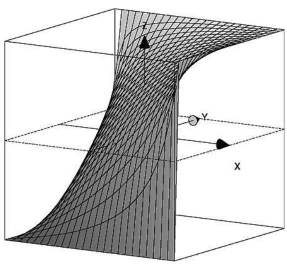

Fig. 3.20

The equation (3.19) shows that the sub-line (3.7) coincides with the sub-plane given by (3.18) . The Fig. 3.20 shows this fact.

The sub-plane determined by the equation

$$(3.21)\qquad z = x \oplus y \left(= \frac{x+y}{1+xy} \right), \quad x, y \in \underline{R}$$

is sub-parallel with the sub-plane given by (3.18). Their surfaces are shown in the following figure:

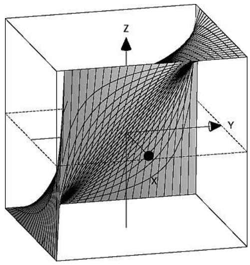

Fig. 3.22

Fig. 3.22 shows that the sub-line (3.10) is on the sub-plane (3.21).

Example 3.23. Considering the set

$$(3.24)\qquad S_{X_0}(\rho) = \{X \in \underline{R}^3 : \ d_{\underline{R}^3}(X, X_0) = \rho, X_0 \in \underline{R}^3 \quad \text{and} \quad \rho \in \underline{R^+}\}$$

by (1.38) and (0.12) we have

$$(3.25)\qquad d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{X_0}) = \overset{\sqcup}{\rho},$$

that is the points $\overset{\sqcup}{X} \in R^3$ form a sphere with centre $\overset{\sqcup}{X}_0$ and radius $\overset{\sqcup}{\rho}$. Therefore $S_{X_0}(\rho)$ is called a *sub-sphere with centre* X_0 *and radius* ρ. By (1.4), (3.25) and (0.10) we get the equation of sub-sphere

$$(3.26)\qquad \begin{aligned} &(\operatorname{ar\,th} x - \operatorname{ar\,th} x_0)^2 + (\operatorname{ar\,th} y - \operatorname{ar\,th} y_0)^2 + \\ &+ (\operatorname{ar\,th} z - \operatorname{ar\,th} z_0)^2 = (\operatorname{ar\,th} \rho)^2 \end{aligned}$$

where $X = (x, y, z)$ and $X_0 = (x_0, y_0, z_0)$ are elements of $\underline{R}^3$.

Although the sub-sphere is determined anambiguously by its centre and radius, its form depends on the place of the centre too. Moreover, it is not symmetrical in a traditional sense for its centre. The following figures show the sub-spheres

$$S_{(\underline{1}, \underline{1}, \underline{1})}\left(\underline{\left(\tfrac{1}{2}\right)}\right), \ S_{(\underline{1}, \underline{1}, \underline{1})}(\underline{1}) \quad \text{and} \quad S_{(\underline{1}, \underline{1}, \underline{1})}\left(\underline{\left(\tfrac{3}{2}\right)}\right)$$

having the equations

$$(\operatorname{ar\,th} x - 1)^2 + (\operatorname{ar\,th} y - 1)^2 + (\operatorname{ar\,th} z - 1)^2 = \frac{1}{4}$$

$$(\operatorname{ar\,th} x - 1)^2 + (\operatorname{ar\,th} y - 1)^2 + (\operatorname{ar\,th} z - 1)^2 = 1$$

and

$$(\operatorname{ar\,th} x - 1)^2 + (\operatorname{ar\,th} y - 1)^2 + (\operatorname{ar\,th} z - 1)^2 = \frac{9}{4},$$

respectively

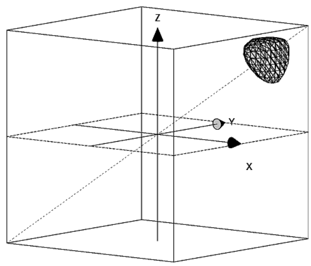

Fig. 3.27

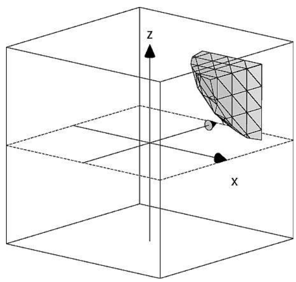

Fig. 3.28

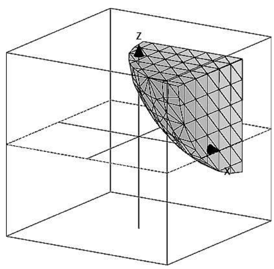

Fig. 3.29

The sub-spheres $S_O(\rho)$ are symmetrical in a traditional sense for their centre o. By (3.26) the sub-sphere $S_0(\rho)$ has the following equation

$$(\mathrm{ar\,th}\,x)^2 + (\mathrm{ar\,th}\,y)^2 + (\mathrm{ar\,th}\,z)^2 = (\mathrm{ar\,th}\,\rho)^2. \tag{3.30}$$

Considering now the sub-spheres $S_O(\underline{{}_{\lfloor}(\frac{1}{2})_{\rfloor}})$, $S_O(\underline{{}_{\lfloor}1_{\rfloor}})$ and $S_o(\underline{{}_{\lfloor}(\frac{3}{2})_{\rfloor}})$ we obtain their equations by (3.30)

$$(\mathrm{ar\,th}\,x)^2 + (\mathrm{ar\,th}\,y)^2 + (\mathrm{ar\,th}\,z)^2 = \frac{1}{4}$$

$$(\mathrm{ar\,th}\,x)^2 + (\mathrm{ar\,th}\,y)^2 + (\mathrm{ar\,th}\,z)^2 = 1$$

and

$$(\mathrm{ar\,th}\,x)^2 + (\mathrm{ar\,th}\,y)^2 + (\mathrm{ar\,th}\,z)^2 = \frac{9}{4}$$

and they are shown in the following figures:

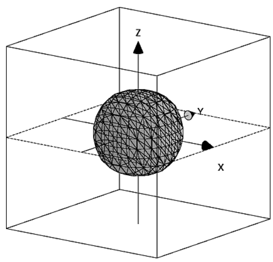

Fig. 3.31

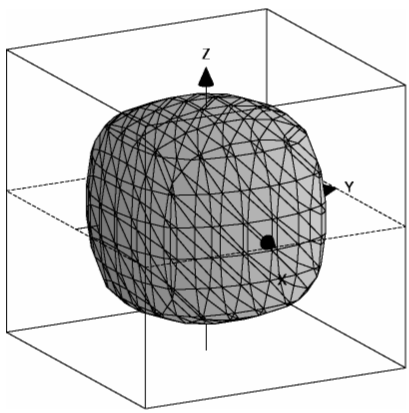

Fig. 3.32

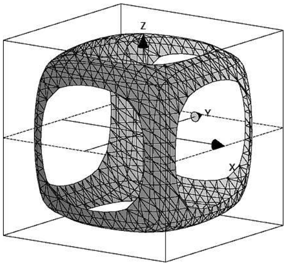

Fig. 3.33

4. Proof of Theorems

4.1. Proof of Theorem 1.10. Considering that the verifications of identitites (1.11)–(1.14) are very similar, we give the proof of identity (1.12), only. After (1.8) and (1.7) we apply the familiar associativity of addition of vectors and using (1.7) and (18) again, we obtain:

$$\begin{aligned}(X\oplus Y)\oplus Z &= \underline{\overset{\sqcup}{X\oplus Y} + \overset{\sqcup}{Z}} = \underline{\overline{(\underline{\overset{\sqcup}{X} + \overset{\sqcup}{Y}})} + \overset{\sqcup}{Z}} \\ &= \underline{(\overset{\sqcup}{X} + \overset{\sqcup}{Y}) + \overset{\sqcup}{Z}} = \underline{\overset{\sqcup}{X} + (\overset{\sqcup}{Y} + \overset{\sqcup}{Z})} = \underline{\overset{\sqcup}{X} + \overline{(\underline{\overset{\sqcup}{Y} + \overset{\sqcup}{Z}})}} \\ &= \underline{\overset{\sqcup}{X} + \overset{\sqcup}{Y\oplus Z}} = X\oplus(Y\oplus Z).\end{aligned}$$

Considering that the verifications of identities (1.15)–(1.18) are very similar, we give the proof of identity (1.16), only. After (1.19), (1.8), and (1.7) we apply a familiar distributive property of multiplication of vectors by scalar and using (1.9) and (18) again, we get

$$\begin{aligned}c\odot(X\oplus Y) &= \underline{\overset{\sqcup}{c} \oplus \overset{\sqcup}{X\oplus Y}} = \underline{\overset{\sqcup}{c}\,\overline{(\underline{\overset{\sqcup}{X} + \overset{\sqcup}{Y}})}} = \underline{\overset{\sqcup}{c}\,(\overset{\sqcup}{X} + \overset{\sqcup}{Y})} \\ &= \underline{\overset{\sqcup}{c}\,\overset{\sqcup}{X} + \overset{\sqcup}{c}\,\overset{\sqcup}{Y}} = \underline{\overline{(\underline{\overset{\sqcup}{c}\,\overset{\sqcup}{X}})} + \overline{(\underline{\overset{\sqcup}{c}\,\overset{\sqcup}{Y}})}} \\ &= \underline{\overset{\sqcup}{c\odot X} + \overset{\sqcup}{c\odot Y}} = (c\odot X)\oplus(c\odot Y).\end{aligned}$$

4.2. Proof of Theorem 1.21. The verifications of identities (1.22)–(1.24) are very similar to the verifications mentioned above, so we prove the property (1.25), only. Using (1.20), (1.4) and (0.1)

$$X\odot X = \underline{\overset{\sqcup}{X}\cdot\overset{\sqcup}{X}} = \operatorname{th}((\overset{\sqcup}{x}_1)^2) + (\overset{\sqcup}{x}_2)^2 + (\overset{\sqcup}{x}_3)^2) \geq 0$$

is obtained. Moreover, we have zero if and only if $\overset{\sqcup}{X} = O$ which by (1.4) and (0.10) means that $X = O$.

4.3. Proof of Theorem 1.31. The proof of property (1.32) is very similar to the proof of property (1.25), so we omit it. The identity (1.33) does not need new methods, so we accept it. We prove inequality (1.34). After (1.29), (1.8), (1.7) and (0.1) we apply the Minkowski-inequality and using (0.2) and (1.29), we can write

$$\|X \oplus Y\|_{\underset{\sqcup}{R}^3} = \underset{\sqcup}{\| \overset{\sqcup}{X \oplus Y} \|_{R^3}} = \underset{\sqcup}{\| \overset{\sqcup}{X} + \overset{\sqcup}{Y} \|_{R^3}} \leq$$

$$\leq \underset{\sqcup}{\| \overset{\sqcup}{X} \|_{R^3} + \| \overset{\sqcup}{Y} \|_{R^3}} = \underset{\sqcup}{\| \overset{\sqcup}{X} \|_{R^3}} \oplus \underset{\sqcup}{\| \overset{\sqcup}{Y} \|_{R^3}} = \|X\|_{\underset{\sqcup}{R}^3} \oplus \|Y\|_{\underset{\sqcup}{R}^3}.$$

4.4. Proof of Theorem 1.39. Identity (1.40) is trivial, the verification of property (1.41) is easy, so we omit them. We verify the inequality (1.42), only. After (1.38) we use the triangular inequality and using (0.2) and (1.38) again, we have

$$d_{\underset{\sqcup}{R}^3}(X,Y) = \underset{\sqcup}{d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Y})} \leq \underset{\sqcup}{d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Z}) + d_{R^3}(\overset{\sqcup}{Z}, \overset{\sqcup}{Y})} =$$

$$= \underset{\sqcup}{d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Z})} \oplus \underset{\sqcup}{d_{R^3}(\overset{\sqcup}{Z}, \overset{\sqcup}{Y})} = d_{\underset{\sqcup}{R}^3}(X,Z) \oplus d_{\underset{\sqcup}{R}^3}(Z,Y).$$

4.5. Proof of Theorem 2.25. Our proof is based on the well-known inequality concerning the familiar angles enclosed by vectors. Namely,

$$(U - W)(V - W) = d_{R^3}(U,W) \cdot d_{R^3}(V,W) \cos \measuredangle UWV$$

where $U, V, W \in R^3$ such that $U \neq W$ and $V \neq W$. Hence, denoting by $U = \overset{\sqcup}{X}$, $V = \overset{\sqcup}{Y}$ and $W = \overset{\sqcup}{Z}$, we have

$$\text{meas} \measuredangle \overset{\sqcup}{X}\,\overset{\sqcup}{Z}\,\overset{\sqcup}{Y} = \arccos \frac{(\overset{\sqcup}{X} - \overset{\sqcup}{Z}) \cdot (\overset{\sqcup}{Y} - \overset{\sqcup}{Z})}{d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Z}) \cdot d_{R^3}(\overset{\sqcup}{Y}, \overset{\sqcup}{Z})}. \tag{4.6}$$

Applying (1.7), (1.8) and (1.37) we have that $\overset{\sqcup}{X} - \overset{\sqcup}{Z} = \overset{\sqcup}{X \ominus Z}$ and $\overset{\sqcup}{Y} - \overset{\sqcup}{Z} = \overset{\sqcup}{Y \ominus Z}$ hold. Hence (1.7) and (1.20) yield

$$(\overset{\sqcup}{X} - \overset{\sqcup}{Z}) \cdot (\overset{\sqcup}{Y} - \overset{\sqcup}{Z}) = \overset{\sqcup}{(X \ominus Z) \odot (Y \ominus Z)}. \tag{4.7}$$

On the other hand, by (0.12), (1.38), (0.12) again, (0.3) and (0.11) we have

$$d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Z}) \cdot d_{R^3}(\overset{\sqcup}{Y}, \overset{\sqcup}{Z}) = \overline{\underline{(d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Z}))}} \cdot \overline{\underline{(d_{R^3}(\overset{\sqcup}{Y}, \overset{\sqcup}{Z}))}}$$

$$= \overline{d_{\underset{\sqcup}{R}^3}(X,Y)} \cdot \overline{d_{\underset{\sqcup}{R}^3}(Y,Z)} = \overline{\underline{(\overline{d_{\underset{\sqcup}{R}^3}(x,Y)} \cdot \overline{d_{\underset{\sqcup}{R}^3}(Y,Z)})}}$$

$$= \overline{\underline{(\overline{d_{\underset{\sqcup}{R}^3}(X,Z)})} \odot \underline{(\overline{d_{\underset{\sqcup}{R}^3}(Y,Z)})}} = \overline{d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z)}\,.$$

Hence, by (4.7), (0.12), (0.7) and (0.11) we can write

$$\frac{(\overset{\sqcup}{X} - \overset{\sqcup}{Z}) \cdot (\overset{\sqcup}{Y} - \overset{\sqcup}{Z})}{d_{R^3}(\overset{\sqcup}{X}, \overset{\sqcup}{Z}) \cdot d_{R^3}(\overset{\sqcup}{Y}, \overset{\sqcup}{Z})} = \frac{\overline{(X \ominus Z) \odot (Y \ominus Z)}}{\overline{d_{\underset{\sqcup}{R}^3}(X,Y) \odot d_{\underset{\sqcup}{R}^3}(Y,Z)}}$$

$$= \overline{\underline{\left(\left(\frac{\overline{(X \ominus z) \odot (Y \ominus Z)}}{\overline{d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z)}}\right)\right)}}$$

$$= \overline{\underline{(\overline{(X \ominus Z) \odot (Y \ominus Z)})} \bigodot \underline{(\overline{d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z)})}}$$

$$= \overline{((X \ominus Z) \odot (Y \ominus Z)) \bigodot (d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z))}\,.$$

Returning to (4.6) we obtain that

$$\operatorname{meas} \measuredangle \overset{\sqcup}{X}\, \overset{\sqcup}{Z}\, \overset{\sqcup}{Y}$$

$$= \arccos \overline{((X \ominus Z) \odot (Y \ominus Z)) \bigodot (d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z))}$$

holds. Hence, (2.23) and (2.24) yield

$$\operatorname{sub} \operatorname{meas} \operatorname{sub} \measuredangle XZY$$

$$= \underline{\arccos \overline{((X \ominus Z) \odot (Y \ominus Z)) \bigodot (d_{\underset{\sqcup}{R}^3}(X,Z) \odot d_{\underset{\sqcup}{R}^3}(Y,Z))}}$$

$$= \operatorname{sub}\arccos(((X \ominus Z) \odot (Y \ominus Z)) \bigodot (d_{\underbracket{R}^3}(X,Z) \odot d_{\underbracket{R}^3}(Y,Z))),$$

that is, we have (2.26).

References

[1] Császár Ákos: *Valós analízis.* Tankönyvkiadó, Budapest, 1983.

[2] *Matematikai kislexikon* (Editor in chief M. Farkas), Műszaki Könyvkiadó 3. kiadás, 1979.

[3] Radó Ferenc és Orbán Béla: *A geometriai mai szemmel.* Dacia Kiadó, Kolozsvár, 1981.

[4] Szalay I., On the compressed Descartes-plane and its applications, *AMAPN* **17** (2001), 37–46.

Szalay István
Department for Matehamatics
Juhász Gyula Teacher Training College
University of Szeged
6701 Szeged, P. O. Box 396.
Hungary
E-mail: szalay@jgytf.u-szeged.hu

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 35–39*

ON ORBITS IN AMBIGUOUS IDEALS

Juraj Kostra (Ostrava, Czech Republic)

Dedicated to the memory of Professor Péter Kiss

Abstract. Let K be a tamely ramified algebraic number field. The paper deals with polynomial cycles for a polynomial $f \in Z[x]$ in ambiguous ideals of Z_K. A connection between the existence of "normal" and "power" basis and the existence of polynomial orbits is given.

AMS Classification Number: 11R18, 11C08, 12F05

1. Introduction

Let R be a ring. A finite subset $\{x_0, x_1, \dots, x_{n-1}\}$ of the ring R is called a cycle, n-cycle or polynomial cycle for polynomial, $f \in R[x]$, if for $i = 0, 1, \dots, n-2$ one has $f(x_i) = x_{i+1}$, $f(x_{n-1}) = x_0$ and $x_i \neq x_j$ for $i \neq j$. The number n is called the length of the cycle and the x_i's are called cyclic elements of order n or fixpoints of f of order n.

We can introduce a similar definition for a polynomial cycle in the situation that S, R are rings and R is an S-module.

A finite subset $\{x_0, x_1, \dots, x_{n-1}\}$ of an S-module R is called a cycle, n-cycle or polynomial cycle for polynomial $f \in S[x]$, if for $i = 0, 1, \dots, n-2$ one has $f(x_i) = x_{i+1}$, $f(x_{n-1}) = x_0$ and $x_i \neq x_j$ for $i \neq j$.

A finite sequence $\{y_0, y_1, \dots, y_m, y_{m+1}, \dots, y_{m+n-1}\}$ is called an orbit of $f \in S[x]$ with the precycle $\{y_0, y_1, \dots, y_{m-1}\}$ of length m and the cycle $\{y_m, y_{m+1}, \dots, y_{m+n-1}\}$ of length n if $f(y_i) = y_{i+1}$, $f(y_{m+n-1}) = y_m$ for distinct elements $y_0, y_1, \dots, y_{m+n-1}$ of R.

Let K be a Galois algebraic number field and let K/Q be a finite extension of rational numbers with a Galois group G. We will be interested in polynomial cycles generated by conjugated elements for polynomials from $Z[x]$ in the ring of integers Z_K of the field K and in ambiguous ideals of Z_K.

First we recall some general properties of ambiguous ideals according to Ullom [8]. Let K/F be a Galois extension of an algebraic number field F with the Galois group G and Z_K (resp. Z_F) be the ring of integers of K (resp. F).

This research was supported by GA ČR Grant 201/01/0471.

Definition 1. An ideal U of Z_K is G-ambiguous or simply ambiguous if U is invariant under action of the Galois group G.

Let $\Im$ be a prime ideal of F whose decomposition into prime ideals in K is

$$\Im Z_K = (\wp_1.\wp_2 \cdots \wp_g)^e.$$

Let $\Psi(\Im) = \wp_1.\wp_2 \cdots \wp_g$. It is known that

(i) $\Psi(\Im)$ is ambiguous and the set of all $\Psi(\Im)$ with $\Im$ prime in F is a free basis for the group of ambiguous ideals of K.

(ii) An ambiguous ideal U of Z_K may be written in the form $U_0.T$ where T is an ideal of Z_F and
$$U_0 = \Psi(\Im_1)^{a_1} \ldots \Psi(\Im_t)^{a_t}$$
where $0 < a_i \leq e_i$ and $e_i > 1$ is the ramification index of a prime ideal of Z_K dividing $\Im_i$. The ideal U determines U_0 and T uniquely. The ambiguous ideal U_0 is called a primitive ambiguous ideal.

In our investigation we will focus a special attention to cyclic extensions K/Q of prime degree l. In this case ambiguous ideals with normal basis were characterized in papers [3], [4] and [8].

2. Results

Let K/Q be a finite normal extension of rational numbers with a Galois group G.

Theorem 1. *Let $f \in Z[x]$ and $Y = \{y_0, y_1, \ldots\}$ be a sequence of elements of Z_K. Let $i < j$ such that y_i and y_j are conjugated over Z. Then Y is an orbit with the precycle of length $m \leq i$.*

Proof of Theorem 1. We denote by f_k the k-iteration of polynomial f. Then

$$f_{j-i}(y_i) = y_j.$$

The elements y_i and y_j are conjugated over Z and there is such an automorphism $\phi \in G$ that $\phi(y_i) = y_j$. Coefficients of f are from Z and it immediately follows that

$$\phi^s(y_i) = \phi^{s-1}(f(y_i)) = f(\phi^{s-1}(y_i)).$$

By induction it follows that

$$\phi^s(y_i) = y_{i+s(j-i)}.$$

The automorphism ϕ is of a finite order and so there is such an s_0 that $\phi^{s_0}(y_i) = y_i$.

Corollary 1. *Let K/Q be a cyclic extension of a prime degree l. Let $x_0, x_1, \dots, x_{l-1}$ be a polynomial cycle of the length l for $f \in Z[x]$ in Z_K. Then either all x_i are conjugated or x_i are pairwise not conjugated.*

Corollary 2. *Let K/Q be a cyclic extension of a prime degree l. Let $x_0, x_1, \dots, x_{n-1}$ be a polynomial cycle of the length n for $f \in Z[x]$ in Z_K. Then either l divides n or x_i are pairwise not conjugated.*

Now we will consider polynomial cycles of conjugated cyclic elements for polynomials $f \in Z[x]$ in ambiguous ideals of Z_K, where K/Q is a tamely ramified extension with Galois group G.

The following theorem gives a connection between the existence of a power basis for ambiguous ideals and the existence of a polynomial cycle consisting of elements of normal basis.

Theorem 2. *Let K/Q be a tamely ramified cyclic algebraic number field of prime degree l over Q. Let $\Im$ be a ambiguous ideal of Z_K with a normal basis $\{\alpha_0, \alpha_1, \dots, \alpha_{l-1}\}$ over Z. There exists a polynomial $f \in Z[x]$ of degree $k \leq l$ with the polynomial cycle $\{\alpha_0, \alpha_1, \dots, \alpha_{l-1}\}$ if and only if there are $0 \leq i \neq j < l$ that*

$$\alpha_i = a_t \alpha_j^t + a_{t-1} \alpha_j^{t-1} + \dots + a_0,$$

where $a_i \in z$.

Proof of Theorem 2. Let $\{\alpha_0, \alpha_1, \dots, \alpha_{l-1}\}$ be a polynomial cycle for $f \in Z[x]$ of degree $k \leq l$

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_0.$$

Then for example

$$\alpha_1 = f(\alpha_0) = a_k \alpha_0^k + a_{k-1} \alpha_0^{k-1} + \dots + a_0.$$

Let there are $0 \leq i \neq j < l$ such that

$$\alpha_i = a_t \alpha_j^t + a_{t-1} \alpha_j^{t-1} + \dots + a_0.$$

Then by Theorem 1 there is a polynomial cycle for $g(x) = a_t x^t + a_{t-1} x^{t-1} + \dots + a_0$ which started with conjugated elements α_j, α_i. It is obvious that all elements of this cycle are conjugated and by Corollary 2 it follows that the polynomial cycle consists of elements $\alpha_0, \alpha_1, \dots, \alpha_{l-1}$. Because all the elements are conjugated and they have the same minimal polynomial over Z of degree l, there exists a polynomial $f \in Z[x]$ of degree $k \leq l$ with the polynomial cycle consisting of elements $\alpha_0, \alpha_1, \dots, \alpha_{l-1}$.

Remark. In the above Theorem 2 let $f \in Z[x]$ be a polynomial with the normal basis

$$\{\alpha_0, \alpha_1, \dots, \alpha_{l-1}\}$$

as a polynomial cycle. Let

$$f_\alpha(x) = x^t + c_{t-1}x^{t-1} + \cdots + c_0$$

be a minimal polynomial for α_i. Then for any $i \in \{0, 1, \ldots, l-1\}$ the set

$$\{c_0, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{l-1}\}$$

is a "power" basis of $\Im$. For example let $Q(\zeta_7)$ be the 7-th cyclotomic field. The ideal $\wp_7$ lying over 7 in maximal real subfield K of $Q(\zeta_7)$ has a normal basis

$$\alpha_0 = 2 - \zeta_7 - \zeta_7^6, \alpha_1 = 2 - \zeta_7^2 - \zeta_7^5, \alpha_2 = 2 - \zeta_7^3 - \zeta_7^4.$$

The polynomial $f(x) = x^2 + 4x$ has the polynomial cycle $\alpha_0, \alpha_1, \alpha_2$. The minimal polynomial of α_i is

$$f_\alpha(x) = x^3 - 7x^2 - 2x - 7 = (x - \alpha_0)(x - \alpha_1)(x - \alpha_2).$$

For example a "power" basis for $\wp_7$ over Z is $\{7, 2 - \zeta_7 - \zeta_7^6, (2 - \zeta_7 - \zeta_7^6)^2\}$.

Some of previous properties hold more generally.

Theorem 3. *Let K/Q be a tamely ramified cyclic algebraic number field of prime degree l with the conductor $m = p_1.p_2 \ldots p_s$. Let $\Im = \wp_1^{t_1}.\wp_2^{t_2} \ldots \wp_s^{t_s}$ with $0 \leq t_j < l$ for $j = 1, 2, \ldots, s$ be an ideal of Z_K lying over conductor of K and let $\{x_0, x_1, \ldots, x_{n-1}\}$ be a polynomial cycle in $\Im$ for*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_i \in Z,$$

such that $\Im$ is a minimal product of ideals $\wp_j$ which contains x_1. Then $\Im$ is a minimal product of ideals $\wp_j$ which contains x_i for $i = 0, 1, \ldots, n-1$ and m divides a_0.

Proof of Theorem 3. Let $f \in Z[x]$ and $\{x_0, x_1, \ldots, x_{n-1}\}$ be a polynomial cycle for f in an ideal $\Im \subset Z_K$. Then for all $i \in \{0, 1, \ldots, n-1\}$ we have $f(x_i) = x_{i+1}$ where indices are taken *mod* n. Both $x_i, x_{i+1} \in \Im$ and so from

$$x_{i+1} = f(x_i) = a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1 x_i + a_0 \in \Im,$$

it follows that

$$a_0 = x_{i+1} - (a_n x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_1 x_i) \in \Im.$$

Let v_j be a valuation coresponding to the ideal $\wp_j$ for $j = 1, 2, \ldots, s$. We have $v_j(x_1) = t_j$ and $v_j(x_i) \geq t_j$. Hence

$$v_j(a_0) \geq min\{v_j(x_2), v_j(a_n x_1^n), v_j(a_{n-1}x_1^{n-1}), \ldots, v_j(a_1 x_1)\}$$

and so m divides a_0. From this it follows that

$$v_j(a_0) \geq l > t_j.$$

Let $v_j(x_i) > t_j$, then

$$v_j(x_{i+1}) \geq min\{v_j(a_0), v_j(a_n x_i^n), v_j(a_{n-1} x_i^{n-1}), \ldots, v_j(a_1 x_i)\} > t_j.$$

But it is impossible, since $f(x_{n-1}) = x_1$. Theorem 3 is proved.

References

[1] Divišová, Z., On cycles of polynomials with integral rational coefficients, *submitted.*

[2] Halter-Koch, F. and Narkiewicz, W., Scarcity of finite polynomial orbits, *Pub. Math.*, **56, No.3-4** (2000).

[3] Jakubec, S. and Kostra, J., A note on normal bases of ideals, *Math. Slovaca*, **42, No.5** (1992), 677–684.

[4] Jakubec, S. and Kostra, J., On the existence of a normal basis for an ambiguous ideal, *Atti Semin. Mat. Fis. Univ. Modena*, **46, No.1** (1998), 125–129.

[5] Kostra, J., A note on Lenstra constant, polynomial cycles and power basis in prime power cyclotomic fields, *submitted.*

[6] Narkiewicz, W., Polynomial cycles in algebraic number field, *Colloquium Mathematicum*, **58** (1989), 151–155.

[7] Narkiewicz, W., *Polynomial Mappings*, Lecture Notes in Mathematics 1600, Springer-Verlag, 1995.

[8] Ullom, S., Normal basis in Galois extensions of number fields, *Nagoya Math. J.*, **34,** (1969), 153–167.

Juraj Kostra
Department of Mathematics of the Faculty of Sciences
University of Ostrava
30.dubna 22
701 03 Ostrava, Czech Republic

NOTE ON RAMANUJAN SUMS

Aleksander Grytczuk (Zielona Góra, Poland)

Dedicated to the memory of Professor Péter Kiss

Abstract. Let $S=\sum_{1\le a\le q}\left|\sum_{\substack{1\le n\le q\\(n,q)=1}} b_n\exp\left(2\pi i\frac{an}{q}\right)\right|^r$, where $r\ge 1$ is a real number, (b_n) is a sequence of complex numbers. Then we obtain a lower and upper bound for S and moreover, we give an application of the Ramanujan sum to produce some identities given in the formulae $(\star\star)$ and (C).

AMS Classification Number: 11L03

Keywords and phrases: Ramanujan sums, arithmetical functions

1. Introduction

Let $f\colon \mathbf{N}\to\mathbf{C}$ be an arithmetic function and let $f^*=\mu * f$ be the Dirichlet convolution of the Möbius function μ and the function f, i.e. $f^*(n)=\sum_{d|n}\mu(d)f\left(\frac{n}{d}\right)$. Moreover, let $c_q(n)=\sum_{\substack{1\le h\le q\\(h,q)=1}}\exp\left(2\pi i\frac{hn}{q}\right)$ be the Ramanujan sum. Then the series of the form: $\sum_q a_q c_q(n)$, where $a_q=\sum_m \frac{f^*(mq)}{mq}$, are called as Ramanujan series. Important result concerning Ramanujan's expansions of certain arithmetic function has been obtained by Delange [3]. Namely, he proved that, if $\sum_n \frac{2^{\omega(n)}}{n}|f^*(n)|<\infty$ then $\sum_q |a_q c_q(n)|<\infty$ for every positive integer n and $\sum_q a_q c_q(n)=f(n)$. In the proof of this result Delange used of the following inequality:

(D) $$\sum_{d|k}|c_d(n)|\le 2^{\omega(k)}n,$$

where $\omega(n)$ is the number of distinct prime divisors of n. Delange conjectured (see [3]) Lemma, p. 263) that the inequality (D) is the best possible. However, we proved in [4] that for all positive integers k and n the following identity is true

$$(\star) \qquad \sum_{d|k} |c_d(n)| = 2^{\omega\left(\frac{k}{(k,n)}\right)} (k,n)\,,$$

where (k,n) is the greatest common divisor of k and n.

Redmond [10] generalized $(\star)$ for larger class of arithmetic functions and Johnson [7] evaluated the left hand side of $(\star)$ for second variable of the Ramanujan sums. Further investigations connected with $(\star)$ have been given by Johnson [8], Chidambaraswamy and Krishnaiah [2], Redmond [11] and Haukkanen [6]. Some patrial converse to Delange result and an evaluation of the Ramanujan sums defined on the arithmetical semigroups has been given in our paper [5].

In the present note we give further applications of $(\star)$. Namely, we prove the following:

Theorem 1. *Let* $S(k,n) = \sum_{d|k} 2^{\omega\left(\frac{d}{(d,n)}\right)} \mu\left(\frac{k}{d}\right)(d,n)$, *then we have*

$$(\star\star) \qquad S(k,n) = \frac{\varphi(k)}{\varphi\left(\frac{k}{(k,n)}\right)}, \ \textit{if } p^2 \nmid \frac{k}{(k,n)} \textit{ for a prime } p,$$

$$S(k,n) = o \quad \textit{otherwise,}$$

where φ *is the Euler function.*

Now, we denote by S the following sum:

$$(\star\star\star) \qquad S = S_q(b_n, r) = \sum_{1\le a\le q} \left| \sum_{\substack{1\le n\le q\\(n,q)=1}} b_n \exp\left(2\pi i \frac{an}{q}\right) \right|^r,$$

where $r \ge 1$ is a real number and (b_n) is a sequence of complex numbers.

In the paper [1] Bachman proved a very interesting inequality for the sum S defined by $(\star\star\star)$, namely

$$(B) \qquad S \ge (\varphi(q))^{-r} \left(\left|{\sum_n}' b_n\right|\right)^r \sum_{1\le k\le q} |c_q(k)|^r,$$

where ${\sum_n}' b_n$ denotes the summation over all natural numbers n such that $1 \le n \le q$ and $(n,q) = 1$. Using (B) and Hölder inequality we prove the following estimation for the sum S.

Theorem 2. *Let $r \geq 1$ be a real number. Then for any sequence (b_n) of complex numbers we have.*

$$\left(2^{\omega(q)}\left|\sum_{\substack{1\leq n\leq q\\(n,q)=1}} b_n\right|\right)^r q^{1-r} \leq S \leq q\left(\varphi(q)\right)^{r-1}\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|^r. \tag{1}$$

Remark. We note that in general the estimation (1) is the best possible. Indeed, putting in (1) $b_n = i$ for all natural number n, $q = 2^\alpha$ with $\alpha = 1$ and $r = 1$, we get $2 \leq S \leq 2$.

Proof of Theorem 1. In the proof of Theorem 1 we use the following well-known Hölder identity (see, [9]):

$$c_k(n) = \frac{\varphi(k)}{\varphi\left(\frac{k}{(k,n)}\right)}\mu\left(\frac{k}{(k,n)}\right), \tag{HI}$$

where $c_k(n)$ is the Ramanujan sum, φ and μ is the Euler and Möbius function, respectively. Let us denote by

$$F(k) = 2^{\omega\left(\frac{k}{(k,n)}\right)}(k,n). \tag{2}$$

Then, if f and F are given multiplicative arithmetical functions then by Möbius inversion formula we have

$$\sum_{d|k} f(d) = F(k) \text{ if and only if } f(k) = \sum_{d|k}\mu\left(\frac{k}{d}\right)F(d). \tag{3}$$

Using (2) we can represent the identity $(\star)$ in the form:

$$F(k) = \sum_{d|k}|c_d(n)|. \tag{4}$$

Hence, by (4), (3) and $(\star)$ we obtain

$$|c_k(n)| = \sum_{d|k} 2^{\omega\left(\frac{d}{(d,n)}\right)}\mu\left(\frac{k}{d}\right)(d,n). \tag{5}$$

On the other hand by (HI) we have

$$|c_k(n)| = \frac{\varphi(k)}{\varphi\left(\frac{k}{(k,n)}\right)}\left|\mu\left(\frac{k}{(k,n)}\right)\right|. \tag{6}$$

Comparing (5) to (6) we get

$$\sum_{d|k} 2^{\omega\left(\frac{d}{(d,n)}\right)} \mu\left(\frac{k}{d}\right)(d,n) = \frac{\varphi(k)}{\varphi\left(\frac{k}{(k,n)}\right)} \left|\mu\left(\frac{k}{(k,n)}\right)\right|. \tag{7}$$

Now, we remark that by the definition of the Möbius function it follows that, with a prime p if $p^2 \mid \frac{k}{(k,n)}$ then $\left|\mu\left(\frac{k}{(k,n)}\right)\right| = 1$ and $\left|\mu\left(\frac{k}{(k,n)}\right)\right| = 0$ if $p^2 \nmid \frac{k}{(k,n)}$. Hence, the proof of Theorem 1 is complete.

From the Theorem 1 immediately follows the following.

Corollary 1. *Let μ denote the Mbius function and let $\omega(d)$ is the number distinct prime divisors of d. Then we have*

$$S(k) = \sum_{d|k} 2^{\omega(d)} \mu\left(\frac{k}{d}\right) = 1, \text{ if } p^2 \nmid k \text{ and } S(k) = 0, \text{if } p^2 \mid k. \tag{C}$$

Proof of Theorem 2. In the proof of Theorem 2 we use of the following

Lemma 1. *Let $a_k \geq 0$ and $r \geq 1$ be real numbers. Then we have*

$$q^{r-1} \sum_{1\leq k\leq q} a_k^r \geq \left(\sum_{1\leq k\leq q} a_k\right)^r. \tag{8}$$

Proof of Lemma 1. Let $r > 1$ and $a_k \geq 0, b_k \geq 0$ be real numbers and $\frac{1}{r} + \frac{1}{s} = 1$. Then by the well-known Hölder's inequality we have

$$\left(\sum_{1\leq k\leq q} a_k^r\right)^{\frac{1}{r}} \left(\sum_{1\leq k\leq q} b_k^s\right)^{\frac{1}{s}} \geq \sum_{1\leq k\leq q} a_k b_k. \tag{H}$$

Putting in the inequality (H) $b_k = 1$ in virtue of $\frac{1}{s} = 1 - \frac{1}{r}$ we obtain (8). For $r = 1$, (8) follows immediately.

Now, we denote by $a_k = |c_q(k)|$, then from (8) we get

$$q^{r-1} \sum_{1\leq k\leq q} |c_q(k)|^r \geq \left(\sum_{1\leq k\leq q} |c_q(k)|\right)^r. \tag{9}$$

On the other hand we can calculate that

$$\sum_{1\leq k\leq q}|c_q(k)|=2^{\omega(q)}\varphi(q)\,. \tag{10}$$

Hence, by (10) and Bachman's inequality (B), we obtain

$$S\geq\left(2^{\omega(q)}\left|\sum_{\substack{1\leq n\leq q\\(n,q)=1}}b_n\right|\right)^r q^{1-r}. \tag{11}$$

It remains to prove the right hand side of (1). In this purpose denote by

$$S_k^{'}=\left|\sum_{\substack{1\leq n\leq q\\(n,q)=1}}b_n\exp\left(2\pi i\frac{kn}{q}\right)\right|.$$

Then we have

$$S_k^{'}\leq\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|\,, \tag{12}$$

and consequently we obtain

$$\left(S_k^{'}\right)^r\leq\left(\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|\right)^r. \tag{13}$$

In the same way as in Lemma 1 we can deduce the following inequality

$$\left(\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|\right)^r\leq(\varphi(q))^{r-1}\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|^r\,. \tag{14}$$

From (13), (14) and $(\star\star\star)$ we obtain

$$S=\sum_{1\leq k\leq q}\left(S_k^{'}\right)^r\leq\sum_{1\leq k\leq q}(\varphi(q))^{r-1}\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|^r=q\,(\varphi(q))^{r-1}\sum_{\substack{1\leq n\leq q\\(n,q)=1}}|b_n|^r\,, \tag{15}$$

that is the proof of Theorem 2 is complete.

References

[1] Bachman, G., On an optimality property of Ramanujan sums, *Proc. Amer. Math. Soc.* 125, No **4** (1997), 1001–1003.

[2] Chidambaraswamy, J. and Krishnaiah, P. V., An identity for a class of arithmetical functions of two variables, *Internat. J. Math. & Math. Sci.* **11** (1988), 351–354.

[3] Delange, H., On Ramanujan expansions of certain arithmetical functions, *Acta Arith.* **31** (1976), 259–270.

[4] Grytczuk, A., An identity involving Ramanujan's sum, *Elem. Math.* **36** (1981), 16–17.

[5] Grytczuk, A., On Ramanujan sums on arithmetical semigoups, *Tsukuba J. Math.* **16** (1992), 315–319.

[6] Haukkanen, P., An identity for a class of arithmetical functions of several variables, *Internat. J. Math. & Mat. Sci.* **16** (1993), 355–358.

[7] Johnson, K. R., A result for other variable Ramanujan's sum, *Elem. Math.* **38** (1983), 122–124.

[8] Johnson, K. R., Explicit formula for sums of Ramanujan type sums, *Indian J. Pure Appl. Math.* **18** (1987), 675–677.

[9] Knopfmacher, J., *Abstract Analytic Number Theory*, North-Holland Publ., 1975.

[10] Redmond, D., A remark on a paper by A. Grytczuk, *Elem. Math.* **32** (1983), 17–20.

[11] Redmond, D., A generalization of a result of K. R. Johnson, *Tsukuba J. Math.* **13** (1989), 99–105.

Aleksander Grytczuk
Institute of Mathematics
Department of Algebra and Number Theory
University of Zielona Góra
65-069 Zielona Gora, Poland
E-mail: A.Grytczuk@im.uz.zgora.pl

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 47–53*

SECOND ORDER LINEAR RECURRENCES AND PELL'S EQUATIONS OF HIGHER DEGREE

Ferenc Mátyás (Eger, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. In this note solutions are given to an infinite family of Pell's equations of degree $n \geq 2$ based on second order linear recursive sequences of integers.

AMS Classification Number: 11B39

1. Introduction

Let A and B be non-zero integers. The second order linear recursive sequences $R = \{R_n\}_{n=0}^{\infty}$ and $V = \{V_n\}_{n=0}^{\infty}$ are defined by the recursions

(1) $$R_n = AR_{n-1} + BR_{n-2} \quad \text{and} \quad V_n = AV_{n-1} + BV_{n-2},$$

for $n \geq 2$, while $R_0 = 0, R_1 = 1, V_0 = 2$ and $V_1 = A$. If $A = B = 1$ then $R_n = F_n$ and $V_n = L_n$, where F_n and L_n denote the n^{th} Fibonacci and Lucas numbers, respectively.

The polynomial $g(x) = x^2 - Ax - B$ is said to be the characteristic polynomial of the sequences R and V, the complex numbers α and β are the roots of $g(x) = 0$. In this note we suppose that $A^2 + 4B \neq 0$, i.e. $\alpha \neq \beta$. Then, by the well-known Binet formulae, for $n \geq 0$

(2) $$R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n.$$

The classical Pell's equation $x^2 - dy^2 = \pm 1$ ($d \in \mathbf{Z}$) can be rewritten as

$$\det \begin{pmatrix} x & dy \\ y & x \end{pmatrix} = \pm 1.$$

Research supported by the Hungarian OTKA Foundation, No. T 032898.

To generalize this Lin Dazheng [1] investigated the quasi-cyclic matrix

$$\mathbf{C}_n = \mathbf{C}_n(d; x_1, x_2, \ldots, x_n) = \begin{pmatrix} x_1 & dx_n & dx_{n-1} & \ldots & dx_2 \\ x_2 & x_1 & dx_n & \ldots & dx_3 \\ x_3 & x_2 & x_1 & \ldots & dx_4 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_n & x_{n-1} & x_{n-2} & \ldots & x_1 \end{pmatrix}, \tag{3}$$

i.e. every entry of the upper triangular part (not including the main diagonal) of the cyclic matrix of entries $x_1, x_2, \ldots, x_n$ is multiplied by d. The equation

$$\det(\mathbf{C}_n) = \pm 1 \tag{4}$$

is called Pell's equation of degree $n \geq 2$. For example, if $n = 3$ then (4) has the form

$$x_1^3 + dx_2^3 + d^2x_3^3 - 3dx_1x_2x_3 = \pm 1.$$

Lin Dazheng [1] proved that $\det(\mathbf{C}_n(L_n; F_{2n-1}, F_{2n-2}, \ldots, F_n)) = 1$, i.e. if $d = L_n$ then $(x_1, x_2, \ldots, x_n) = (F_{2n-1}, F_{2n-2}, \ldots, F_n)$ is a solution of (4). The aim of this paper is to extend and generalize this result for more general sequences defined by (1) with $A^2 + 4B \neq 0$. In the proofs of our theorems we'll apply the methods and algorithms developed and presented in [1] by Lin Dazheng.

2. Results

Using (1) with $A^2 + 4B \neq 0$ and (3), we can state our results.

Theorem 1. *For $n \geq 2$*

$$\det(\mathbf{C}_n(V_n; R_{2n-1}, R_{2n-2}, \ldots, R_n)) = B^{n(n-1)},$$

i.e. $(x_1, x_2, \ldots, x_n) = (R_{2n-1}, R_{2n-2}, \ldots, R_n)$ is a solution of the generalized Pell's equation of degree n

$$\det(\mathbf{C}_n(V_n; x_1, x_2, \ldots, x_n)) = B^{n(n-1)}.$$

Corollary 1. *For $n \geq 2$*

$$\prod_{k=0}^{n-1} \left(\sum_{j=1}^{n} R_{2n-j} \left(\sqrt[n]{V_n} \right)^{j-1} \varepsilon^{k(j-1)} \right) = B^{n(n-1)},$$

where $\sqrt[n]{V_n}$ denotes a fixed n^{th} complex root of V_n and $\varepsilon = e^{2\pi i/n}$.

It is known from [3] that the inverse of a quasi-cyclic matrix is quasi-cyclic. In our case we can prove the following result, too.

Theorem 2. *For $n \geq 3$ the matrix $\mathbf{C}_n\left(V_n; R_{2n-1}, R_{2n-2}, \ldots, R_n\right)$ is invertible and its inverse matrix $\mathbf{C}_n^{-1}$ is as follows:*

$$\mathbf{C}_n^{-1}\left(V_n; R_{2n-1}, R_{2n-2}, \ldots, R_n\right) = (-1)^{n-1} B^{-n} (B\mathbf{I}_n + A\mathbf{E}_n - \mathbf{E}_n^2),$$

where $\mathbf{I}_n$ and $\mathbf{E}_n$ denotes the identity matrix of order n and the n by n matrix

$$\mathbf{E}_n = \begin{pmatrix} 0 & 0 & \ldots & 0 & V_n \\ 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \end{pmatrix}, \tag{5}$$

respectively.

Remark. Naturally, if $|B| \neq 1$ then the entries of the matrix

$$\mathbf{C}_n^{-1}\left(V_n; R_{2n-1}, R_{2n-2}, \ldots, R_n\right)$$

are not integers.

Corollary 2.

$$(x_1, x_2, \ldots, x_n) = \begin{cases} (1, A, -1, 0, \ldots, 0), & \text{if } n \geq 3 \text{ odd and } B = 1, \\ (1, -A, 1, 0, \ldots, 0), & \text{if } n \geq 3 \text{ odd and } B = -1, \\ (-1, -A, 1, 0, \ldots, 0), & \text{if } n \geq 4 \text{ even and } B = 1, \\ (1, -A, 1, 0, \ldots, 0), & \text{if } n \geq 4 \text{ even and } B = -1 \end{cases}$$

is an other solution of the generalized Pell's equation

$$\det\left(\mathbf{C}_n\left(V_n; x_1, x_2, \ldots, x_n\right)\right) = 1. \tag{6}$$

3. Proofs

To prove our theorems we need the following

Lemma. *Let the sequences R and V be defined by (1) and we suppose that $\alpha \neq \beta$ in (2). Then*

$$R_{n+1}R_{n-1} - R_n^2 = (-1)^n B^{n-1} \quad (n \geq 1), \tag{7/1}$$

(7/2) $$R_nV_n = R_{2n} \quad (n \geq 0),$$

(7/3) $$V_nR_{n+1} = R_{2n+1} + (-B)^n \quad (n \geq 0),$$

(7/4) $$\mathbf{E}_n^n = V_n\mathbf{I}_n \quad \textit{and} \quad \mathbf{E}_n^{n+1} = V_n\mathbf{E}_n \quad (n \geq 3),$$

where $\mathbf{E}_n$ *is defined by (5).*

Proof. The first three properties of the Lemma are known or, using (2), they can be proven easily. For the proof of (7/4) consider the multiplication of matrices. For example:

$$\mathbf{E}_n^2 = \mathbf{E}_n \cdot \mathbf{E}_n = \begin{pmatrix} 0 & 0 & \dots & 0 & V_n & 0 \\ 0 & 0 & \dots & 0 & 0 & V_n \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 \end{pmatrix},$$

$$\mathbf{E}_n^3 = \mathbf{E}_n^2 \cdot \mathbf{E}_n = \begin{pmatrix} 0 & 0 & \dots & 0 & V_n & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 & V_n & 0 \\ 0 & 0 & \dots & 0 & 0 & 0 & V_n \\ 1 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 & 0 & 0 \end{pmatrix}, \dots,$$

$$\mathbf{E}_n^n = \begin{pmatrix} V_n & 0 & \dots & 0 & 0 \\ 0 & V_n & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & V_n & 0 \\ 0 & 0 & \dots & 0 & V_n \end{pmatrix} = V_n\mathbf{I}_n$$

and so $\mathbf{E}_n^{n+1} = \mathbf{E}_n^n \cdot \mathbf{E}_n = (V_n\mathbf{I}_n)\,\mathbf{E}_n = V_n\mathbf{E}_n$.

Proof of Theorem 1. For $n = 2$ we get that

$$\det\left(\mathbf{C}_2(V_2; R_3, R_2)\right) = \begin{vmatrix} A^2 + B & A^3 + 2AB \\ A & A^2 + B \end{vmatrix} = B^2.$$

If $n > 2$, let us consider the n by n matrices

$$\mathbf{T}_n = \begin{pmatrix} 1 & -A & -B & 0 & \dots & 0 & 0 \\ 0 & 1 & -A & -B & \dots & 0 & 0 \\ 0 & 0 & 1 & -A & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & -A & -B \\ 0 & 0 & 0 & 0 & \dots & 1 & -A \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

and

$$\mathbf{C}_n = \mathbf{C}_n(V_n, R_{2n-1}, R_{2n-2}, \dots, R_n) = \begin{pmatrix} R_{2n-1} & V_nR_n & \dots & V_nR_{2n-2} \\ R_{2n-2} & R_{2n-1} & \dots & V_nR_{2n-3} \\ \vdots & \vdots & \ddots & \vdots \\ R_n & R_{n+1} & \dots & R_{2n-1} \end{pmatrix}.$$

Then, by (1), (2) and (7/1)–(7/3), one can verify that

$$\mathbf{C}_n\mathbf{T}_n = \begin{pmatrix} R_{2n-1} & BR_{2n-2} & (-B)^n & 0 & \dots & 0 \\ R_{2n-2} & BR_{2n-3} & 0 & (-B)^n & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ R_{n+2} & BR_{n+1} & 0 & 0 & \dots & (-B)^n \\ R_{n+1} & BR_n & 0 & 0 & \dots & 0 \\ R_n & BR_{n-1} & 0 & 0 & \dots & 0 \end{pmatrix}.$$

Developing the $\det(\mathbf{C}_n\mathbf{T}_n)$ we get that

$$\begin{aligned} \det(\mathbf{C}_n\mathbf{T}_n) &= (-1)^{2n+2}\det\begin{pmatrix} R_{n+1} & BR_n \\ R_n & BR_{n-1} \end{pmatrix}\det\left((-B)^n\mathbf{I}_{n-2}\right) \\ &= B(R_{n+1}R_{n-1} - R_n^2)(-B)^{n(n-2)} = B(-1)^nB^{n-1}(-B)^{n(n-2)} \\ &= (-1)^{n(n-1)}B^{n(n-1)} = B^{n(n-1)}. \end{aligned}$$

But, since $\det(\mathbf{T}_n) = 1$, $\det(\mathbf{C}_n\mathbf{T}_n) = \det(\mathbf{C}_n)\cdot\det(\mathbf{T}_n) = \det(\mathbf{C}_n)$, therefore $\det(\mathbf{C}_n) = B^{n(n-1)}$, i.e. Theorem 1 is true.

Proof of Corollary 1. In [2] it is proven that if $\mathbf{C}_n$ is as in (3) then

$$\det\left(\mathbf{C}_n(d, x_1, x_2, \dots, x_n)\right) = \prod_{k=0}^{n-1}\left(\sum_{j=1}^{n} x_j\left(\sqrt[n]{d}\right)^{j-1}\varepsilon^{k(j-1)}\right), \tag{8}$$

where $\varepsilon = e^{2\pi i/n}$. Substituting in (8)

$$d = V_n \quad \text{and} \quad (x_1, x_2, \dots, x_n) = (R_{2n-1}, R_{2n-2}, \dots, R_n),$$

by Theorem 1, the statement of Corollary 1 immediately yields.

Proof of Theorem 2. Theorem 1 implies that $\mathbf{C}_n^{-1}(V_n; R_{2n-1}, R_{2n-2}, \dots, R_n)$ exists. It is easily verifyable that

$$\mathbf{C}_n(V_n; R_{2n-1}, R_{2n-2}, \dots, R_n) = R_{2n-1}\mathbf{I}_n + R_{2n-2}\mathbf{E}_n + \dots + R_n\mathbf{E}_n^{n-1},$$

therefore we have to show that

$$(9)\quad \left(R_{2n-1}\mathbf{I}_n + R_{2n-2}\mathbf{E}_n + \dots + R_n\mathbf{E}_n^{n-1}\right)(-1)^{n-1}B^{-n}(B\mathbf{I}_n + A\mathbf{E}_n - \mathbf{E}_n^2) = \mathbf{I}_n.$$

By (1), the left hand side of (9) can be written as

$$(10)\qquad (-1)^{n-1}B^{-n}\big(R_{2n-1}B\mathbf{I}_n + R_{2n-2}B\mathbf{E}_n + R_{2n-1}A\mathbf{E}_n + R_nA\mathbf{E}_n^n$$
$$-R_{n+1}\mathbf{E}_n^n - R_n\mathbf{E}_n^{n+1} + \mathbf{O}_n + \dots + \mathbf{O}_n\big),$$

where $\mathbf{O}_n$ is the zero-matrix of order n.
Thus, applying (1), (7/1)–(7/4) and (2), the form (10) is equal to

$$\begin{aligned}
&(-1)^{n-1}B^{-n}\left(R_{2n-1}B\mathbf{I}_n + (BR_{2n-2} + AR_{2n-1})\,\mathbf{E}_n\right.\\
&\left.+ R_nAV_n\mathbf{I}_n - R_{n+1}V_n\mathbf{I}_n - R_nV_n\mathbf{E}_n\right)\\
&= (-1)^{n-1}B^{-n}\left(R_{2n-1}B\mathbf{I}_n + (R_{2n} - R_nV_n)\,\mathbf{E}_n + V_n(AR_n - R_{n+1})\mathbf{I}_n\right)\\
&= (-1)^{n-1}B^{-n}\left(R_{2n-1}B\mathbf{I}_n + \mathbf{O}_n - V_nBR_{n-1}\mathbf{I}_n\right)\\
&= (-1)^{n-1}B^{-n+1}\left(R_{2n-1} - V_nR_{n-1}\right)\mathbf{I}_n\\
&= (-1)^{n-1}B^{-n+1}(-B)^{n-1}\mathbf{I}_n = (-1)^{2n-2}B^0\mathbf{I}_n = \mathbf{I}_n,
\end{aligned}$$

which completes the proof of Theorem 2.

Proof of Corollary 2. By Theorem 2

$$\det\left(\mathbf{C}_n(V_n; R_{2n-1}, R_{2n-2}, \dots, R_n)\right) \cdot \det\left(\mathbf{C}_n^{-1}(V_n; R_{2n-1}, R_{2n-2}, \dots, R_n)\right) = 1$$

thus, if $|B| = 1$ then, by Theorem 1,

$$\det\left(\mathbf{C}_n^{-1}(V_n; R_{2n-1}, R_{2n-2}, \dots, R_n)\right) = 1.$$

E.g. let $n \geq 3$ be an odd integer and $B = 1$. Then, by Theorem 2,

$$\mathbf{C}_n^{-1}(V_n; R_{2n-1}, R_{2n-2}, \dots, R_n) = \mathbf{I}_n + A\mathbf{E}_n - \mathbf{E}_n^2$$
$$= \begin{pmatrix} 1 & 0 & 0 & \dots & 0 & -V_n & AV_n \\ A & 1 & 0 & \dots & 0 & 0 & -V_n \\ -1 & A & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & -1 & A & 1 \end{pmatrix},$$

i.e. $(x_1, x_2, \dots, x_n) = (1, A, -1, 0, \dots, 0)$ is a solution of (6).

The proof is similar when $n \geq 3$ odd and $B = -1$, or $n \geq 4$ even and $|B| = 1$.

References

[1] Lin Dazheng, Fibonacci–Lucas Quasi-Cyclic Matrices, *The Fibonacci Quarterly* **40.2** (2002), 280–286.

[2] Shen Guangxing, On Eigenvalues of Some Cyclic Matrices, *Math. Application* **4.3** (1991), 76–82.

[3] Tang Taiming and Lin Dazheng, Diophantine Approximation, Circulant Matrix and Pell Equation, *J. Shaansi Normal Univ. (Natural Science Ed.)*, **28.14** (2000), 6–11.

Ferenc Mátyás
Department of Mathematics
Károly Eszterházy College
H-3301, Eger, P. O. Box 43.
Hungary
E-mail: matyas@ektf.hu

On a special interpolation problem of functional B-spline curves

Miklós Hoffmann (Eger, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. A multistep interpolation method is presented in this paper by which one can compute a planar functional B-spline curve from its gradient function with special endconditions. The method is applied in turbine blade section curve design where the curve consists of two interpolating B-spline arcs connecting two predefined circular arcs.

AMS Classification Number: 68U05

1.Introduction and problem statement

Interpolation or approximation of a set of data by B-spline curves is a well-studied area of computer aided design and manufacture. One can find numerous methods solving the problem for different types of data, see e.g. [3] and references therein. All of these classical methods, however, require direct geometrical data (points and/or tangent lines) of the curve.

In the problem presented here, the curve has to be created from the *angles* of its tangent lines, while the exact position of the curve is determined by endpoints and tangential information in them. A special, multistep method will be described in the following section to solve this problem. Application of this method for turbine blade section curve design can be found in Section 3. Finally conclusion and directions of future research close the paper.

To clarify the notations here we present the definition of the B-spline curve.

Definition. The curve $\mathbf{s}(u)$ defined by

$$\mathbf{s}(u) = \sum_{l=0}^{n} N_l^k(u)\mathbf{d}_l, \quad u \in [u_{k-1}, u_{n+1}]$$

is called B-spline curve of order k (degree $k-1$), where $N_l^k(u)$ is the l^{th} normalized B-spline basis function, for the evaluation of which the knots $u_0, u_1, \ldots, u_{n+k}$ are

This research was sponsored by the Hungarian Scientific Research Foundation (OTKA No. F032679), the Hungarian Ministry of Education (FKFP No.0027/2001) and the European Research Training Network MINGLE (HPRN-1999-00117).

necessary. The points $\mathbf{d}_l$ are called control points, while the polygon formed by these points is called control polygon.

The turbine blade section curve (or simply profile curve) consists of two circular arcs and two B-spline arcs connecting them. In profile curve design the connecting B-spline curves are smooth, almost linear pieces along the x direction, hence throughout this paper one can consider them as functions of x, which is certainly not the general case.

2. Multistep interpolation

Let a continuously differentiable real function $\alpha = f(x), x \in [a, b]$ be given. We would like to create an arc (function) over $[a, b]$ with the following property: at every $x_0 \in [a, b]$ the angle of the x axis and the tangent line of the arc at this point is $\alpha_0 = f(x_0)$. Thus the function $\alpha = f(x)$ can be considered as the gradient function of the arc we are looking for. Moreover, the arcs have to be defined as a B-spline curves, because this type of curves is the standard description method in CAGD. Thus let this arc be denoted by $\mathbf{s}(u), u \in [a, b]$.

At first a sample set of pairs $(x_i, \alpha_i), i = 1, ..., n$ is chosen, where n depends on the desired error bound. The x_i-s can be uniformly distributed over $[a, b]$. We will create a cubic B-spline curve $\mathbf{s}(u)$ in a way that at every point of the curve cooresponding to the coordinate values x_i the angle between the tangent line of the curve and the x axis is α_i. Denote these corresponding points of the curve by $\mathbf{q}_i(x_i, y_i)$. Thus

$$\mathbf{s}(u_i) = \mathbf{q}_i(x_i, y_i), \quad i = 1, ..., n \tag{1}$$

where the parameters u_i and the coordinates y_i are the unknowns. Let $\mathbf{e}_i(\cos\alpha_i, \sin\alpha_i)$ denote the unit vector at the direction of the i^{th} tangent line. This yields the equations

$$\dot{\mathbf{s}}(u_i) = \lambda_i \mathbf{e}_i, \quad i = 1, ..., n \tag{2}$$

where the values λ_i are unknowns.

Denote the coordinates of the future control points $\mathbf{d_j}$ by $(x_j^{\mathbf{d}}, y_j^{\mathbf{d}}), j = 1, ..., n$ and the coordinate functions of the B-spline curve by $\mathbf{s}(u) = (x^{\mathbf{s}}(u), y^{\mathbf{s}}(u))$. Note, that the number of control points is the same as the number of samples. Thus from (1) and (2) we obtain the following system of equations:

$$\begin{aligned} x^{\mathbf{s}}(u_i) &= x_i, \\ \dot{x}^{\mathbf{s}}(u_i) &= \lambda_i \cos\alpha_i, \qquad i = 1, ..., n. \\ \dot{y}^{\mathbf{s}}(u_i) &= \lambda_i \sin\alpha_i, \end{aligned}$$

By the definition of the B-spline curve this system can be written as

$$
\begin{aligned}
\sum_{j=0}^{n} N_j^4(u_i)x_j^{\mathbf{d}} &= x_i, \\
\sum_{j=0}^{n} \dot{N}_j^4(u_i)x_j^{\mathbf{d}} &= \lambda_i \cos\alpha_i, \qquad i = 1, ..., n. \\
\sum_{j=0}^{n} \dot{N}_j^4(u_i)y_j^{\mathbf{d}} &= \lambda_i \sin\alpha_i,
\end{aligned} \tag{3}
$$

Here each row represents n equations and all subsystems are linear. If we fix the parameter values u_i then we can compute the B-spline basis functions $N_j^4(u_i)$ and their derivatives $\dot{N}_j^4(u_i)$. There are several methods for the choice of u_i (uniform, cumulative chord length, centripetal model, c.f. [1]), but our future curve is quite simple, smooth, and the samples x_i are uniformly distributed, thus we can apply the uniform model as

$$u_i = \frac{i-1}{n-1}.$$

Now the first subsystem of (3) —containing the first n equations— can be solved for $x_j^{\mathbf{d}}$, then the second subsystem for λ_i, finally the third n equations for $y_j^{\mathbf{d}}$. The first and the third systems of equations have a banded matrix where the bandwidth is 4, while the solution of the second one is even more straightforward, containing one unknown per equation. After this process we will obtain the control points $\mathbf{d_j}$ $(x_i^{\mathbf{d}}, y_i^{\mathbf{d}})$, with the help of which one can compute the desired B-spline curve. In case of non-uniform curve the knot vector can be the same as the sequence of the parameter values.

2. An application: turbine blade section curve design

The design process of turbine blades generally contains several steps. At first designers create planar curves which will serve as section curves of the future surface. A typical section curve can be seen in Fig.1.

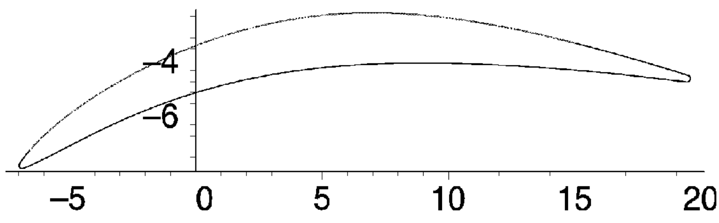

Figure 1

Focusing on this problem a designer may prefer the following scenario: he can define two circular arcs by their centres, radii and endpoints. The system connects them by two B-spline arcs which can be modified by direct manipulation of their predefined gradient functions. The gradient functions, of course, always satisfy the endconditions defined by the circular arcs.

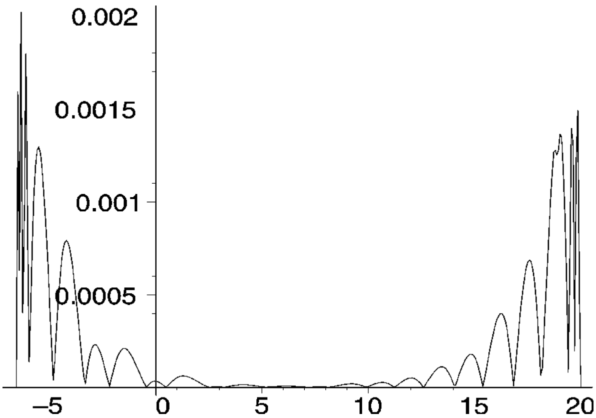

Figure 2

These two B-spline arcs can be calculated by the interpolation methods described in the previous section. To estimate the correctness of this technique we considered an arc of an existing section curve and picked 350 points of them as samples.

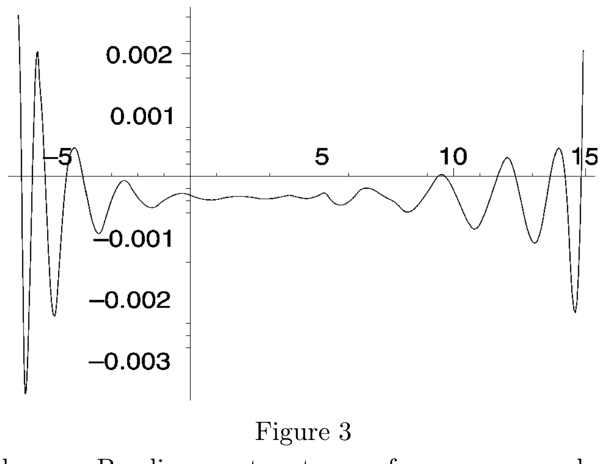

Figure 3

Creating the new B-spline arc two types of error measured at these sample points: the distance of the two curve and the difference between the tangential angles of the two curve. The distance is measured by the following way: at each sample point **p** of the original curve a perpendicular straight line is dropped. This line intersects the computed B-spline curve at $\hat{\mathbf{p}}$ and the error at this point is defined as the length of $\hat{\mathbf{p}}\mathbf{p}$. The graph of this error function (connecting the discrete points for better visualization) can be seen in Fig.2.

The other type of error is measured by the difference between the angles of the tangent lines of the original and the computed curve at the sample points. This graph can be seen in Fig.3.

4. Conclusion

A special interpolation method has been presented in this paper with the help of which one can create and modify a planar B-spline curve based on its gradient function. Using this method a turbine blade section curve design technique has been developed: two circular arcs are defined which are connected by B-spline arcs computed by the new method.

References

[1] Ma, W., Kruth, J. P., Parametrization of randomly measured points for least squares fitting of B-spline curves and surfaces, *Computer-Aided Design*, **27**, 663–675 (1995).

[2] Lee, E. T., Choosing nodes in parametric curve interpolation, *Computer-Aided Design*, **21**, 363–370, (1989).

[3] Piegl, L., Tiller, W., *The NURBS book*, Springer-Verlag, (1995).

Miklós Hoffmann
Department of Mathematics
Károly Eszterházy College
H-3301 Eger, P. O. Box 43.
Hungary
E-mail: hofi@ektf.hu

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 61–66*

ON TRANSFORMATION MATRICES CONNECTED TO NORMAL BASES IN CUBIC FIELDS

Z. Divišová, J. Kostra, M. Pomp (Ostrava, Czech Republic)

Dedicated to the memory of Professor Péter Kiss

Abstract. In the paper it is proved that special class of circulant matrices transforming normal bases of orders in cubic fields to normal bases of their suborders consists of matrices of the type $\mathrm{circ}_3(a_1,a_2,a_3)$ where $a_1+a_2+a_3=\pm 1$ and one of the equalities $a_1=a_2$, $a_1=a_3$, $a_2=a_3$ holds.

AMS Classification Number: 11R16, 11C20

1. Introduction

Let K be a cyclic algebraic number field of degree n over the rational numbers $\mathbb{Q}$. Such a field has a normal basis over the rationals $\mathbb{Q}$ i.e. a basis consisting of all conjugations of one element. Transformation matrices between two normal bases of K over $\mathbb{Q}$ are exactly regular rational circulant matrices of degree n. In the paper [4], the special class of circulant matrices with integral rational elements is characterized by the following proposition.

Proposition 1. *Let K be a cyclic algebraic number field of degree n over rational numbers. Let*

$$\mathbf{A} = \mathrm{circ}_n(a_1, a_2, \ldots, a_n)$$

be a circulant matrix and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. By A_i, $i = 1, 2, \ldots n$ we denote the algebraic complement of element a_i in the matrix $\mathbf{A}$. Let

$$a_1 + a_2 + \cdots + a_n = \pm 1$$

and

$$a_i \equiv a_j \pmod{h}$$

for $i, j \in \{1, 2, \ldots, n\}$, where

$$h = \frac{\det \mathbf{A}}{\gcd(A_1, A_2, \ldots, A_n)}\,.$$

This research was supported by GA of the Czech Academy of Sciences Grant A1187101/01.

Then the matrix $\mathbf{A}$ *transforms a normal basis of an order* B *of the field* K *to a normal basis of an order* C *of the field* K*, where* $C \subseteq B$*.*

2. Results

Theorem 1. *Let* $\mathbf{A}$ *be a circulant matrix* $\mathbf{A} = \mathrm{circ}_3(a_1, a_2, a_3)$, $a_i \in \mathbb{Z}$*, where*

$$a_1 + a_2 + a_3 = \pm 1.$$

Then the following conditions are equivalent

(1) $a_i \equiv a_j \pmod{h}$ *for* $i, j \in \{1, 2, 3\}$*, where*

$$h = \frac{\det \mathbf{A}}{\gcd(A_1, A_2, A_3)}\,,$$

where A_i *is algebraic complement of element* a_i *in the matrix* $\mathbf{A}$ *for every* $i \in \{1, 2, 3\}$*.*

(2) *One of the next equalities holds*

$$a_1 = a_2 \quad \mathit{or} \quad a_2 = a_3 \quad \mathit{or} \quad a_1 = a_3\,.$$

Proof. (1) $\Rightarrow$ (2) Let $\mathbf{A} = \mathrm{circ}_3(a_1, a_2, a_3)$ be a circulant matrix fulfilling assumptions of our theorem. If $a_1 + a_2 + a_3 = 1$, we can write

$$\mathbf{A} = (1 - a_2 - a_3, a_2, a_3)\,.$$

Determinant of the matrix $\mathbf{A}$ is

$$\begin{aligned} \det \mathbf{A} &= 1 + 3a_2^2 + 3a_3^2 - 3a_2 - 3a_3 + 3a_2 a_3 \\ &= (1 - 3a_2)(1 - 3a_3) + 3(a_2 - a_3)^2 \end{aligned} \tag{1}$$

and the subdeterminants are

$$\begin{aligned} A_1 &= 1 + a_2^2 + a_3^2 - 2a_2 - 2a_3 + a_2 a_3\,, \\ A_2 &= a_2^2 + a_3^2 + a_2 a_3 - a_3\,, \\ A_3 &= a_2^2 + a_3^2 + a_2 a_3 - a_2\,. \end{aligned}$$

Their greatest common divisor is

$$\begin{aligned}
&\gcd(A_1, A_2, A_3) = \gcd(A_1 - A_2, A_2, A_3 - A_2)\\
&= \gcd(1 - 2a_2 - a_3, a_2^2 + a_3^2 + a_2a_3 - a_3, a_3 - a_2)\\
&= \gcd\big(1 - 2a_2 - a_3 + (a_3 - a_2), a_2^2 + a_3^2 + a_2a_3 - a_3 + (a_2 + 2a_3)(a_3 - a_2), a_3 - a_2\big)\\
&= \gcd(1 - 3a_2, -a_3 + 3a_3^2, a_3 - a_2)\\
&= \gcd\big(1 - 3a_2, -a_3(1 - 3a_3), a_3 - a_2\big).
\end{aligned}$$

In regards with (1) we obtain that $\gcd(A_1, A_2, A_3)^2$ is a divisor of $\det \mathbf{A}$. Now we need to prove that $\det \mathbf{A}$ is a divisor of $\gcd(A_1, A_2, A_3)^2$.

Because of $a_i \equiv a_j \pmod{h}$ for $i, j \in \{1, 2, 3\}$, we obtain the congruences

$$\begin{aligned}
a_3 - a_2 &\equiv 0 \pmod{h},\\
1 - 3a_2 &\equiv 0 \pmod{h},\\
1 - 3a_3 &\equiv 0 \pmod{h}.
\end{aligned} \tag{2}$$

Then h is a divisor of $\gcd(A_1, A_2, A_3)$,

$$\begin{aligned}
\gcd(A_1, A_2, A_3) &= kh = k\frac{\det \mathbf{A}}{\gcd(A_1, A_2, A_3)}\,,\\
\gcd(A_1, A_2, A_3)^2 &= k \det \mathbf{A}\,,
\end{aligned}$$

and $\det \mathbf{A}$ is a divisor of $\gcd(A_1, A_2, A_3)^2$. Therefore

$$\det \mathbf{A} = \pm\gcd(A_1, A_2, A_3)^2$$

and

$$h = \gcd(A_1, A_2, A_3)\,.$$

In regards of (2) we denote

$$hX = 1 - 3a_2\,, \quad hY = 1 - 3a_3\,, \quad hZ = a_2 - a_3\,,$$

then

$$\det \mathbf{A} = h^2XY + 3h^2Z^2\,.$$

We obtain the equation $XY + 3Z^2 = \pm 1$. Assumption $a_1 + a_2 + a_3 = 1$ yields the equation $hX + 3hZ = hY$.

(a) Let $\det \mathbf{A} = -h^2$. From the system of equations

$$\begin{aligned}
XY + 3Z^2 &= -1\,,\\
X + 3Z &= Y\,,
\end{aligned}$$

we obtain the quadratic equation in Z

$$3Z^2 - 3ZY + (Y^2 + 1) = 0$$

which has a negative discriminant, so there is no integral solution.

(b) Let $\det \mathbf{A} = h^2$. We obtain a system of equations

$$\begin{aligned} XY + 3Z^2 &= 1\,, \\ X + 3Z &= Y\,. \end{aligned}$$

From the integral solutions of this system it follows that
(a) $X = 1$, $Y = 1$, $Z = 0$ or $X = -1$, $Y = -1$, $Z = 0$ then $a_2 = a_3$,
(b) $X = 1$, $Y = -2$, $Z = -1$ or $X = -1$, $Y = 2$, $Z = 1$ then $a_1 = a_2$,
(c) $X = 2$, $Y = -1$, $Z = -1$ or $X = -2$, $Y = 1$, $Z = 1$ then $a_1 = a_3$.
The case $a_1 + a_2 + a_3 = -1$ can be proved similarly.

(2) $\Rightarrow$ (1) Without loss of generality it is sufficient to suppose that $a_2 = a_3$, so we can denote the matrix $\mathbf{A} = \mathrm{circ}_3(a, b, b)$. The algebraic complements are $A_1 = (a-b)(a+b)$, $A_2 = A_3 = b(b-a)$ so the $\gcd(A_1, A_2, A_3) = (b-a)\gcd(b, a+b)$. From the fact that $a + 2b = \pm 1$ it follows $\gcd(a, b) = 1$ and so $\gcd(b, a + b) = 1$. Hence $h = (b-a)^2/(b-a) = b-a$ and because $b \equiv a \pmod{b-a}$, the condition (1) holds.

Corollary 1. *Let K be a cyclic algebraic number field of degree 3 over $\mathbb{Q}$. Let the matrix $\mathbf{A} = \mathrm{circ}_3(a, b, b)$ satisfy assumptions of Theorem 1 and transform a normal basis of the order B to a normal basis $(\gamma_1, \gamma_2, \gamma_3)$ of the order C, where $C \subseteq B$. Then any polynomial cycle of $f \in \mathbb{Z}[X]$ contains at most one of the elements $\gamma_1, \gamma_2, \gamma_3$.*

Proof. From [3, Theorem 1] it follows that if a number γ_i ($i = \{1, 2, 3\}$) does not generate the power basis of order C, then two of elements $\gamma_1, \gamma_2, \gamma_3$ cannot be in the same polynomial cycle for a polynomial with rational integral coefficients. So it is sufficient to prove that γ_i (for example γ_1) does not generate a power basis of C.

Let $(\beta_1, \beta_2, \beta_3)$ be a normal basis of an order B. Let matrix $\mathbf{A} = \mathrm{circ}_3(a, b, b)$ satisfy the assumption of Theorem 1. Then the matrix $\mathbf{A}$ transforms the basis $(\beta_1, \beta_2, \beta_3)$ to the basis $(\gamma_1, \gamma_2, \gamma_3)$, where

$$(\gamma_1, \gamma_2, \gamma_3) = (\beta_1, \beta_2, \beta_3)\mathbf{A}^{\mathrm{T}}\,.$$

Because the basis $(\beta_1, \beta_2, \beta_3)$ is a normal basis of an order, thus

$$\beta_1 + \beta_2 + \beta_3 = \pm 1$$

holds, and

$$\gamma_1 = a\beta_1 + b(\beta_2+\beta_3) = a\beta_1 + b(\pm 1 - \beta_1) = (a-b)\beta_1 \pm b\,.$$

Elements γ_2 and γ_3 can be composed similarly, and we obtain the basis $(\gamma_1,\gamma_2,\gamma_3)$ in the form

$$\begin{aligned}\gamma_1 &= (a-b)\beta_1 \pm b\,,\\ \gamma_2 &= (a-b)\beta_2 \pm b\,,\\ \gamma_3 &= (a-b)\beta_3 \pm b\,.\end{aligned}$$

We consider the basis $(1,\gamma_1,\gamma_1^2)$, where

$$\gamma_1^2 = (a-b)^2\beta_1^2 \pm 2b(a-b)\beta_1 + b^2$$

the basis $(\beta_1,\beta_2,\beta_3)$ is an integral basis, therefore there exist $b_1,b_2,b_3\in\mathbb{Z}$ such that

$$\begin{aligned}\gamma_1^2 &= (a-b)^2(b_1\beta_1+b_2\beta_2+b_3\beta_3) \pm 2b(a-b)\beta_1 + b^2\\ &= \big((a-b)b_1 \pm 2b\big)(a-b)\beta_1 + (a-b)^2b_2\beta_2 + (a-b)^2b_3\beta_3 + b^2\,.\end{aligned}$$

Let

$$\begin{aligned}s_1 &= (a-b)b_1 \pm 2b\,,\\ s_2 &= (a-b)b_2\,,\\ s_3 &= (a-b)b_3\,.\end{aligned}$$

Then

$$\begin{aligned}&\gamma_1^2 = s_1(a-b)\beta_1 + s_2(a-b)\beta_2 + s_3(a-b)\beta_3 + b^2\\ &= s_1\big((a-b)\beta_1 \pm b\big) + s_2\big((a-b)\beta_2 \pm b\big) + s_3\big((a-b)\beta_3 \pm b\big) + b^2 \mp (s_1+s_2+s_3)b\\ &= s_1\gamma_1 + s_2\gamma_2 + s_3\gamma_3 + b^2 \mp (s_1+s_2+s_3)b\end{aligned}$$

Because $\gamma_1+\gamma_2+\gamma_3=\pm 1$, we can write

$$b^2 \mp (s_1+s_2+s_3)b = r(\gamma_1+\gamma_2+\gamma_3)\,,$$

so

$$\gamma_1^2 = (s_1+r)\gamma_1 + (s_2+r)\gamma_2 + (s_3+r)\gamma_3\,.$$

Suppose that $(\gamma_1,\gamma_2,\gamma_3)$ and $(1,\gamma_1,\gamma_1^2)$ are bases of the order C over $\mathbb{Z}$. Then the matrix $\mathbf{C}$ transforming the basis $(\gamma_1,\gamma_2,\gamma_3)$ to the basis $(1,\gamma_1,\gamma_1^2)$ has determinant equals ± 1. But

$$\det\mathbf{C} = \pm\begin{vmatrix}1 & 1 & s_1+r\\ 1 & 0 & s_2+r\\ 1 & 0 & s_3+r\end{vmatrix} = \pm(s_2-s_3) = \pm(a-b)(b_2-b_3)$$

where $a, b, b_2, b_3 \in \mathbb{Z}$, which is a contradiction to $a \equiv b \pmod{h}$, where $h \neq \pm 1$.

References

[1] Borevich, Z. I. and Shafarevich, I. R., *Number theory*, Nauka, Moscow, 1985, 3^{rd} ed., (in Russian).

[2] Davis, P. J., *Circulant matrices*, A. Wiley-Interscience publisher, John Wiley and Sons, New York–Chichester–Brisbane–Toronto, 1979.

[3] Divišová, Z., On cycles of polynomials with integral rational coefficients, *Mathematica Slovaca*, to appear.

[4] Kostra, J., Orders with a normal basis, *Czechoslovak Math. Journal* **35** 110, 1985.

Z. Divišová
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: zuzana.divisova@osu.cz

J. Kostra
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: juraj.kostra@osu.cz

M. Pomp
Department of Mathematics
University of Ostrava
30. dubna 22
Ostrava, Czech Republic
E-mail: marek.pomp@osu.cz

USING COMPUTER TO DISCOVER SOME THEOREMS IN GEOMETRY

Jaroslav Hora & Pavel Pech (Plzeň & Č. Budějovice, Czech Rep.)

Dedicated to the memory of Professor Péter Kiss

Abstract. By means of Buchberger's algorithm for computing Groebner bases of ideals some theorems from elementary geometry are proved. Besides the well-known formula of Heron for the calculation of the area of a triangle analogical formulas and relations for planar quadrangles are derived. It is shown that with the help of a common software (Maple, Mathematica) formulas from elementary geometry can be proved and even discovered.

Keywords: Groebner basis, ideals, polygons

1. Introduction

It is likely known that after the year 1960 Buchberger and Hironaka discovered a new algorithm for solving a system of algebraic equations. A great interest in this area of mathematics and a general using computers and mathematical software, which makes possible not only numerical computation but computations with symbols, caused big changes in commutative algebra and algebraic geometry. Nowadays is so called Buchberger's algorithm for computing of a Groebner basis of an ideal implemented even in some calculators (models TI 89 or TI 92).

Example. Solve the system of equations

$$\begin{aligned} x^2+y^2+z^2&=6,\\ x^3+y^3+z^3-xyz&=-4,\\ xy+xz+yz&=-3. \end{aligned} \tag{1}$$

Solution. First we shall "prove" that even calculators mentioned above are able to solve such a quite difficult system of equations. Calculators mentioned above are equipped with the command 4: `solve(and,(x,y))` for solving system of equations. We write

`solve(x^2 + y^2 + z^2 = 6 and x^3 + y^3 + z^3 − xyz = −4 and`
`xy + xz + yz = −3, {x, y, z})`

This research is partially supported by the Grant Project MSM 124100006.

and in a while the result appears on the screen. On the screen we see only a part of the result, but a display is rolling and by means of arrows we can shift it. We can read

`x=1 and y=1 and z=-2 or x=1 and y=-2 and z=1 or x = -2 and y =1 and z=1`

i.e., the solution P of the given system (1) is

$$P = \{[1, 1, -2], [1, -2, 1], [-2, 1, 1]\}.$$

In manuals of calculators there is explained, that in the case of solving a system of algebraic equations the Buchberger's algorithm for computing Groebner bases of an ideal by so called lexicographic order of variables is used. If the user wants to know more it is suitable to take advantage of some commercial programs of a computer algebra (Maple, Mathematica) or free to download programs from Internet (Singular, CoCoA). In Mathematica /version 4/ we can write `poly = {x^2 + y^2 + z^2 == 6, x^3 + y^3 + z^3 - x * y * z == -4, x * y + x * z + y * z == -3}` and after that we put `GroebnerBasis[poly, {x, y, z}]` and obtain $-12z + 9z^2 + 4z^3 - 6z^4 + z^6 + 4, 49y^2 + 12yz^5 - 16yz^4 - 18yz^3 + 72yz^2 - 37yz + 36y - 16z^5 + 54z^4 + 24z^3 - 145z^2 + 180z - 195, 49x + 49y + 12z^5 - 16z^4 - 18z^3 + 72z^2 - 37z + 36$. To comment the situation better denote the above polynomials by

$$\begin{aligned}
g_1(z) &= -12z + 9z^2 + 4z^3 - 6z^4 + z^6 + 4, \\
g_2(y, z) &= 49y^2 + 12yz^5 - 16yz^4 - 18yz^3 + 72yz^2 - 37yz + 36y - 16z^5 \\
&\quad + 54z^4 + 24z^3 - 145z^2 + 180z - 195, \\
g_3(x, y, z) &= 49x + 49y + 12z^5 - 16z^4 - 18z^3 + 72z^2 - 37z + 36.
\end{aligned}$$

Solutions of the system (1) are certain ordered triples of real (or complex) numbers $[x, y, z]$. How to find them? It is obvious that instead of the system (1) it is better to solve the equivalent system

$$g_1(z) = 0, \quad g_2(y, z) = 0, \quad g_3(x, y, z) = 0, \tag{2}$$

where the polynomials $g_1(z), g_2(y, z), g_3(x, y, z)$ form a Groebner basis of the ideal $I = \langle f_1, f_2, f_3 \rangle$ by the lexicographic order $<_L$, where $z <_L y <_L x$. To find the solution of (2) the simplest way is first to solve the equation $g_1(z) = 0$, which contains only one unknown z. Although the polynomial $g_1(z)$ doesn't look simple, we can use the function `Factor[expr]`, which decomposes a given expression `expr`. In this case we have $g_1(z) = (z-1)^4(z+2)^2$ and see that the equation $g_1(z) = 0$ has two real (and multiple) roots $z_1 = 1,\ z_2 = -2$. Setting e.g. the value $z_1 = 1$ into the equation $g_2(y, z) = 0$ we obtain $g_2(y, 1) = 49y^2 + 49y - 98 = 0$, with the roots

$y_1 = 1, y_2 = -2$. If we substitute all these values into the last equation $g_3(x, y, z) = 0$, we arrive at the solution P of (2), which is the same as the solution of (1) $P = \{[1, 1, -2], [1, -2, 1], [-2, 1, 1]\}$. Behind the result which the calculator yielded not only new technology is hidden but also a big progress, which commutative algebra and algebraic geometry achieved in the last third of the last century. The extent of this paper doesn't allow us to write more about these issues, we prefer rather non formal, intuitive approach. For detailed information see the books [4], [2], or [6] on Internet or [3], [9], [7].

We could notice that in the course of solving the system of equations (1) by the lexicographic order $<_L$, where $z <_L y <_L x$ the variable x is first eliminated and then y. In the end in the Groebner basis of the ideal $I = \langle f_1, f_2, f_3 \rangle$, where $f_i,\ i = 1, 2, 3$ denote the polynomials which form the system (1) the polynomial g_1 occurs, which is a function only of one variable z. The equation $g_1(z) = 0$ is not a problem to solve.

The elimination of variables, which is realized in programs of computer algebra using Groebner bases can also bring the method of proving and discovering theorems. In the next part of this paper we would want to give non traditional proofs of some theorems from elementary geometry. In these proofs we shall take advantage of the elimination of variables. To do this first we have to look at the elimination closely.

Definition. Let $I = \langle f_1, f_2, \ldots, f_s \rangle \subset k[x_1, x_2, \ldots, x_n]$ be an ideal. The r^{th} elimination ideal I_r is the ideal of the domain of integrity $k[x_1, x_2, \ldots, x_n]$ which fulfils

$$I_r = I \cap k[x_{r+1}, x_{r+2}, \ldots, x_n].$$

In general the following theorem about elimination holds, see [4].

Theorem. *Let $I \subset k[x_1, x_2, \ldots, x_n]$ be an ideal and G the Groebner basis of the ideal I with respect to lexicographic order, where $x_1 >_L x_2 >_L \cdots >_L x_n$. Then for every $r,\ 0 \le r \le n$, the set $G_r = G \cap k[x_{r+1}, x_{r+2}, \ldots, x_n]$ is a Groebner basis of the r^{th} elimination ideal I_r.*

Example 1. Find the formula of Heron for the area F of a triangle ABC with sides a, b, c. Give "a computer proof".

Solution. Choose the coordinate system so that coordinates of the vertices of a triangle ABC are $A = [0, 0],\ B = [c, 0],\ C = [x, y]$ and $|AB| = c,\ |BC| = a,\ |AC| = b$. Let us construct the ideal $I = \langle a^2 - (c-x)^2 - y^2, b^2 - x^2 - y^2, F - \frac{1}{2}cy \rangle$ in the ring $R[a, b, c, x, y, F]$. We try to obtain a formula, which describes a relation between the lengths of sides a, b, c of a triangle ABC and its area F. Such a polynom should belong into the elimination ideal $I \cap R[a, b, c, F]$. In this example the whole computation can be performed not only with the software specialized on ideals but even with such a common software like Mathematica /version 4/. We write

```
Eliminate[{(c - x)^2 + y^2 == a^2, x^2 + y^2 == b^2, F == 1/2c * y}, {x, y}]
```

and obtain

$$16F^2 == -a^4 + 2a^2b^2 - b^4 + 2a^2c^2 + 2b^2c^2 - c^4$$

the result. The next command

`Factor[−a^4 + 2a^2b^2 − b^4 + 2a^2c^2 + 2b^2c^2 − c^4]`

gives

$$-(a-b-c)(a+b-c)(a-b+c)(a+b+c).$$

It is easy to see that the last relation is the same as

$$F = \sqrt{s(s-a)(s-b)(s-c)},$$

where $s = \frac{1}{2}(a+b+c)$. We get the formula of Heron.

Now we will investigate the area of a quadrangle in a plane.

Example 2. Let $ABCD$ be a planar quadrangle with sides a, b, c, d and diagonals e, f. Find the formula of the area F of a quadrangle $ABCD$. Give a "computer proof".

Solution. Let the coordinates of the vertices of a quadrangle $ABCD$ be $A = [a, 0]$, $B = [x, y]$, $C = [z, v]$, $D = [0, 0]$ and $a = |DA|$, $b = |AB|$, $c = |BC|$, $d = |CD|$, $e = |BD|$, $f = |AC|$. It is easy to see that for the area of a quadrangle $F = \frac{1}{2}(xv - zy + ay)$ holds. By means of Mathematica we write

```
Eliminate[{(x − a)^2 + y^2 == b^2, (x − z)^2 + (y − v)^2 == c^2, z^2 + v^2 =
= d^2, x^2 + y^2 == e^2, (z − a)^2 + v^2 == f^2, 2F == x ∗ v − z ∗ y + a ∗ y},
{x, y, z, v}]
```

which gives

$$\begin{aligned} &e^4f^2 + e^2(a^2b^2 - a^2c^2 - b^2d^2 + c^2d^2 - a^2f^2 - b^2f^2 - c^2f^2 - d^2f^2 + f^4) == \\ &- a^4c^2 + a^2b^2c^2 - a^2c^4 + a^2b^2d^2 - b^4d^2 + a^2c^2d^2 + b^2c^2d^2 - b^2d^4 + a^2c^2f^2 \\ &- b^2c^2f^2 - a^2d^2f^2 + b^2d^2f^2 \&\& 16F^2 == -a^4 + 2a^2b^2 - b^{-}2a^2c^2 + 2b^2c^24 \\ &- c^4 + 2a^2d^2 - 2b^2d^2 + 2c^2d^2 - d^4 + 4e^2f^2. \end{aligned} \tag{3}$$

It seems that the second equality is the relation we are looking for. We can simplify it by

```
FullSimplify[16F^2 == −a^4 + 2a^2b^2 − b^4 − 2a^2c^2 + 2b^2c^2 − c^4+
2a^2d^2 − 2b^2d^2 + 2c^2d^2 − d^4 + 4e^2f^2]
```

and get

$$(a^2 - b^2 + c^2 - d^2)^2 + 16F^2 == 4e^2f^2,$$

which is a desired result.

Remark. This formula by means of which we can express the area of a quadrangle by the all six distances between the four vertices has often been given in the form

$$16F^2 = 4e^2f^2 - (a^2 - b^2 + c^2 - d^2)^2. \tag{4}$$

The formula (4) was published by Staudt [11]. Notice that if we set e.g. $d = 0$ into (3) we obtain the formula of Heron.

The first equality in (3) is related to the so called Euler's four points relation, see [5], which expresses the dependence of six distances a, b, c, d, e, f between four vertices of a quadrangle. Euler's four points relation follows from the Cayley–Menger determinant for the volume V of a tetrahedron with edges of lengths a, b, c, d, e, f

$$288V^2 = \begin{vmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & b^2 & f^2 & a^2 \\ 1 & b^2 & 0 & c^2 & e^2 \\ 1 & f^2 & c^2 & 0 & d^2 \\ 1 & a^2 & e^2 & d^2 & 0 \end{vmatrix} \tag{5}$$

if we put $V = 0$. We will compare the equation $V = 0$ from (5) with the first equality in (3). Denote by m the determinant above

```
m = {{0,1,1,1,1},{1,0,b^2,f^2,a^2},{1,b^2,0,c^2,e^2},{1,f^2,c^2,0,d^2},
{1,a^2,e^2,d^2,0}}.
```

Then the command

```
Det[m]
```

gives $-2a^4c^2 + 2a^2b^2c^2 - 2a^2c^4 + 2a^2b^2d^2 - 2b^4d^2 + 2a^2c^2d^2 + 2b^2c^2d^2 - 2b^2d^4 - 2a^2b^2e^2 + 2a^2c^2e^2 + 2b^2d^2e^2 - 2c^2d^2e^2 + 2a^2c^2f^2 - 2b^2c^2f^2 - 2a^2d^2f^2 + 2b^2d^2f^2 + 2a^2e^2f^2 + 2b^2e^2f^2 + 2c^2e^2f^2 + 2d^2e^2f^2 - 2e^4f^2 - 2e^2f^4$.

We see that the condition $V = 0$ is the same as the first condition in (3).

Now we will investigate the case of a cyclic quadrangle, i.e., a quadrangle which is inscribed into the circle. Suppose we are given a cyclic quadrangle A, B, C, D with the sides $a = |AB|,\ b = |BC|,\ c = |CD|,\ d = |DA|$ and the radius r of the circumscribed circle. The well-known formula of Brahmagupta for the evaluation of the area F of a cyclic convex quadrangle with the sides a, b, c, d is as follows:

$$F = \sqrt{\frac{(-a+b+c+d)}{2}\frac{(a-b+c+d)}{2}\frac{(a+b-c+d)}{2}\frac{(a+b+c-d)}{2}}. \tag{6}$$

Example 3. Find the formula of Brahmagupta. Give "a computer proof".

Solution. Choose the Cartesian coordinate system so that $A = [r, 0]$, $B = [x, y]$, $C = [u, v]$, $D = [z, w]$ and place the origin into the center of the circumscribed circle with radius r. To express the area F of a quadrangle A, B, C, D we use the following formula for evaluating the oriented area of a n-gon $A_1, A_2, \ldots, A_n$ with coordinates $A_i = [x_i, y_i]$. Then

$$F = \frac{1}{2}\sum_{i=1}^{n}\begin{vmatrix} x_i & y_i \\ x_{i+1} & y_{i+1} \end{vmatrix} \tag{7}$$

holds. Using Mathematica we enter

```
Eliminate[{x^2 + y^2 == r^2, u^2 + v^2 == r^2, z^2 + w^2 == r^2, (x − r)^2+
y^2 == a^2, (u − x)^2 + (v − y)^2 == b^2, (z − u)^2 + (w − v)^2 == c^2,
(r − z)^2 + w^2 == d^2, 2F == y ∗ r − u ∗ y + x ∗ v − z ∗ v + u ∗ w − r ∗ w},
{x, y, u, v, z, w, r}]
```

and get

$(32a^4 - 64a^2b^2 + 32b^4 - 64a^2c^2 - 64b^2c^2 + 32c^4 - 64a^2d^2 - 64b^2d^2 - 64c^2d^2 + 32d^4)F^2 + 256F^4 == -a^8 + 4a^6b^2 - 6a^4b^4 + 4a^2b^6 - b^8 + 4a^6c^2 - 4a^4b^2c^2 - 4a^2b^4c^2 + 4b^6c^2 - 6a^4c^4 - 4a^2b^2c^4 - 6b^4c^4 + 4a^2c^6 + 4b^2c^6 - c^8 + 4a^6d^2 - 4a^4b^2d^2 - 4a^2b^4d^2 + 4b^6d^2 - 4a^4c^2d^2 + 40a^2b^2c^2d^2 - 4b^4c^2d^2 - 4a^2c^4d^2 - 4b^2c^4d^2 + 4c^6d^2 - 6a^4d^4 - 4a^2b^2d^4 - 6b^4d^4 - 4a^2c^2d^4 - 4b^2c^2d^4 - 6c^4d^4 + 4a^2d^6 + 4b^2d^6 + 4c^2d^6 - d^8.$

After the command

```
FullSimplify[%]
```

we obtain

$$\begin{aligned} &((a-b-c-d)(a+b+c-d)(a+b-c+d)(a-b+c+d)+16F^2) \\ &((a+b-c-d)(a-b+c-d)(a-b-c+d)(a+b+c+d)+16F^2) == 0. \end{aligned} \tag{8}$$

From (8) we get two relations. The first one

$$16F^2 = (-a+b+c+d)(a+b+c-d)(a+b-c+d)(a-b+c+d)$$

gives the Brahmagupta's relation (6).

Remark. The second relation wchich follows from (8) is

$$16F^2 = (-a-b+c+d)(a-b+c-d)(a-b-c+d)(a+b+c+d). \tag{9}$$

It is easy to show that F from (9) is the (oriented) area of a non convex quadrangle with the sides a, b, c, d which is inscribed into the circle, whereas the Brahmagupta's formula (6) holds for cyclic *convex* quadrangles. We could arrive at it from the Brahmagupta's formula writing $-b$ instead of b.

In the last example we will deal with the well-known Ptolemy's formula. We won't be able to do "a computer discovery" but we will be successful in proving it.

Example 4. Let A, B, C, D be a quadrangle with lengths of sides $|AB| = a$, $|BC| = b$, $|CD| = c$, $|DA| = d$, $|BD| = e$, $|AC| = f$. The necessary and sufficient condition for the points A, B, C, D to be on a circle is, see [8]

$$\begin{vmatrix} 0 & a^2 & f^2 & d^2 \\ a^2 & 0 & b^2 & e^2 \\ f^2 & b^2 & 0 & c^2 \\ d^2 & e^2 & c^2 & 0 \end{vmatrix} = 0. \tag{10}$$

Give "a computer proof" of (10).

Solution. Let us evaluate the determinant in the equation (10).

By the command

`Det[{0, a^2, f^2, d^2}, {a^2, 0, b^2, e^2}, {f^2, b^2, 0, c^2}, {d^2, e^2, c^2, 0}] == 0`

we get

$$a^4c^4 - 2a^2b^2c^2d^2 + b^4d^4 - 2a^2c^2e^2f^2 - 2b^2d^2e^2f^2 + e^4f^4 == 0,$$

and after

`Factor[a^4c^4 - 2a^2b^2c^2d^2 + b^4d^4 - 2a^2c^2e^2f^2 - 2b^2d^2e^2f^2 + e^4f^4]`

we obtain

$$(ac - bd - ef)(ac + bd - ef)(ac - bd + ef)(ac + bd + ef) = 0. \tag{11}$$

From (11) we could derive various types of Ptolemy's formula in accordance with the order of the vertices A, B, C, D of a quadrangle on the circle. First we will try "to discover" (11) in a similar way we did it in previous examples. Suppose we have chosen the same coordinate system as in the Example 3. We put

`Eliminate[{x^2 + y^2 == r^2, u^2 + v^2 == r^2, z^2 + w^2 == r^2, (x - r)^2 + y^2 == a^2, (u - x)^2 + (v - y)^2 == b^2, (z - u)^2 + (w - v)^2 == c^2, (r - z)^2 + w^2 == d^2, (x - z)^2 + (y - w)^2 == e^2, (u - r)^2 + v^2 == f^2}, {x, y, u, v, z, w, r}]`

and get

$a^4b^2c^2+a^2(-b^4d^2-c^4d^2-2b^2c^2e^2+2b^2d^2e^2+2c^2d^2e^2-d^2e^4) == b^2c^2(-d^4+2d^2e^2-e^4)\&\&e^2(b^2+c^2-e^2)f^2 == -a^2b^2c^2+a^2c^4+b^4d^2-b^2c^2d^2-a^2c^2e^2+2b^2c^2e^2-b^2d^2e^2\&\&e^2(a^2+d^2-e^2)f^2 == a^4c^2-a^2b^2d^2-a^2c^2d^2+b^2d^4-a^2c^2e^2+2a^2d^2e^2-b^2d^2e^2\&\&(a^2b^2-c^2d^2+c^2e^2+d^2e^2-e^4)f^2 == a^2c^4-a^2c^2d^2-b^2c^2d^2+b^2d^4-a^2c^2e^2+b^2c^2e^2+a^2d^2e^2-b^2d^2e^2\&\&(-a^2c^2-b^2d^2+2c^2d^2-c^2e^2-d^2e^2)f^2+e^2f^4 == -a^2c^4+a^2c^2d^2+b^2c^2d^2-b^2d^4.$

We obtained a Groebner basis of the elimination ideal $I \cap R[a,b,c,d,e,f]$ but the relation (11) is not involved in it. To prove (11) we will try to find out whether the polynomial given by (11) belongs to the ideal $I \cap R[a,b,c,d,e,f]$. It suffices to prove that the remainder on division of the polynom from (11) by the elements of a Groebner basis of $I \cap R[a,b,c,d,e,f]$ is zero, see [4]. The remainder is often called normal form. Since the command `normalf` for evaluating of the remainder is not present in Mathematica (but is available in Maple) we will use the command `PolynomialReduce` instead. The syntax of this command is as follows:

```
In[1]:=PolynomialReduce[f,polylist,varlist,options]
```

This command computes the quotients and remainder of f on division by the polynomials in `polylist` using monomial order specified by `varlist` and `MonomialOrder` in option. If we do not type this option, Mathematica will use default order, which is `Lexicographic`. The output is a list of two entries: the first is the list of quotients and the second the remainder. We type

```
PolynomialReduce[a^4c^4 - 2a^2b^2c^2d^2 + b^4d^4 - 2a^2c^2e^2f^2 - 2b^2
d^2e^2f^2 + e^4f^4, a^4b^2c^2 + a^2(-b^4d^2 - c^4d^2 - 2b^2c^2e^2 + 2b^2
d^2e^2 + 2c^2d^2e^2 - d^2e^4) - (b^2c^2(-d^4 + 2d^2e^2 - e^4)), e^2(b^2 + c
^2 - e^2)f^2 - (-a^2b^ 2c^2 + a^2c ^ 4 + b^4d^2 - b^2c^2d^2 - a^2c^2e^2+
2b^2c^2e^2 - b^2d^2e^2), e^2(a^2 + d^2 - e^2)f^2 - (a^4c^2 - a^2b^2d^2 - a^
2c^2d^2 + b^2d^4 - a^2c^2e^2 + 2a^2d^2e^2 - b^2d^2e^2), (a^2b^2 - c^2d^2+
c^2e^2 + d^2e^2 - e^4)f^2 - (a^2c^4 - a^2c^2d^2 - b^2c^2d^2 + b^2d^4 - a^
2c^2e^2 + b ^2c^2e^2 + a^2d^2e^2 - b^2d^2e^2), (-a^2c^2 - b^2d^2 + 2c^2d^
2 - c^2e^2 - d^2e^2)f^ 2 + e^2f^4 - (-a^2c^4 + a^2c^2d^2 + b^2c^2d^2 - b^
2d^4)}, {a, b, c, d, e, f}]
```

and the result

$$\{\{0, -d^2, -c^2, 0, e^2\}, 0\}$$

immediately appears. It means that the remainder is zero and (11) holds. In addition we know that the polynomials needed for multipying of the elements of a Groebner basis above to arrive at the Ptolemy's formula (11) are $0, -d^2, -c^2, 0, e^2$.

Remark. Using the same method to investigate properties of planar n-gons for $n > 4$ fails for the present. To improve the process of elimination perhaps it could be helpful to use special monomial orders of r-elimination type [1].

References

[1] Bayer, D., Stillman, M., A theorem on refining division orders by the reverse lexicographic order, *Duke J. Math.* **55** (1987), 321–328.

[2] Becker, Th., Weispfeiming, V., Kredel, H., *Groebner Bases: a Computational Approach to Commutative Algebra*, Graduate Text in Mathematics, Vol. **141** Springer-Verlag, New York, 1993.

[3] Buchberger, B., Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems, *Aegn. Math. H.* (1970), 374–383.

[4] Cox, D., Little, J., O'Shea, D., *Ideals, varieties and algorithms*, Second Edition, Springer-Verlag, 1997.

[5] Dörrie, B. H., *Triumph der Mathematik*, Breslau 1933.

[6] Heck, A., A Bird's-Eye View of GrBases, In: `http://www.can.nl/~ heck/AIHENP96/AIHENP96.html`

[7] Hora, J., *O některých otázkách souvisejících s využíváním programu počítačové algebry ve škole, II. díl*, Pedagogické centrum, Plzeň, 1998.

[8] Kowalewski, G., *Einführung in die Determinantentheorie*, Veit & Comp., Leipzig, 1909.

[9] Pethő, A., *Algebraische Algorithmen*, Vieweg, Braunschweig, Wiesbaden, 1999.

[10] Robbins, D. P., Areas of polygons inscribed in a circle, *Discrete Comput. Geom.* **12** (1994), 223–236.

[11] Staudt, Ch. R., Über die Inhalte der Polygone und Polyeder, *Journal für die reine und angewandte Mathematik* **24** (1842), 252–256.

Jaroslav Hora
University of West Bohemia
Pedagogical Faculty, Klatovská 51
306 14 Plzeň, Czech Republic
E-mail: horajar@kmt.zcu.cz

Pavel Pech
University of South Bohemia
Pedagogical Faculty,
Jeronýmova 10 371 15 České Budějovice,
Czech Republic
E-mail: pech@pf.jcu.cz

ALMOST SURE FUNCTIONAL LIMIT THEOREMS IN $L^p(]0,1[)$, WHERE $1 \le p < \infty$

József Túri (Nyíregyháza, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. The almost sure version of Donsker's theorem is proved in $L^p(]0,1[)$, where $1 \le p < \infty$. The almost sure functional limit theorem is obtained for the empirical process in $L^p(]0,1[)$, where $1 \le p < \infty$.

AMS Classification Number: 60F17

Keywords: Functional limit theorem, almost sure central limit theorem, independent variables

1. Introduction

The simplest form of the central limit theorem is $\frac{1}{\sigma\sqrt{n}} S_n \Rightarrow \mathcal{N}(0,1)$, as $n \to \infty$, if S_n is the n^{th} partial sum of independent, identically distributed (i.i.d.) random variables with mean zero and variance σ^2. Here $\Rightarrow$ denotes convergence in distribution, while $\mathcal{N}(0,1)$ is the standard normal law. The functional central limit theorem, proved by Donsker, states that the broken line process connecting the points $(\frac{i}{n}, \frac{1}{\sigma\sqrt{n}} S_i)$, $i = 0, 1, \dots, n$, converges weakly to the standard Wiener process W in the space $C([0,1])$, see Billingsley [3].

A relatively new version of the CLT is the so called almost sure (a.s.) CLT, see Brosamler [4], Schatte [13], Lacey and Philipp [9]. The simplest form of the a.s. CLT is the following. Drop $\frac{1}{\log n} \frac{1}{k}$ weight to the point $\frac{1}{\sigma\sqrt{k}} S_k(\omega)$, $k = 1, \dots, n$. Then this discrete measure weakly converges to $\mathcal{N}(0,1)$ for P-almost every $\omega \in \Omega$. (Here $(\Omega, \mathcal{A}, P)$ is the underlying probability space.) The almost sure version of Donsker's theorem is also known, see e.g. Fazekas and Rychlik [7] and the references therein.

In this paper we will prove the a.s. version of Donker's theorem in $L^p(]0,1[)$, see Theorem 2.1.

In this space in contrast to the case of $C([0,1])$, we can manage without any maximal inequality. Using elementary facts of probability theory, we derive our result from the general a.s. limit theorem in Fazekas and Rychlik [7].

A well-known result of statistics is that the uniform empirical process converges to the Brownian bridge B in the space $D([0,1])$, see Billingsley [3]. The almost sure version of this theorem is also known, see e.g. Fazekas and Rychlik [7]. The proof of that theorem is based on a sophisticated inequality of Dvoretzky, Kiefer and Wolfowitz.

Here we show that the a.s. version of the limit theorem for the empirical process is valid in $L^p(]0,1[)$, see Theorem 3.1. Our proof uses only elementary facts.

We also prove the (non a.s.) functional limit theorems in $L^p(]0,1[)$. Proposition 2.1 is the Donsker theorem, Proposition 3.1 contains the convergence of the empirical process. The proof of these propositions are straightforward calculations to check the tightness conditions given in Oliveira and Suquet [12] and Marcinkiewicz and Zygmund, see e.g. in [5].

All results of this paper was proved for $p = 2$ in [14].

2. The almost sure Donsker theorem in $L^p(]0,1[)$

In this part we consider the process

$$Y_n(t) = \frac{1}{\sigma\sqrt{n}} S_{[nt]}, \quad \text{if} \quad t \in [0,1], \tag{1}$$

where $S_0 = 0$, $S_k = X_1 + X_2 + \cdots + X_k$, $k \geq 1$, and $X_1, X_2, \ldots$ are i.i.d. real random variables with $EX_1 = 0$ and $D^2 X_1 = \sigma^2$ and $E|X_1|^p < \infty$. Here $[\cdot]$ denotes the integer part. We shall prove a.s. limit theorem for $Y_n(t)$ in $L^p(]0,1[)$. For the sake of completeness first we prove the usual limit theorem.

We will use the next result due to Marcinkiewicz and Zygmund (see [5]) and its consequence (Remark 2.1).

Remark 2.1. If $\{X_n, n \geq 1\}$ are independent random variables with $EX_n = 0$, then for every $p \geq 1$ there exists a positive constant C_p depending only upon p for which

$$\left\| \sum_{i=1}^n X_i \right\|_p \leq C_p \left\| \left(\sum_{i=1}^n X_i^2 \right)^{1/2} \right\|_p .$$

Remark 2.2. If $\{X_n, n \geq 1\}$ are i.i.d. with $EX_1 = 0$, $E|X_1|^p < \infty$ if $2 \leq p < \infty$ and $E|X_1|^2 < \infty$ if $1 \leq p \leq 2$ and $S_n = \sum_{i=1}^n X_i$, then $E|S_n|^p = O\left(n^{p/2}\right)$.

We also need the result below due to Oliveira and Suquet [12].

Remark 2.3. Let $(Y_n(t), n \geq 1)$ be a sequence of random elements in $L^p(]0,1[)$, $p \geq 1$. Assume that

(i) for some $\gamma > 1$, $\sup_{n \geq 1} E\|Y_n\|_1^\gamma < \infty$,

(ii) $\lim_{h \to 0} \sup_{n \geq 1} E\|Y_n(\cdot + h) - Y_n(\cdot)\|_p^p = 0$.

Then $(Y_n(t), n \geq 1)$ is tight in $L^p(]0,1[)$.

Proposition 2.1. *The sequence of processes $(Y_n(t), n \geq 1)$ defined in (1) converges weakly to the standard Wiener process W in $L^p(]0,1[)$, where $1 \leq p < \infty$.*

Proof. According to Theorem 6.2.2. of [8] we have to prove that the family $(Y_n(t), n \geq 1)$ is tight and $\langle f, Y_n(t)\rangle \Rightarrow \langle f, W\rangle$ for each f from the dual space of $L^p(]0,1[)$. First consider the convergence in distribution of $\int_0^1 Y_n(t)f(t)dt$ to $\int_0^1 W(t)f(t)dt$ for f in $L^q(]0,1[)$, the dual space of $L^p(]0,1[)$.

But $\int_0^1 Y_n(t)f(t)dt$ converges weakly to normal distribution with mean zero and variance $\int_0^1\int_0^1 min\{s,t\}f(s)f(t)dsdt$. However it is the distribution of the random variable $\int_0^1 W(t)f(t)dt$.

Now, we prove that the conditions (i) and (ii) of Remark 2.3 are satisfied.

First we show that (i) is fulfilled with $\gamma = 2$, i.e., $\sup_{n\geq 1} E\|Y_n\|_1^2 < \infty$ is satisfied. This is implied by the following calculation:

$$\begin{aligned}
\sup_{n\geq 1} E\|Y_n\|_1^2 &= \sup_{n\geq 1} E\left\|\frac{1}{\sigma\sqrt{n}}S_{[nt]}\right\|_1^2 = \sup_{n\geq 1} E\left(\int_0^1 \left|\frac{1}{\sigma\sqrt{n}}S_{[nt]}\right| dt\right)^2 \\
&= \sup_{n\geq 1} E\left(\sum_{i=0}^{n-1}\int_{i/n}^{(i+1)/n}\left|\frac{S_i}{\sigma\sqrt{n}}\right| dt\right)^2 = \sup_{n\geq 1} E\left(\frac{1}{\sigma\sqrt{n}}\,\frac{1}{n}\sum_{i=0}^{n-1}|S_i|\right)^2 \\
&\leq \sup_{n\geq 1}\frac{1}{\sigma^2 n}E\left(\frac{1}{n}\sum_{i=0}^{n-1}|S_i|^2\right) = \sup_{n\geq 1}\frac{1}{\sigma^2 n^2}\sum_{i=0}^{n-1}E|S_i|^2 \\
&= \sup_{n\geq 1}\frac{1}{\sigma^2 n^2}\sigma^2\sum_{i=0}^{n-1} i = \sup_{n\geq 1}\left(\frac{1}{n^2}\,\frac{n(n-1)}{2}\right) = \sup_{n\geq 1}\left(\frac{n-1}{2n}\right) < \infty.
\end{aligned}$$

Now we prove condition (ii). This follows from the argument below, where $\{\cdot\}$ denotes the fractional part.

$$\begin{aligned}
E\|Y_n(t+h) - Y_n(t)\|_p^p &= E\int_0^1 |Y_n(t+h) - Y_n(t)|^p\, dt \\
&= E\int_0^{1-h}\left|\frac{1}{\sigma\sqrt{n}}S_{[n(t+h)]} - \frac{1}{\sigma\sqrt{n}}S_{[nt]}\right|^p dt \\
&\quad + E\int_{1-h}^1\left|\frac{1}{\sigma\sqrt{n}}S_{[nt]}\right|^p dt
\end{aligned}$$

$$
\begin{aligned}
&= \int_0^{1-h} E\left|\frac{1}{\sigma\sqrt{n}}\left(X_{[n(t+h)]}+\cdots+X_{[nt]+1}\right)\right|^p dt \\
&\quad + \int_{1-h}^{1} E\left|\frac{1}{\sigma\sqrt{n}}S_{[nt]}\right|^p dt \\
&= \int_0^{1-h} \frac{1}{n^{p/2}\sigma^p} E\left|X_{[n(t+h)]}+\cdots+X_{[nt]+1}\right|^p dt \\
&\quad + \int_{1-h}^{1} \frac{1}{n^{p/2}\sigma^p} E|S_{[nt]}|^p\, dt \\
&\le \int_0^{1-h} \frac{1}{n^{p/2}\sigma^p} C([n(t+h)]-[nt])^{p/2}\, dt \\
&\quad + \int_{1-h}^{1} \frac{1}{n^{p/2}\sigma^p} C[nt]^{p/2}\, dt \\
&\le \frac{C}{n^{p/2}\sigma^p}\int_0^1 ([\{nt\}+\{nh\}]+[nh])^{p/2}\, dt + \frac{C}{n^{p/2}} h n^{p/2} \\
&\le C^* h \to 0, \quad \text{as } h \to 0.
\end{aligned}
$$

The proof of Proposition 2.1 is complete.

To prove a.s. Donsker's theorem we shall need the next result due to Fazekas and Rychlik [7] (see also Chuprunov and Fazekas [6]). Let μ_X denote the distribution of X. Let δ_x be the unit mass at x.

Remark 2.4. Let (M, ρ) be a complete separable metric space and X_n, $n \in N$, be a sequence of random elements in M. Assume that there exist $C > 0$, $\varepsilon > 0$ and an increasing sequence of positive numbers C_n with $\lim_{n\to\infty} C_n = \infty$, $C_{n+1}/C_n = O(1)$, and M-valued random elements $X_{k,l}$, $k, l \in N$, $k < l$, such that the random elements X_k and $X_{k,l}$ are independent for $k < l$ and

$$
E\rho(X_{k,l}, X_l) \le C\left(\frac{C_k}{C_l}\right)^\beta \tag{2}
$$

for $k < l$, where $\beta > 0$. Let $0 \le d_k \le \log(C_{k+1}/C_k)$, assume that $\sum_{k=1}^\infty d_k = \infty$. Let $D_n = \sum_{k=1}^n d_k$. Then, for any probability distribution μ on the Borel σ-algebra of M, the following two statements are equivalent

$$
\frac{1}{D_n}\sum_{k=1}^n d_k \delta_{X_k(\omega)} \Rightarrow \mu, \qquad \text{as } n \to \infty \text{ for almost every } \omega \in \Omega;
$$

$$
\frac{1}{D_n}\sum_{k=1}^n d_k \mu_{X_k} \Rightarrow \mu, \qquad \text{as } n \to \infty.
$$

The following result is the a.s. Donsker's theorem in $L^p(]0,1[)$, where $1 \leq p < \infty$.

Theorem 2.1. *Let* $1 \leq p < \infty$.

$$\frac{1}{\log n} \sum_{k=1}^{n} \frac{1}{k} \delta_{Y_{k(\cdot,\omega)}} \Rightarrow \mu_W,$$

in $L^p(]0,1[)$*, as* $n \to \infty$*, for almost every* $\omega \in \Omega$*, where* W *is the standard Wiener process and* $Y_k(t,\omega) = Y_k(t)$ *is defined in (1).*

Proof. We shall prove that the conditions of Remark 2.4 are fulfilled. The separability and completeness of space $L^p(]0,1[)$ $(1 \leq p < \infty)$ are well-known facts.

Let us define the process

$$Y_{k,n}(t) = \left(Y_n(t) - \frac{S_k}{\sigma\sqrt{n}}\right) I_{]k/n,1]}(t), \qquad k = 1, 2, \ldots, n-1,\ t \in [0,1],$$

where I_A denotes the indicator function of the set A. Then $Y_{k,n}$ and Y_k are independent for $k < n$.

$$\begin{aligned}
&E\rho(Y_n, Y_{k,n}) = E\left(\int_0^1 \left|Y_n(t) - \left(Y_n(t) - \frac{S_k}{\sigma\sqrt{n}}\right) I_{]k/n,1]}(t)\right|^p dt\right)^{1/p} \\
&\leq \left(E\int_0^1 \left|Y_n(t) - \left(Y_n(t) - \frac{S_k}{\sigma\sqrt{n}}\right) I_{]k/n,1]}(t)\right|^p dt\right)^{1/p} \\
&= \left(E\left(\left|\frac{S_1}{\sigma\sqrt{n}}\right|^p \frac{1}{n} + \left|\frac{S_2}{\sigma\sqrt{n}}\right|^p \frac{1}{n} + \cdots + \left|\frac{S_{k-1}}{\sigma\sqrt{n}}\right|^p \frac{1}{n} + \left|\frac{S_k}{\sigma\sqrt{n}}\right|^p \frac{n-k}{n}\right)\right)^{1/p} \\
&\leq \left(\frac{1}{\sigma^p n^{p/2} n} C\left(1^{p/2} + 2^{p/2} + \cdots + (k-1)^{p/2} + (k)^{p/2}(n-k)\right)\right)^{1/p} \\
&\leq \left(\frac{C}{\sigma^p n^{p/2} n} k^{p/2}[(k-1) + (n-k)]\right)^{1/p} \\
&\leq C^* \left(\frac{k^{p/2}}{n^{p/2}}\right)^{1/p} = C^* \sqrt{\frac{k}{n}}.
\end{aligned}$$

So condition (2) of Remark 2.4 holds and the proof of Theorem 2.1 is complete.

3. The empirical process in $L^p(]0,1[)$

In this section, we consider the empirical process

$$Z_n(t) = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (I_{[0,t]}(U_i) - t), \qquad t \in [0,1],$$

where U_i $(i = 1, 2, \ldots)$ are independent random variables with uniform distribution on the interval $[0,1]$.

For the sake of completeness we prove the weak convergence of Z_n.

Proposition 3.1. *The process $(Z_n(t),\ n \geq 1)$ weakly converges to the Brownian bridge B in space $L^p(]0,1[)$, where $1 \leq p < \infty$.*

Proof. First we prove the convergence in distribution of $\int_0^1 Z_n(t)f(t)dt$ to $\int_0^1 B(t)f(t)dt$ for each f in $L^q(]0,1[)$ the dual space of $L^p(]0,1[)$. $\int_0^1 Z_n(t)f(t)dt$ converges weakly to the normal distribution with mean zero and variance $\int_0^1 \int_0^1 (min\{s,t\} - st)f(s)f(t)dsdt$. But it is the distribution of $\int_0^1 B(t)f(t)dt$.

Now we prove that the condition (i) of Remark 2.3 is fulfilled with $\gamma = 2$. Since $\|\cdot\|_1 \leq \|\cdot\|_2$ this will be done if we show $\sup_{n\geq 1} E\|Z_n\|_2^2 < \infty$.

$$\begin{aligned}
E\|Z_n\|_2^2 &= E \left\| \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (I_{[0,t]}(U_i) - t) \right\|_2^2 = E \int_0^1 \left| \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (I_{[0,t]}(U_i) - t) \right|^2 dt \\
&= \frac{1}{n} E \int_0^1 \left| \sum_{i=1}^{n} (I_{[0,t]}(U_i) - t) \right|^2 dt \\
&= \frac{1}{n} \int_0^1 E(\xi - nt)^2 \, dt = \frac{1}{n} \int_0^1 nt(1-t)\, dt = \frac{1}{6},
\end{aligned}$$

where ξ is a binomial random variable with parameters t and n.

Now, we will show that condition (ii) of Remark 2.3 is fulfilled.

$$\begin{aligned}
E\|Z_n(\cdot + h) - Z_n(\cdot)\|_p^p &= E \int_0^1 |Z_n(t+h) - Z_n(t)|^p \, dt \\
&= E \int_0^{1-h} |Z_n(t+h) - Z_n(t)|^p \, dt + E \int_{1-h}^1 |Z_n(t)|^p \, dt
\end{aligned}$$

$$
\begin{aligned}
&= E\int_0^{1-h}\left|\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\left(I_{[0,t+h]}(U_i)-(t+h)\right)\right.\\
&\quad\left.-\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\left(I_{[0,t]}(U_i)-t\right)\right|^p dt\\
&\quad+E\int_{1-h}^{1}\left|\frac{1}{\sqrt{n}}\sum_{i=1}^{n}\left(I_{[0,t]}(U_i)-t\right)\right|^p dt\\
&= E\frac{1}{n^{p/2}}\int_0^{1-h}\left|\sum_{i=1}^{n}\left(I_{]t,t+h]}(U_i)-h\right)\right|^p dt\\
&\quad+E\frac{1}{n^{p/2}}\int_{1-h}^{1}\left|\sum_{i=1}^{n}\left(I_{[0,t]}(U_i)-t\right)\right|^p dt\\
&= \frac{1}{n^{p/2}}\int_0^{1-h}E\left|\sum_{i=1}^{n}(I_{]t,t+h]}(U_i)-h)\right|^p dt\\
&\quad+\frac{1}{n^{p/2}}\int_{1-h}^{1}E\left|\sum_{i=1}^{n}(I_{[0,t]}(U_i)-t)\right|^p dt\\
&\le \frac{1}{n^{p/2}}\int_0^{1-h}A_p^pE\left(\left(\sum_{i=1}^{n}(I_{]t,t+h]}(U_i)-h)^2\right)^{1/2}\right)^p dt\\
&\quad+\frac{1}{n^{p/2}}\int_{1-h}^{1}B_p^pE\left(\left(\sum_{i=1}^{n}(I_{[0,t]}(U_i)-t)^2\right)^{1/2}\right)^p dt\\
&= \frac{1}{n^{p/2}}\int_0^{1-h}A_p^pE\left(\sum_{i=1}^{n}(I_{]t,t+h]}(U_i)-h)^2\right)^{p/2} dt\\
&\quad+\frac{1}{n^{p/2}}\int_{1-h}^{1}B_p^pE\left(\sum_{i=1}^{n}(I_{[0,t]}(U_i)-t)^2\right)^{p/2} dt,
\end{aligned}
$$

where the used the Marcinkiewicz–Zygmund inequality, see Remark 2.1. We will distinguish two cases. In the first case $1 \le p \le 2$.

$$
\begin{aligned}
&\frac{1}{n^{p/2}}\int_0^{1-h}A_p^pE\left(\sum_{i=1}^{n}(I_{]t,t+h]}(U_i)-h)^2\right)^{p/2} dt\\
&\qquad+\frac{1}{n^{p/2}}\int_{1-h}^{1}B_p^pE\left(\sum_{i=1}^{n}(I_{[0,t]}(U_i)-t)^2\right)^{p/2} dt
\end{aligned}
$$

$$
\begin{aligned}
&\le \frac{1}{n^{p/2}} \int_0^{1-h} A_p^p \left(E \sum_{i=1}^n (I_{]t,t+h]}(U_i) - h)^2 \right)^{p/2} dt \\
&+ \frac{1}{n^{p/2}} \int_{1-h}^1 B_p^p \left(E \sum_{i=1}^n (I_{[0,t]}(U_i) - t)^2 \right)^{p/2} dt \\
&= \frac{A_p^p}{n^{p/2}} \int_0^{1-h} (E(\xi - nh)^2)^{p/2}\, dt + \frac{B_p^p}{n^{p/2}} \int_{1-h}^1 (E(\eta - nt)^2)^{p/2}\, dt \\
&= \frac{A_p^p}{n^{p/2}} \int_0^{1-h} (nh(1-h))^{p/2}\, dt + \frac{B_p^p}{n^{p/2}} \int_{1-h}^1 (nt(1-t))^{p/2}\, dt \\
&\le A_p^p h^{p/2} (1-h)^{\frac{p+2}{2}} + B_p^p \int_{1-h}^1 (t(1-t))^{p/2}\, dt \\
&\le A_p^p h^{p/2} (1-h)^{\frac{p+2}{2}} + B_p^p h^{\frac{p+2}{2}} \to 0, \qquad \text{as } h \to 0,
\end{aligned}
$$

where ξ is a binomial random variable with parameters h and n, and η is binomial with parameters t and n.

In the second case $2 < p < \infty$.

$$
\begin{aligned}
&\frac{1}{n^{p/2}} \int_0^{1-h} A_p^p E \left(\sum_{i=1}^n (I_{]t,t+h]}(U_i) - h)^2 \right)^{p/2} dt \\
&\quad + \frac{1}{n^{p/2}} \int_{1-h}^1 B_p^p E \left(\sum_{i=1}^n (I_{[0,t]}(U_i) - t)^2 \right)^{p/2} dt \\
&\quad \le \frac{A_p^p}{n^{p/2}} \int_0^{1-h} E \left(n^{\frac{p-2}{p}} \left(\sum_{i=1}^n |I_{]t,t+h]}(U_i) - h|^p \right)^{2/p} \right)^{p/2} dt \\
&\quad + \frac{B_p^p}{n^{p/2}} \int_{1-h}^1 E \left(n^{\frac{p-2}{p}} \left(\sum_{i=1}^n |I_{[0,t]}(U_i) - t|^p \right)^{2/p} \right)^{p/2} dt \\
&\quad = \frac{A_p^p}{n^{p/2}} n^{\frac{p-2}{2}} \int_0^{1-h} E \left(\sum_{i=1}^n |I_{]t,t+h]}(U_i) - h|^p \right) dt \\
&\quad + \frac{B_p^p}{n^{p/2}} n^{\frac{p-2}{2}} \int_{1-h}^1 E \left(\sum_{i=1}^n |I_{[0,t]}(U_i) - t|^p \right) dt \\
&\quad = \frac{A_p^p}{n} \int_0^{1-h} \sum_{i=1}^n E|I_{]t,t+h]}(U_i) - h|^p\, dt \\
&\quad + \frac{B_p^p}{n} \int_{1-h}^1 \sum_{i=1}^n E|I_{[0,t]}(U_i) - t|^p\, dt
\end{aligned}
$$

$$= A_p^p \int_0^{1-h} E|I_{]t,t+h]}(U_i) - h|^p \, dt + B_p^p \int_{1-h}^1 E|I_{[0,t]}(U_i) - t|^p \, dt$$
$$= A_p^p \int_0^{1-h} E|\xi - h|^p + B_p^p \int_{1-h}^1 E|\eta - t|^p$$
$$= A_p^p \left[(1-h)^{p+1}h + h^p(1-h)^2\right] + B_p^p \int_{1-h}^1 [(1-t)^p t + t^p(1-t)] \, dt$$
$$\leq A_p^p[(1-h)^{p+1}h + h^p(1-h)^2] + B_p^p \int_{1-h}^1 2dt$$
$$= A_p^p[(1-h)^{p+1}h + h^p(1-h)^2] + 2B_p^p h \to 0, \qquad \text{as } h \to 0,$$

where ξ is a Bernoulli random variable with parameter h and η is Bernoulli with parameter t. This completes the proof of the Proposition 3.1.

Theorem 3.1.
$$\frac{1}{\log n} \sum_{k=1}^n \frac{1}{k} \delta_{Z_k(\cdot,\omega)} \Rightarrow \mu_B,$$
in $L^p(]0,1[)$, as $n \to \infty$, for almost every $\omega \in \Omega$, where B is the Brownian bridge.

Proof. We shall prove that the conditions of Remark 2.4 are fulfilled.

The separability and completeness of $L^p(]0,1[)$ are well-known facts. Let us define the process

$$Z_{k,n}(t) = \frac{1}{\sqrt{n}} \sum_{i=1}^n (I_{[0,t]}(U_i) - t) - \frac{1}{\sqrt{n}} \sum_{i=1}^k (I_{[0,t]}(U_i) - t).$$

Then $Z_{k,n}$ and Z_k are independent for $k < n$.

We show that the condition (2) is valid.

$$E\rho(Z_n, Z_{k,n}) = E\left(\int_0^1 \left|\frac{1}{\sqrt{n}} \sum_{i=1}^k (I_{[0,t]}(U_i) - t)\right|^p dt\right)^{1/p}$$
$$= \frac{1}{\sqrt{n}} E\left(\int_0^1 \left|\sum_{i=1}^k (I_{[0,t]}(U_i) - t)\right|^p dt\right)^{1/p}$$
$$\leq \frac{1}{\sqrt{n}} \left(\int_0^1 E\left|\sum_{i=1}^k (I_{[0,t]}(U_i) - t)\right|^p dt\right)^{1/p}$$
$$\leq \frac{1}{\sqrt{n}} \left(\int_0^1 C_p^p E\left(\left(\sum_{i=1}^k (I_{[0,t]}(U_i) - t)^2\right)^{1/2}\right)^p dt\right)^{1/p}$$
$$\leq \frac{1}{\sqrt{n}} \left(\int_0^1 C_p^p E\left(\sum_{i=1}^k (I_{[0,t]}(U_i) - t)^2\right)^{p/2} dt\right)^{1/p},$$

where we used the Marcinkiewicz–Zygmund inequality, see Remark 2.1. We will distinguish two cases. In the first case $1 \le p \le 2$.

$$\frac{1}{\sqrt{n}}\left(\int_0^1 C_p^p E\left(\sum_{i=1}^k (I_{[0,t]}(U_i)-t)^2\right)^{p/2} dt\right)^{1/p}$$

$$\le \frac{C_p}{\sqrt{n}}\left(\int_0^1 \left(E\sum_{i=1}^k (I_{[0,t]}(U_i)-t)^2\right)^{p/2} dt\right)^{1/p}$$

$$= \frac{C_p}{\sqrt{n}}\left(\int_0^1 (E(\xi-kt)^2)^{p/2}\, dt\right)^{1/p}$$

$$= \frac{C_p}{\sqrt{n}}\left(\int_0^1 (kt(1-t))^{p/2}\, dt\right)^{1/p} = C^* \frac{\sqrt{k}}{\sqrt{n}},$$

where ξ has binomial distribution with parameters t and k.

In the second case $2 < p < \infty$.

$$\frac{1}{\sqrt{n}}\left(\int_0^1 C_p^p E\left(\sum_{i=1}^k (I_{[0,t]}(U_i)-t)^2\right)^{p/2} dt\right)^{1/p}$$

$$\le \frac{C_p}{\sqrt{n}}\left(\int_0^1 E\left(k^{\frac{p-2}{p}}\left(\sum_{i=1}^k |I_{[0,t]}(U_i)-t|^p\right)^{2/p}\right)^{p/2} dt\right)^{1/p}$$

$$= \frac{C_p}{\sqrt{n}}\left(\int_0^1 E\left(k^{\frac{p-2}{2}}\left(\sum_{i=1}^k |I_{[0,t]}(U_i)-t|^p\right)\right) dt\right)^{1/p}$$

$$= \frac{C_p}{\sqrt{n}}\left(\int_0^1 k^{\frac{p-2}{2}}\left(\sum_{i=1}^k E|I_{[0,t]}(U_i)-t|^p\right) dt\right)^{1/p}$$

$$= \frac{C_p}{\sqrt{n}}\left(\int_0^1 k^{p/2} E|\xi-t|^p\, dt\right)^{1/p}$$

$$= C_p\frac{\sqrt{k}}{\sqrt{n}}\left(\int_0^1 E|\xi-t|^p\, dt\right)^{1/p}$$

$$= C_p\frac{\sqrt{k}}{\sqrt{n}}\left(\int_0^1 [(1-t)^p t + (1-t)t^p]\, dt\right)^{1/p}$$

$$\le C_p\frac{\sqrt{k}}{\sqrt{n}} 2^{1/p} = C^* \frac{\sqrt{k}}{\sqrt{n}},$$

where ξ is a Bernoulli random variable with parameter t. This completes the proof of the Theorem 3.1.

References

[1] Berkes, I., Results and problems related to the pointwise central limit theorem. In: B. Szyszkowicz (Ed.) *Asymptotic results in probability and statistics*, Elsevier, Amsterdam (1998), 59–96.

[2] Berkes, I. and Csáki, E., A universal result in almost sure central limit theory *Stoch. Proc. Appl.* **94** no. 1 (2001), 105–134.

[3] Billingsley, P., *Convergence of Probability Measures*, John Wiley & Sons, New York, London, 1968.

[4] Brosamler, G. A., An almost everywhere central limit theorem *Math. Proc. Cambridge Philos. Soc.* **104** (1988), 561–574.

[5] Chow, Y. S. and Teicher, H., *Probability Theory*, Springer-Verlag, New York, Berlin, Heidelberg, London, Paris, Tokyo, 1988.

[6] Chuprunov, A. and Fazekas, I., Almost sure limit theorems for the Pearson statistic, *Technical Report no. 2001/6, University of Debrecen, Hungary.*

[7] Fazekas, I. and Rychlik, Z., Almost sure functional limit theorems, Technical Report no. 2001/11, University of Debrecen, Hungary. (submitted to Annales Universitas Maria Curie -Skodlodowska Lublin - Polonia, Vol.LVI,1, 2002).

[8] Grenander, U., *Probabilities on Algebraic Structures*, John Wiley & Sons, New York, London, 1963.

[9] Lacey, M. T. and Philipp, W., A note on the almost sure central limit theorem, *Statistics & Probability Letters* **9** no. 2 (1990), 201–205.

[10] Major, P., Almost sure functional limit theorems, Part I. The general case, *Studia Sci. Math. Hungar.* **34** (1998), 273–304.

[11] Major, P., Almost sure functional limit theorems, Part II. The case of independent random variables, *Studia Sci. Math. Hungar.* **36** (2000), 231–273.

[12] Oliveira, P. E. and Suquet, Ch., Weak convergence in $L^p]0,1[$ of the uniform empirical process under dependence, *Statistics & Probability Letters* **39** (1998), 363–370.

[13] Schatte, P., On strong versions of the central limit theorem, *Math. Nachr.* **137** (1998), 249–256.

[14] Túri, J., Almost sure functional limit theorems in $L^2(]0,1[)$, *Acta Math. Acad. Paed. Nyíregyh.* **18** (2002), 27–32.

József Túri
College of Nyíregyháza
Institute of Mathematics and Computer Sciences
P.O.Box 166
H-4400 Nyíregyháza, Hungary
E-mail: turij@nyf.hu

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 89–94*

ALMOST SURE CENTRAL LIMIT THEOREMS FOR m-DEPENDENT RANDOM FIELDS

Tibor Tómács (Eger, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. It is proved that the almost sure central limit theorem holds true for m-dependent random fields.

AMS Classification Number: 60 F 05, 60 F 15

1. Introduction

Let $\mathbf{N}$ be the set of the positive integers and $\mathbf{N}^d$ the positive integer d-dimensional lattice points, where d is a fixed positive integer. Denote $\mathbf{R}$ the set of real numbers and $\mathcal{B}$ the σ-algebra of Borel sets of $\mathbf{R}$. Let $\zeta_{\mathbf{n}}$, $\mathbf{n} \in \mathbf{N}^d$, be a multiindex sequence of random variables on the probability space $(\Omega, \mathcal{A}, \mathrm{P})$. Almost sure limit theorems in multiindex case state that

$$\frac{1}{D_{\mathbf{n}}} \sum_{\mathbf{k} \leq \mathbf{n}} d_{\mathbf{k}} \delta_{\zeta_{\mathbf{k}}(\omega)} \Rightarrow \mu, \text{ as } \mathbf{n} \to \infty, \text{ for almost every } \omega \in \Omega.$$

Here δ_x is the unit mass at point x, that is $\delta_x \colon \mathcal{B} \to \mathbf{R}$, $\delta_x(B) = 1$ if $x \in B$ and $\delta_x(B) = 0$ if $x \notin B$, moreover $\Rightarrow \mu$ denotes weak convergence to the probability measure μ. Theorems of this type are not direct consequences of the corresponding theorems for ordinary sequences.

In this paper $\mathbf{k} = (k_1, \dots, k_d), \mathbf{n} = (n_1, \dots, n_d), \dots \in \mathbf{N}^d$. Relations $\leq$, $\not\leq$, min, $\to$ etc. are defined coordinatewise, i.e. $\mathbf{n} \to \infty$ means that $n_i \to \infty$ for all $i \in \{1, \dots, d\}$. Let $|\mathbf{n}| = \prod_{i=1}^{d} n_i$ and $|\log \mathbf{n}| = \prod_{i=1}^{d} \log_+ n_i$, where $\log_+ x = \log x$ if $x \geq e$ and $\log_+ x = 1$ if $x < e$.

In the multiindex version of the classical almost sure limit theorem $\zeta_{\mathbf{n}} = \frac{1}{\sqrt{|\mathbf{n}|}} \sum_{\mathbf{k} \leq \mathbf{n}} X_{\mathbf{k}}$, where $X_{\mathbf{k}}$, $\mathbf{k} \in \mathbf{N}^d$, are independent identically distributed random variables with expectation $\mathrm{E} X_{\mathbf{k}} = 0$ and variance $\mathrm{D}^2 X_{\mathbf{k}} = 1$, moreover $d_{\mathbf{k}} = \frac{1}{|\mathbf{k}|}$, $D_{\mathbf{n}} = |\log \mathbf{n}|$, finally μ is the standard normal distribution $\mathcal{N}(0,1)$. (See [2] in multiindex case, while [1] and [3] for single index case.)

We shall prove a similar proposition, but in so-called m-dependent case. For this purpose we need the next known theorems and lemmas.

Theorem 1.1. *Assume that for any pair* $\mathbf{h},\mathbf{l}\in\mathbf{N}^d$, $\mathbf{h}\le\mathbf{l}$ *there exists a random variable* $\zeta_{\mathbf{h},\mathbf{l}}$ *with the following properties.* $\zeta_{\mathbf{h},\mathbf{l}}=0$ *if* $\mathbf{h}=\mathbf{l}$. *If* $\mathbf{k},\mathbf{l}\in\mathbf{N}^d$, *then for* $\mathbf{h}=\min\{\mathbf{k},\mathbf{l}\}$ *we suppose that the following pairs of random variables are independent:* $\zeta_{\mathbf{k}}$ *and* $\zeta_{\mathbf{h},\mathbf{l}}$; $\zeta_{\mathbf{l}}$ *and* $\zeta_{\mathbf{h},\mathbf{k}}$; $\zeta_{\mathbf{h},\mathbf{k}}$ *and* $\zeta_{\mathbf{h},\mathbf{l}}$. *Assume that there exist* $c>0$ *and* $\mathbf{n}_0\in\mathbf{N}^d$ *such that* $E(\zeta_{\mathbf{l}}-\zeta_{\mathbf{h},\mathbf{l}})^2\le c|\mathbf{h}|/|\mathbf{l}|$ *for all* $\mathbf{n}_0\le\mathbf{h}\le\mathbf{l}$, $\mathbf{h},\mathbf{l}\in\mathbf{N}^d$.

Let $0\le d_k^{(i)}\le c\log\frac{k+1}{k}$, *assume that* $\sum\limits_{k=1}^{\infty}d_k^{(i)}=\infty$ *for* $i\in\{1,\dots,d\}$. *Let* $d_{\mathbf{k}}=\prod\limits_{i=1}^{d}d_{k_i}^{(i)}$ *and* $D_{\mathbf{n}}=\sum\limits_{\mathbf{k}\le\mathbf{n}}d_{\mathbf{k}}$. *Then for any probability distribution* μ *the following two statements are equivalent*

$$\frac{1}{D_{\mathbf{n}}}\sum_{\mathbf{k}\le\mathbf{n}}d_{\mathbf{k}}\delta_{\zeta_{\mathbf{k}}(\omega)}\Rightarrow\mu,\ \textit{as}\ \mathbf{n}\to\infty,\ \textit{for almost every}\ \omega\in\Omega;$$

$$\frac{1}{D_{\mathbf{n}}}\sum_{\mathbf{k}\le\mathbf{n}}d_{\mathbf{k}}\mu_{\zeta_{\mathbf{k}}}\Rightarrow\mu,\ \textit{as}\ \mathbf{n}\to\infty,$$

where $\mu_{\zeta_{\mathbf{k}}}$ *denotes the distribution of the* $\zeta_{\mathbf{k}}$.

Proof. Choose in [2], Theorem 2.1 and Remark 2.2, $B=\mathbf{R}$, $\varrho(x,y)=|x-y|$, $c_n^{(i)}=n$ and $\beta=1$.

Let $X_{\mathbf{n}}$, $\mathbf{n}\in\mathbf{N}^d$, be a multiindex sequence of random variables on the probability space $(\Omega,\mathcal{A},\mathrm{P})$. Suppose that $\mathrm{E}X_{\mathbf{n}}=0$ and $\mathrm{D}^2X_{\mathbf{n}}<\infty$ for all $\mathbf{n}\in\mathbf{N}^d$. Let $||\mathbf{n}||=\max\{n_1,\dots,n_d\}$ and $d(V_1,V_2)=\inf\{||\mathbf{n}-\mathbf{m}||:\mathbf{n}\in V_1,\mathbf{m}\in V_2\}$, where $V_1,V_2\subset\mathbf{N}^d$. Let $\sigma(V)$, where $V\subset\mathbf{N}^d$, be the smallest σ-algebra with respect to which $\{X_{\mathbf{n}},\mathbf{n}\in V\}$ are measurable.

Definition 1.2. Let $m\in\mathbf{N}$ be fixed. The random field $\{X_{\mathbf{n}},\mathbf{n}\in\mathbf{N}^d\}$ is said to be m-dependent if the σ-algebras $\sigma(V_1)$ and $\sigma(V_2)$ are independent whenever $d(V_1,V_2)>m$, $V_1,V_2\subset\mathbf{N}^d$.

In the following let $S_{\mathbf{n}}=\sum\limits_{\mathbf{k}\le\mathbf{n}}X_{\mathbf{k}}$, $B_{\mathbf{n}}=\mathrm{D}^2S_{\mathbf{n}}$, $\zeta_{\mathbf{n}}=S_{\mathbf{n}}/\sqrt{B_{\mathbf{n}}}$ and let $\mu_{\zeta_{\mathbf{n}}}$ denote the distribution of the random variable $\zeta_{\mathbf{n}}$.

Lemma 1.3. *Let* $\{X_{\mathbf{n}},\mathbf{n}\in\mathbf{N}^d\}$ *be an* m*-dependent random field,* $EX_{\mathbf{n}}=0$, $\mathbf{n}\in\mathbf{N}^d$. *Assume that*

(1.1) *there exist* $M,\delta\in\mathbf{R}$ *such that* $E|X_{\mathbf{n}}|^{2+\delta}\le M<\infty$ *for all* $\mathbf{n}\in\mathbf{N}^d$,

for some $\delta\ge0$. *Then there exists constant* $C_\delta>0$ *such that*

$$E|S_{\mathbf{n}}|^{2+\delta}\le C_\delta|\mathbf{n}|^{\frac{2+\delta}{2}}$$

for all $\mathbf{n} \in \mathbf{N}^d$.

Proof. See [4], Lemma 5.

Lemma 1.4. *Let* $\mu, \mu_{\mathbf{n}}$, $\mathbf{n} \in \mathbf{N}^d$, *be distributions with* $\mu_{\mathbf{n}} \Rightarrow \mu$, *as* $\mathbf{n} \to \infty$. *Let* $d_{\mathbf{k}}$, $\mathbf{k} \in \mathbf{N}^d$, *be a nonidentically zero sequence of nonnegative real numbers. Assume that for each fixed* $\mathbf{n}_0 \in \mathbf{N}^d$,

$$\frac{1}{\sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}} \sum_{\mathbf{k}\in A_{\mathbf{n}_0}} d_{\mathbf{k}} \to 0, \ \textit{as } \mathbf{n} \to \infty,$$

where $A_{\mathbf{n}_0} = \{\mathbf{k} \in \mathbf{N}^d : \mathbf{k} \le \mathbf{n} \textit{ and } \mathbf{k} \not\ge \mathbf{n}_0\}$. *Then*

$$\frac{1}{\sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}} \sum_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}\mu_{\mathbf{k}} \Rightarrow \mu, \ \textit{as } \mathbf{n} \to \infty.$$

Proof. Let $f\colon \mathbf{R} \to \mathbf{R}$ be a bounded and continuous function. Then for $\varepsilon > 0$ there exists $\mathbf{n}_\varepsilon \in \mathbf{N}^d$ such that for $\mathbf{n} \ge \mathbf{n}_\varepsilon$

$$\left|\int f \mathrm{d}\mu_{\mathbf{n}} - \int f \mathrm{d}\mu\right| < \frac{\varepsilon}{2} \quad \text{and} \quad \frac{1}{\sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}} \sum_{\mathbf{k}\in A_{\mathbf{n}_\varepsilon}} d_{\mathbf{k}} < \frac{\varepsilon}{2K},$$

where $\left|\int f \mathrm{d}\mu_{\mathbf{n}} - \int f \mathrm{d}\mu\right| \le K < \infty$. Let $\gamma_{\mathbf{n}} = \sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}\mu_{\mathbf{k}} \Big/ \sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}$. Then

$$\begin{aligned}\left|\int f \mathrm{d}\gamma_{\mathbf{n}} - \int f \mathrm{d}\mu\right| \le{} & \frac{1}{\sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}} \sum_{\mathbf{k}\in A_{\mathbf{n}_\varepsilon}} d_{\mathbf{k}} \left|\int f \mathrm{d}\mu_{\mathbf{k}} - \int f \mathrm{d}\mu\right| \\ & + \frac{1}{\sum\limits_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}} \sum_{\mathbf{n}_\varepsilon\le\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}} \left|\int f \mathrm{d}\mu_{\mathbf{k}} - \int f \mathrm{d}\mu\right| < \varepsilon,\end{aligned}$$

which implies Lemma 1.4.

It is easy to see that the conditions of Lemma 1.4 are satisfied for $d_{\mathbf{k}} = \frac{1}{|\mathbf{k}|}$. The next proposition is a central limit theorem for m-dependent random fields.

Theorem 1.5. *Let* $\{X_{\mathbf{n}}, \mathbf{n} \in \mathbf{N}^d\}$ *be an* m*-dependent random field,* $EX_{\mathbf{n}} = 0$, $\mathbf{n} \in \mathbf{N}^d$. *Assume that (1.1) holds for some* $\delta > 0$ *and*

(1.2) *there exist* $\sigma > 0$ *and* $\mathbf{n}_\sigma \in \mathbf{N}^d$ *such that* $\dfrac{B_{\mathbf{n}}}{|\mathbf{n}|} \ge \sigma$ *for all* $\mathbf{n} \ge \mathbf{n}_\sigma$.

Then

$$\mu_{\zeta_{\mathbf{n}}} \Rightarrow \mathcal{N}(0,1) \text{ as } \mathbf{n} \to \infty.$$

Proof. It is a simple corollary of [4], Theorem 1.

2. Results

Theorem 2.1. *Let $\{X_{\mathbf{n}}, \mathbf{n} \in \mathbf{N}^d\}$ be an m-dependent random field, $EX_{\mathbf{n}} = 0$, $\mathbf{n} \in \mathbf{N}^d$. Suppose that* (1.1) *and* (1.2) *hold for some $\delta \geq 0$. Let $0 \leq d_k^{(i)} \leq c \log \frac{k+1}{k}$, assume that $\sum_{k=1}^{\infty} d_k^{(i)} = \infty$ for $i \in \{1,\dots,d\}$. Let $d_{\mathbf{k}} = \prod_{i=1}^{d} d_{k_i}^{(i)}$ and $D_{\mathbf{n}} = \sum_{\mathbf{k}\leq\mathbf{n}} d_{\mathbf{k}}$. Then for any probability distribution μ the following two statements are equivalent*

$$\frac{1}{D_{\mathbf{n}}} \sum_{\mathbf{k}\leq\mathbf{n}} d_{\mathbf{k}} \delta_{\zeta_{\mathbf{k}}(\omega)} \Rightarrow \mu, \text{ as } \mathbf{n} \to \infty, \text{ for almost every } \omega \in \Omega;$$

$$\frac{1}{D_{\mathbf{n}}} \sum_{\mathbf{k}\leq\mathbf{n}} d_{\mathbf{k}} \mu_{\zeta_{\mathbf{k}}} \Rightarrow \mu, \text{ as } \mathbf{n} \to \infty.$$

Proof. Let $\mathbf{h}, \mathbf{l} \in \mathbf{N}^d$, $\mathbf{h} \leq \mathbf{l}$, $\mathbf{m} = (m,\dots,m) \in \mathbf{N}^d$, $V_{\mathbf{l}} = \{\mathbf{t} \in \mathbf{N}^d : \mathbf{t} \leq \mathbf{l}\}$, $V_{\mathbf{h},\mathbf{l}} = \{\mathbf{t} \in \mathbf{N}^d : \mathbf{t} \leq \mathbf{l} \text{ and } \mathbf{t} \not\leq \mathbf{h}+\mathbf{m}\}$, $\zeta_{\mathbf{h},\mathbf{l}} = \frac{1}{\sqrt{B_{\mathbf{l}}}} \sum_{\mathbf{t}\in V_{\mathbf{h},\mathbf{l}}} X_{\mathbf{t}}$. Let us verify in this case the assumptions of Theorem 1.1.

(I) $\zeta_{\mathbf{l},\mathbf{l}} = 0$ because $V_{\mathbf{l},\mathbf{l}} = \emptyset$.

(II) Let $\mathbf{k}, \mathbf{l} \in \mathbf{N}^d$ and $\mathbf{h} = \min\{\mathbf{k}, \mathbf{l}\}$. Then

$$\zeta_{\mathbf{k}} \text{ is } \sigma(V_{\mathbf{k}})\text{-measurable}, \quad \zeta_{\mathbf{l}} \text{ is } \sigma(V_{\mathbf{l}})\text{-measurable},$$

$$\zeta_{\mathbf{h},\mathbf{l}} \text{ is } \sigma(V_{\mathbf{h},\mathbf{l}})\text{-measurable if } V_{\mathbf{h},\mathbf{l}} \neq \emptyset, \text{ otherwise } \zeta_{\mathbf{h},\mathbf{l}} = 0,$$

$$\zeta_{\mathbf{h},\mathbf{k}} \text{ is } \sigma(V_{\mathbf{h},\mathbf{k}})\text{-measurable if } V_{\mathbf{h},\mathbf{k}} \neq \emptyset, \text{ otherwise } \zeta_{\mathbf{h},\mathbf{k}} = 0,$$

$$d(V_{\mathbf{k}}, V_{\mathbf{h},\mathbf{l}}) > m \text{ if } V_{\mathbf{h},\mathbf{l}} \neq \emptyset,$$

$$d(V_{\mathbf{l}}, V_{\mathbf{h},\mathbf{k}}) > m \text{ if } V_{\mathbf{h},\mathbf{k}} \neq \emptyset,$$

$$d(V_{\mathbf{h},\mathbf{k}}, V_{\mathbf{h},\mathbf{l}}) > m \text{ if } V_{\mathbf{h},\mathbf{k}} \neq \emptyset \text{ and } V_{\mathbf{h},\mathbf{l}} \neq \emptyset.$$

Thus the following pairs of random variables are independent: $\zeta_{\mathbf{k}}$ and $\zeta_{\mathbf{h},\mathbf{l}}$; $\zeta_{\mathbf{l}}$ and $\zeta_{\mathbf{h},\mathbf{k}}$; $\zeta_{\mathbf{h},\mathbf{k}}$ and $\zeta_{\mathbf{h},\mathbf{l}}$.

(III) By Lyapunov's inequality, $(\mathrm{E}|\xi|^s)^{1/s} \le (\mathrm{E}|\xi|^t)^{1/t}$ if $0 < s \le t$. (See it for example in [5].) Thus we have

$$\mathrm{E}S^2_{\mathbf{h}+\mathbf{m}} \le (\mathrm{E}|S_{\mathbf{h}+\mathbf{m}}|^{2+\delta})^{\frac{2}{2+\delta}}.$$

By Lemma 1.3,

$$\mathrm{E}S^2_{\mathbf{h}+\mathbf{m}} \le \left(c_1|\mathbf{h}+\mathbf{m}|^{\frac{2+\delta}{2}}\right)^{\frac{2}{2+\delta}} = c_2|\mathbf{h}+\mathbf{m}|. \tag{2.1}$$

Let $\mathbf{h}, \mathbf{l} \in \mathbf{N}^d$ such that $\max\{\mathbf{m}, \mathbf{n}_\sigma\} \le \mathbf{h} \le \mathbf{l}$. Then $\mathbf{m} \le \mathbf{h}$ and (2.1) imply that

$$\mathrm{E}(\zeta_{\mathbf{l}} - \zeta_{\mathbf{h},\mathbf{l}})^2 = \mathrm{E}\left(\frac{1}{\sqrt{B_{\mathbf{l}}}} S_{\mathbf{h}+\mathbf{m}}\right)^2 = \frac{1}{B_{\mathbf{l}}}\mathrm{E}S^2_{\mathbf{h}+\mathbf{m}} \le \frac{c_2}{B_{\mathbf{l}}}|\mathbf{h}+\mathbf{m}|. \tag{2.2}$$

Since $\mathbf{l} \ge \mathbf{n}_\sigma$ thus, by assumption (1.2), $\frac{1}{B_{\mathbf{l}}} \le \frac{1}{\sigma|\mathbf{l}|}$. So (2.2) implies that

$$\mathrm{E}(\zeta_{\mathbf{l}} - \zeta_{\mathbf{h},\mathbf{l}})^2 \le \frac{c_2}{\sigma}\frac{|\mathbf{h}+\mathbf{m}|}{|\mathbf{l}|} = c_3\frac{\prod_{i=1}^{d}(h_i+m)}{|\mathbf{l}|} \le 2^d c_3 \frac{|\mathbf{h}|}{|\mathbf{l}|} = c_4\frac{|\mathbf{h}|}{|\mathbf{l}|}.$$

Therefore random variables $\zeta_{\mathbf{l}}$ and $\zeta_{\mathbf{h},\mathbf{l}}$ satisfy the conditions of Theorem 1.1, which implies Theorem 2.1.

Theorem 2.2. *Let $\{X_{\mathbf{n}}, \mathbf{n} \in \mathbf{N}^d\}$ be an m-dependent random field, $EX_{\mathbf{n}} = 0$, $\mathbf{n} \in \mathbf{N}^d$. Assume that* (1.1) *and* (1.2) *hold for some $\delta > 0$. Then*

$$\frac{1}{|\log \mathbf{n}|}\sum_{\mathbf{k}\le\mathbf{n}}\frac{1}{|\mathbf{k}|}\delta_{\zeta_{\mathbf{k}}(\omega)} \Rightarrow \mathcal{N}(0,1), \text{ as } \mathbf{n}\to\infty, \text{ for almost every } \omega \in \Omega.$$

Proof. Let $d_k^{(i)} = \frac{1}{k}$, $k \in \mathbf{N}$, $i \in \{1,\dots,d\}$. The conditions of Theorem 2.1 are satisfied, because $2 \le \left(1+\frac{1}{k}\right)^k$, so $\frac{1}{k} \le \frac{1}{\log 2}\log\frac{k+1}{k}$, moreover $\sum_{k=1}^{\infty}\frac{1}{k} = \infty$. Then $d_{\mathbf{k}} = \frac{1}{|\mathbf{k}|}$ and

$$D_{\mathbf{n}} = \sum_{\mathbf{k}\le\mathbf{n}}\prod_{i=1}^{d}\frac{1}{k_i} = \prod_{i=1}^{d}\sum_{k_i=1}^{n_i}\frac{1}{k_i} \sim \prod_{i=1}^{d}\log n_i \sim |\log \mathbf{n}|, \tag{2.3}$$

where $a_{\mathbf{n}} \sim b_{\mathbf{n}}$ if $a_{\mathbf{n}}/b_{\mathbf{n}} \to 1$, as $\mathbf{n}\to\infty$. By Theorem 1.5, $\mu_{\zeta_{\mathbf{n}}} \Rightarrow \mathcal{N}(0,1)$, as $\mathbf{n}\to\infty$. Therefore Lemma 1.4 implies that

$$\frac{1}{D_{\mathbf{n}}}\sum_{\mathbf{k}\le\mathbf{n}} d_{\mathbf{k}}\mu_{\zeta_{\mathbf{k}}} = \frac{1}{\sum_{\mathbf{k}\le\mathbf{n}}\frac{1}{|\mathbf{k}|}}\sum_{\mathbf{k}\le\mathbf{n}}\frac{1}{|\mathbf{k}|}\mu_{\zeta_{\mathbf{k}}} \Rightarrow \mathcal{N}(0,1), \text{ as } \mathbf{n}\to\infty.$$

Now using Theorem 2.1, we obtain

$$\frac{1}{\sum\limits_{\mathbf{k}\le\mathbf{n}}\frac{1}{|\mathbf{k}|}}\sum_{\mathbf{k}\le\mathbf{n}}\frac{1}{|\mathbf{k}|}\delta_{\zeta_{\mathbf{k}}(\omega)}\Rightarrow\mathcal{N}(0,1),\ \text{as } \mathbf{n}\to\infty,\ \text{for almost every } \omega\in\Omega.$$

This fact and (2.3) imply Theorem 2.2.

References

[1] Berkes, I., Results and problems related to the pointwise central limit theorem, In: Szyszkowicz, B. (Ed.) *Asymptotic results in probability and statistics*, Elsevier, Amsterdam, (1998), 59–96.

[2] Fazekas, I., Rychlik, Z., Almost sure central limit theorems for random fields, *Technical Report No. 2001/12, University of Debrecen, Hungary* (submitted to Math. Nachr.).

[3] Fazekas, I., Rychlik, Z., Almost sure functional limit theorems, *Technical Report No. 2001/11, University of Debrecen, Hungary* (submitted to Annales Universitas Maria Curie -Skodlodowska Lublin - Polonia, Vol.LVI,1, 2002.)

[4] Prakasa Rao, B. L. S., A non-uniform estimate of the rate of convergence in the central limit theorem for m-dependent random fields, *Z. Wahrscheinlichkeitstheorie verw. Gebiete* **58** (1981), 247–256.

[5] Shiryayev, A. N., *Probability,* Springer-Verlag New York Inc. (1984).

Tibor Tómács
Department of Mathematics
Károly Eszterházy College
H-3301, Eger, P. O. Box 43.
Hungary
E-mail: tomacs@ektf.hu

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 95–103*

GENERATED PREORDERS AND EQUIVALENCES

Tamás Glavosits (Debrecen, Hungary)

Dedicated to the memory of Professor Péter Kiss

Abstract. For any relation R, we denote by R^* and $R^\bullet$ the smallest preorder and equivalence containing R, respectively. We establish some basic properties of the closures R^* and $R^\bullet$. Moreover, we provide some new characterizations of equivalences in terms of generated preorders.

The results obtained naturally supplement some former statements of Árpád Száz on preorders and equivalences. Moreover, they can be applied to relators (relational systems). Namely, each topology can be derived from a preorder relator. Moreover, equivalence relators also frequently occur in the applications.

1. Preorders, equivalences and closures

A subset R of a product set X^2 is called a relation on X. In particular, the relation $\Delta_X = \{(x,\, x) : \ x \in X\}$ is called the identity relation on X. Moreover, the relation $R^{-1} = \{(y,\, x) : \ (x,\, y) \in R\}$ is called the inverse of R.

Furthermore, if R and S are relations on X, then the relation $S \circ R = \big\{(x,\, z) : \ \exists\ y \in X : \ (x,\, y) \in R\,, \ (y,\, z) \in S\big\}$ is called the composition of S and R. In particular, we write $R^n = R \circ R^{n-1}$ for all $n \in N$ by agreeing that $R^0 = \Delta_X$.

A relation R on X is called reflexive, symmetric, and transitive if $\Delta_X \subset R$, $R^{-1} \subset R$ and $R^2 \subset R$, respectively. Moreover, a reflexive and transitive relation is called a preorder, and a symmetric preorder is called an equivalence.

Thus, we have $R^{-1} = R$ if R is a symmetric relation, and $R^2 = R$ if R is a preorder. Moreover, by using the above definitions, we can also easily prove the following basic characterization theorems.

Theorem 1.1. *If R is a relation on X, then the following assertions are equivalent:* (1) *R is a preorder (equivalence);* (2) *R^{-1} is a preorder (equivalence).*

Theorem 1.2. *If R is a relation on X, then the following assertions are equivalent:* (1) *R is a preorder;* (2) *$\Delta_X \cup R^2 \subset R$;* (3) *$\Delta_X \cup R^2 = R$.*

Remark 1.3. In [10], it was proved that R is a preorder if and only if $R = \big(R^{-1} \circ R^c\big)^c$, where $R^c = X^2 \setminus R$.

Theorem 1.4. *If R is a relation on X, then the following assertions are equivalent:* (1) *R is an equivalence;* (2) $\Delta_X \cup R \circ R^{-1} \subset R$; (3) $\Delta_X \cup R \circ R^{-1} = R$.

Remark 1.5. In the above theorem, by Theorem 1.1, we may write $R^{-1} \circ R$ in place of $R \circ R^{-1}$.

In [10], it was proved that if $R(x) \neq \emptyset$ for all $x \in X$, then R is an equivalence if and only if $R = R^{-1} \circ R$.

Definition 1.6. A function $^-$ of the power set $\mathcal{P}(X)$ into itself is called an algebraic closure [1, p. 111] on $\mathcal{P}(X)$ if

(1) $A \subset B$ implies $A^- \subset B^-$ for all $A, B \subset X$;

(2) $A \subset A^-$ for all $A \subset X$; (3) $A^- = \left(A^-\right)^-$ for all $A \subset X$.

The following characterization theorem could have already been established in [2]. However, it was later stressed only in [7] and [11].

Theorem 1.7. *If $^-$ is a function of $\mathcal{P}(X)$ into itself, then the following assertions are equivalent:*

(1) *the function $^-$ is a closure on $\mathcal{P}(X)$,*

(2) *for any $A, B \subset X$, we have $A \subset B^-$ if and only if $A^- \subset B^-$.*

Remark 1.8. If $^-$ is a closure on X, then we have $A^- \cup B^- \subset (A \cup B)^-$ for all $A, B \subset X$.

However, the corresponding equality is not, in general, true. Therefore, an algebraic closure need not be a topological closure [3, p. 43].

2. Basic properties of generated preorders

Theorem 2.1. *If $\mathcal{R}$ is a family of preorders on X, then $S = \bigcap \mathcal{R}$ is also a preorder on X.*

Hint. To prove the transitivity of S, note that $S^2 \subset R^2 \subset R$ for all $R \in \mathcal{R}$, and thus $S^2 \subset \bigcap \mathcal{R} = \mathcal{S}$.

Theorem 2.2. *If R is a relation on X, then there exists a smallest preorder R^* on X such that $R \subset R^*$.*

Proof. To prove this, denote by $\mathcal{R}$ the family of all preorders on X containing R, and define $R^* = \bigcap \mathcal{R}$.

Theorem 2.3. *If R is a relation on X, then the following assertions are equivalent:* (1) *R is a preorder;* (2) $R^* \subset R$; (3) $R^* = R$.

Proof. If the assertion (1) holds, then because of the inclusion $R \subset R$ and Theorem 2.2, the assertion (2) also holds. The implications (2)$\Longrightarrow$(3)$\Longrightarrow$(1) are even more obvious by Theorem 2.2.

Theorem 2.4. *The mapping* $R \mapsto R^*$ *is an algebraic closure on* $\mathcal{P}(X^2)$.

Proof. If $R, S \subset X^2$ such that $R \subset S^*$, then by Theorem 2.2 it is clear that $R^* \subset S^*$.

While, if $R^* \subset S^*$, then again by Theorem 2.2, it clear that $R \subset S^*$. Thus, by Theorem 1.7, the required assertion is also true.

Remark 2.5. By the above theorem, we have $R^* \cup S^* \subset (R \cup S)^*$ for all $R, S \subset X^2$.

The following example shows that the corresponding equality need not be true. Therefore, the mapping considered in Theorem 2.4 is not, in general, a topological closure.

Example 2.6. If $X = \{1, 2, 3\}$, and $R = \{(1, 2)\}$ and $S = \{(2, 3)\}$, then it can be easily seen that $(R \cup S)^* \setminus \big(R^* \cup S^*\big) = \{(1, 3)\}$.

Theorem 2.7. *If* R *is a relation on* X, *then*

$$\big(R^*\big)^{-1} = \big(R^{-1}\big)^*.$$

Proof. Since $R^{-1} \subset (R^*)^{-1}$ and $(R^*)^{-1}$ is also a preorder, we evidently have $\big(R^{-1}\big)^* \subset (R^*)^{-1}$. Hence, by writing R^{-1} in place of R, we can infer that $R^* \subset \big(\big(R^{-1}\big)^*\big)^{-1}$, and thus $(R^*)^{-1} \subset \big(R^{-1}\big)^*$ is also true.

Corollary 2.8. *If* R *is a symmetric relation on* X, *then* R^* *is an equivalence.*

Proof. In this case, by Theorem 2.7, we have $\big(R^*\big)^{-1} = \big(R^{-1}\big)^* = R^*$, and thus the preorder R^* is also symmetric.

The following example shows that the converse of the above corollary need not be true.

Example 2.9. If $X = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3), (3, 1)\}$, then $R^* = X^2$ is an equivalence despite that R is not symmetric.

Theorem 2.10. *If* R *is a relation on* X, *then*

$$R^* = \bigcup_{n=0}^{\infty} R^n.$$

Proof. By Theorem 2.2, it is clear that

$$S=\bigcup_{n=0}^{\infty} R^{\,n} \subset \bigcup_{n=0}^{\infty} (R^{*})^{n} \subset \bigcup_{n=0}^{\infty} R^{*} = R^{*}.$$

Moreover, it can be easily seen that

$$S\circ S=\left(\bigcup_{n=0}^{\infty} R^{n}\right)\circ\left(\bigcup_{m=0}^{\infty} R^{m}\right) \subset \bigcup_{n=0}^{\infty}\bigcup_{m=0}^{\infty} R^{n+m} \subset \bigcup_{k=0}^{\infty} R^{k} = S\,.$$

Now, it is clear that S is a preorder on X containing R. Therefore, by Theorem 2.2, the inclusion $R^{*}\subset S$ is also true.

The above theorem allows an easy computation of the preorder hull R^{*} of a relation R.

Example 2.11. If $X=\{1,2,3,4\}$ and $R=\{(2,1),(3,2),(4,1),(4,3)\}$, then it can be easily seen that $R^{2}=\{(3,1),(4,2)\}$, $R^{3}=\{(4,1)\}$ and $R^{4}=\emptyset$. Therefore, by Theorem 2.10, $R^{*}=\Delta_X\cup R\cup R^{2}$.

Remark 2.12. Because of Theorem 2.10, one may naturally write R^{∞} in place of R^{*}.

3. Basic properties of generated equivalences

Analogously to the corresponding results of Section 2, we can also easily establish the following theorems.

Theorem 3.1. *If $\mathcal{R}$ is a family of equivalences on X, then $S=\bigcap\mathcal{R}$ is also an equivalence on X.*

Theorem 3.2. *If R is a relation on X, then there exists a smallest equivalence $R^{\bullet}$ on X such that $R\subset R^{\bullet}$.*

Theorem 3.3. *If R is a relation on X, then the following assertions are equivalent:*

(1) *R is an equivalence;* (2) $R^{\bullet}\subset R$; (3) $R=R^{\bullet}$.

Theorem 3.4. *The mapping $R\mapsto R^{\bullet}$ is an algebraic closure on $\mathcal{P}(X^{2})$.*

Remark 3.5. By the above theorem, we have $R^{\bullet}\cup S^{\bullet}\subset(R\cup S)^{\bullet}$ for all $R,S\subset X^{2}$.

The following example shows that the corresponding equality need not be true. Therefore, the mapping considered in Theorem 3.4 is not, in general, a topological closure.

Example 3.6. It can be easily seen that, under the notations of Example 2.6, we have $(R \cup S)^\bullet \setminus \left(R^\bullet \cup S^\bullet\right) = \{(1, 3), (3, 1)\}$.

Theorem 3.7. *If R is a relation on X, then*

$$R^\bullet = \left(R^\bullet\right)^{-1} = \left(R^{-1}\right)^\bullet.$$

Proof. By Theorem 3.2, it is clear that $R^{-1} \subset (R^\bullet)^{-1} = R^\bullet$. Hence, by Theorem 3.4, it follows that $\left(R^{-1}\right)^\bullet \subset \left(R^\bullet\right)^\bullet = R^\bullet$. Now, by writing R^{-1} in place of R, we can at once see that the converse inclusion is also true.

Theorem 3.8. *If R is a relation on X, then $R^* \subset R^\bullet$.*

Proof. By Theorem 3.2, $R^\bullet$ is, in particular, a preorder containing R. Therefore, by Theorem 2.2, the required inclusion is also true.

Corollary 3.9. *If R is a symmetric relation on X, then $R^* = R^\bullet$.*

Proof. In this case, by Corollary 2.8 and Theorem 2.2, R^* is an equivalence containing R. Thus, by Theorem 3.2, $R^\bullet \subset R^*$. Moreover, by Theorem 3.8, the converse inclusion is always true.

Remark 3.10. From Example 2.9, we can see that the converse of the above corollary need not be true.

Theorem 3.11. *If R is a relation on X, then*

$$R^\bullet = \left(R^\bullet\right)^* = \left(R^*\right)^\bullet.$$

Proof. By Theorems 3.2 and 2.3, it is clear that $\left(R^\bullet\right)^* = R^\bullet$. On the other hand, since $R \subset R^* \subset \left(R^*\right)^\bullet$ and $\left(R^*\right)^\bullet$ is an equivalence on X, it is clear that $R^\bullet \subset \left(R^*\right)^\bullet$. Moreover, since $R^* \subset R^\bullet$ and $R^\bullet$ is an equivalence on X, it is clear that $\left(R^*\right)^\bullet \subset R^\bullet$ is also true.

Theorem 3.12. *If R is a relation on X, then*

$$R^\bullet = \left(R \cup R^{-1}\right)^*.$$

Proof. By Theorem 3.4 and Corollary 3.9, it is clear that $R^\bullet \subset \left(R \cup R^{-1}\right)^\bullet = \left(R \cup R^{-1}\right)^*$.

Moreover, by Theorem 3.2, it is clear that $R \cup R^{-1} \subset R^\bullet \cup \left(R^\bullet\right)^{-1} = R^\bullet$. Hence, by Theorems 3.4 and 3.11, it follows that $\left(R \cup R^{-1}\right)^* \subset \left(R^\bullet\right)^* = R^\bullet$.

Remark 3.13. Concernig the intersection $R \cap R^{-1}$, we can only state that $\left(R \cap R^{-1}\right)^{*} = \left(R \cap R^{-1}\right)^{\bullet} \subset R^{\bullet}$.

Namely, the following example shows that the corresponding equality need not be true.

Example 3.14. If $X = \{1, 2\}$ and $R = \{(1, 2)\}$, then $R^{\bullet} \setminus \left(R \cap R^{-1}\right)^{*} = R \cup R^{-1}$.

Now, in contrast to Example 3.6, we can also prove the following

Theorem 3.15. *If R is a relation on X, then*

$$\left(R \cup R^{-1}\right)^{\bullet} = R^{\bullet} \cup \left(R^{-1}\right)^{\bullet}.$$

Proof. By Corollary 3.9 and Theorems 3.12 and 3.7, we evidently have $\left(R \cup R^{-1}\right)^{\bullet} = \left(R \cup R^{-1}\right)^{*} = R^{\bullet} = R^{\bullet} \cup \left(R^{-1}\right)^{\bullet}$.

Remark 3.16. Note that, by Remark 2.5, $R^{*} \cup \left(R^{-1}\right)^{*} \subset \left(R \cup R^{-1}\right)^{*}$ is always true.

However, the following example shows that, in contrast to Theorem 3.15, the corresponding equality need not be true.

Example 3.17. If $X = \{1, 2, 3\}$ and $R = \{(1, 2), (1, 3)\}$, then $\left(R \cup R^{-1}\right)^{*} \setminus \left(R^{*} \cup \left(R^{-1}\right)^{*}\right) = \{(2, 3), (3, 2)\}$.

Theorem 3.18. *If R is a reflexive relation on X, then*

$$R^{\bullet} = \left(R \circ R^{-1}\right)^{*} = \left(R^{-1} \circ R\right)^{*}.$$

Proof. Because of the reflexivity of R and Theorem 3.2, we evidently have $R \subset R \circ \Delta_X \subset R \circ R^{-1} \subset \left(R \circ R^{-1}\right)^{*}$. Moreover, by using Corollary 2.8, we can at once see that $\left(R \circ R^{-1}\right)^{*}$ is an equivalence on X. Therefore, by Theorem 3.2, we have $R^{\bullet} \subset \left(R \circ R^{-1}\right)^{*}$.

On the other hand, by using Theorems 3.2, 3.7 and 3.11, we can easily see that $\left(R \circ R^{-1}\right)^{*} \subset \left(R^{\bullet} \circ \left(R^{-1}\right)^{\bullet}\right)^{*} = \left(R^{\bullet} \circ R^{\bullet}\right)^{*} = \left(R^{\bullet}\right)^{*} = R^{\bullet}$ also holds. Therefore, $R^{\bullet} = \left(R \circ R^{-1}\right)^{*}$. Hence, by writing R^{-1} in place of R, we can at once see that $\left(R^{-1} \circ R\right)^{*} = \left(R^{-1}\right)^{\bullet} = R^{\bullet}$ is also true.

Theorem 3.19. *If R is a relation on X, then*

$$R^{\bullet} = \left(R^{*} \circ \left(R^{-1}\right)^{*}\right)^{*} = \left(\left(R^{-1}\right)^{*} \circ R^{*}\right)^{*}.$$

Proof. By Theorems 3.11, 3.18 and 2.7, it is clear that $R^{\bullet} = \big(R^{*}\big)^{\bullet} = \big(R^{*} \circ \big(R^{*}\big)^{-1}\big)^{*} = \big(R^{*} \circ \big(R^{-1}\big)^{*}\big)^{*}$.

Hence, by writing R^{-1} in place of R, and using Theorem 3.7, we can see that the other equality is also true.

4. Further characterizations of equivalences

By Theorems 3.3 and 3.12, we evidently have the following

Theorem 4.1. *If R is a relation on X, then the following assertions are equivalent:*

(1) *R is an equivalence;* (2) $\big(R \cup R^{-1}\big)^{*} \subset R$*;* (3) $\big(R \cup R^{-1}\big)^{*} = R$.

Remark 4.2. Note that, by Corollary 3.9 and Theorem 3.15, we have $\big(R \cup R^{-1}\big)^{*} = \big(R \cup R^{-1}\big)^{\bullet} = R^{\bullet} \cup \big(R^{-1}\big)^{\bullet}$.

Therefore, it is also of some interest to prove the following

Theorem 4.3. *If R is a relation on X, then the following assertions are equivalent:*

(1) *R is an equivalence;* (2) $R^{*} \cup \big(R^{-1}\big)^{*} \subset R$*;* (3) $R^{*} \cup \big(R^{-1}\big)^{*} = R$.

Proof. If the assertion (1) holds, then by Theorem 2.3, it is clear that $R^{*} \cup \big(R^{-1}\big)^{*} = R^{*} \cup R^{*} = R^{*} = R$. That is, the assertion (3) also holds.

While, if the assertion (2) holds, then by Theorem 2.2 it is clear that $\Delta_X \subset R^{*} \subset R^{*} \cup \big(R^{-1}\big)^{*} \subset R$. Moreover, $R^{-1} \subset \big(R^{-1}\big)^{*} \subset R^{*} \cup \big(R^{-1}\big)^{*} \subset R$, and thus $R \circ R^{-1} \subset R^{2} \subset \big(R^{*}\big)^{2} \subset R^{*} \subset R^{*} \cup \big(R^{-1}\big)^{*} \subset R$. Therefore, by Theorem 1.4, the assertion (1) also holds.

Theorem 4.4. *If R is a relation on X, then the following assertions are equivalent:*

(1) *R is an equivalence;* (2) $\big(R \circ R^{-1}\big)^{*} \subset R$*;* (3) $\big(R \circ R^{-1}\big)^{*} = R$.

Proof. If the assertion (1) holds, then by Theorem 2.3, it is clear that $\big(R \circ R^{-1}\big)^{*} = \big(R \circ R\big)^{*} = R^{*} = R$. That is, the assertion (3) also holds.

While if the assertion (2) holds, then by Theorem 2.2 we have $\Delta_X \cup R \circ R^{-1} \subset \big(R \circ R^{-1}\big)^{*} \subset R$. Therefore, by Theorem 1.4, the assertion (1) also holds.

Theorem 4.5. *If R is a relation on X, then the following assertions are equivalent:*

(1) *R is an equivalence;* (2) $R^{*} \circ \big(R^{-1}\big)^{*} \subset R$*;* (3) $R^{*} \circ \big(R^{-1}\big)^{*} = R$.

Proof. If the assertion (1) holds, then by Theorems 2.2, 3.19 and 3.3, it is clear that $R = R \circ \Delta_X \subset R^* \circ \big(R^{-1}\big)^* \subset \Big(R^* \circ \big(R^{-1}\big)^*\Big)^* = R^\bullet = R$. Therefore, the assertion (3) also holds.

While if the assertion (2) holds, then by Theorem 2.2 we have $\Delta_X \subset \Delta_X \circ \Delta_X \subset R^* \circ \big(R^{-1}\big)^* \subset R$ and $R \circ R^{-1} \subset R^* \circ \big(R^{-1}\big)^* \subset R$. Therefore, by Theorem 1.4, the assertion (1) also holds.

Remark 4.6. In the above theorems, by Theorems 1.1 and 2.7, we may write $\big(R^{-1} \circ R\big)^*$ and $\big(R^{-1}\big)^* \circ R^*$ in place of $\big(R \circ R^{-1}\big)^*$ and $R^* \circ \big(R^{-1}\big)^*$, respectively.

Theorem 4.7. *If R is a relation on X, then the following assertions are equivalent:*

(1) *R is an equivalence;* (2) $R = \big(R \cap R^{-1}\big)^*$; (3) $R = R^* \cap \big(R^{-1}\big)^*$.

Proof. If the assertion (1) holds, then by Theorem 2.3 and the symmmetry of R it is clear that $R = R^* = \big(R \cap R^{-1}\big)^*$ and $R = R^* = R^* \cap \big(R^{-1}\big)^*$. That is, the assertions (2) and (3) also hold.

While, if the assertion (2) holds, then by Corollary 2.8 it is clear that the assertion (1) also holds. On the other hand, if the assertion (3) holds, then by Theorems 2.2 and 2.1, it is clear that R is a preorder. Moreover, by using Theorem 2.7 we can see that $R^{-1} = \Big(R^* \cap \big(R^{-1}\big)^*\Big)^{-1} = \big(R^*\big)^{-1} \cap \Big(\big(R^{-1}\big)^*\Big)^{-1} = \big(R^{-1}\big)^* \cap R^* = R$. Therefore, the assertion (1) also holds.

The following examples shows that in Theorem 4.7 we cannot write inclusions in place of the equalities.

Example 4.8. If $X = \{1, 2\}$ and $R = \Delta_X \cup \{(1, 2)\}$, then $\big(R \cap R^{-1}\big)^* \subset R$ and $R^* \cap \big(R^{-1}\big)^* \subset R$ despite that R is not an equivalence.

Example 4.9. If $X = \{1, 2\}$ and $R = \{(1, 2), (2, 1)\}$, then $R \subset \big(R \cap R^{-1}\big)^*$ and $R \subset R^* \cap \big(R^{-1}\big)^*$ despite that R is not an equivalence.

Remark 4.10. Note that, by Theorem 2.2, $\big(R \cap R^{-1}\big)^* \subset R^* \cap \big(R^{-1}\big)^*$ is always true.

However, if $X = \{1, 2, 3\}$ and $R = \{(1, 2), (2, 3), (3, 1)\}$, then $\big(R \cap R^{-1}\big)^* = \Delta_X$ and $R^* \cap \big(R^{-1}\big)^* = X^2$.

Acknowledgement. The author wishes to express his gratitude to Árpád Száz for many helpful conversations and valuable suggestions which led to the present form of the manuscript.

References

[1] Birkhoff, G., Lattice Theory, *Amer. Math. Soc. Colloq. Publ.* **25**, Providence, Rhode Island, 1967.

[2] Everett, C. J., Closure operators and Galois theory in lattices, *Trans. Amer. Math. Soc.* **55** (1944), 514–525.

[3] Kelley, J. L., *General Topology*, Van Nostrand Reinhold, New York, 1955.

[4] Kurdics, J. and Száz, Á., Well-chained relator spaces, *Kyungpook Math. J.* **32** (1992), 263–271.

[5] Levine, N., On uniformities generated by equivalence relations, *Rend. Circ. Mat. Palermo* **18** (1969), 62–70.

[6] Mala, J. and Száz, Á., Modifications of relators, *Acta Math. Hungar.* **77** (1997), 69–81.

[7] Pataki, G., On the extensions, refinements and modifications of relators, *Math. Balk.* **15** (2001), 155–186, (to appear).

[8] Pataki, G. and Száz, Á., A unified treatment of well-chainedness and connectedness properties, *Tech. Rep., Inst. Math. Inf., Univ. Debrecen* **260** (2001), 1–66.

[9] Pervin, W. J., Quasi-uniformization of topological spaces, *Math. Ann.* **147** (1962), 316–317.

[10] Száz, Á., Topological characterizations of relational properties, *Grazer Math. Ber.* **327** (1996), 37–52.

[11] Száz, Á., A Galois connection between distance functions and inequality relations, *Math. Bohem.*, (to appear).

Tamás Glavosits
Institute of Mathematics and Informatics
University of Debrecen
H–4010 Debrecen, Pf. 12, Hungary
E-mail: glavosit@dragon.klte.hu

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 107–114*

PARTÍCIÓK PÁRATLAN SZÁMOKKAL

Orosz Gyuláné (Eger, Hungary)

Kiss Péter professzor emlékére

Abstract. In this article, we characterize the odd-summing natural numbers. We also find that many natural numbers can be represented by more than one such sum. We investigate the features that allow a natural number to have this property and characterize those that have a unique representation. In the process, we find an algorithm that generates a set of consecutive odd natural numbers that add to a specific n.

Középiskolában és felsőfokú intézményben matematikát tanuló diákok számára sok nehézséget okoz az elmélethez kapcsolódó tételek bizonyításának megértése. Tanárnak és diáknak egyaránt hasznos lehet, ha olyan elemi tételeket bizonyítunk, amelyek megértését konkrét példák bemutatásával segíteni tudjuk.

Cikkünk célja olyan egyszerű tételek, bizonyítások és algoritmusok ismertetése, amelyek fejleszthetik a bizonyítások megértésének képességét, és ezzel egy időben a diákok megismerhetik a természetes számok néhány érdekes tulajdonságát is.

A $p(n)$ partíciófüggvényt a következőképpen definiálja Niven–Zuckerman [1]-ben: $p(n)$ az n pozitív egész szám pozitív egészek összegeként való előállításainak száma. Két partíciót egyenlőnek tekintünk, ha csak az összeadandók sorrendjében különböznek. Célszerűen a $p(0)$-t 1-nek definiálja.

Olyan partíciófüggvények is definiálhatók, amelyekben az összeadandók bizonyos feltételeket elégítenek ki: az olyan partíciók, amelyekben az összeadandók mind páratlanok, vagy mind különbözők, vagy amelyekben páros számú összeadandó szerepel, amelyekben az összeadandók nem nagyobbak, mint m, amelyekben páratlan számú különböző összeadandó szerepel; stb.

Olson [2]-ben bizonyította, hogy egy n természetes szám akkor és csak akkor írható fel két vagy több egymást követő természetes szám összegeként, ha nem 2-nek hatványa.

Ray C. és Harris S. [3]-ban olyan partíciókat ismertetnek, amelyben a tagok egymást követő páratlan természetes számok. Definiálják a páratlan összegű szám fogalmát, négy tételt ismertetnek. A tételek bizonyítását több esetben az olvasóra bízzák.

Cikkünkben a [3]-ban megfogalmazott értelmezést és tételeket ismertetjük (1., 2., 3., 4.). A tételeket azok bizonyításával, további példákkal és egy bővebb táblázattal egészítjük ki. További tételeket is megfogalmazunk (5., 6.).

Definíció. Egy n természetes számot páratlan-összegű számnak nevezünk, ha előáll két vagy több egymást követő páratlan természetes szám összegeként.

Például: $15 = 3 + 5 + 7$. A 36-nak két különböző reprezentációja is létezik: $36 = 17 + 19$, $36 = 1 + 3 + 5 + 7 + 9 + 11$. A 10-nek és a 22-nek nincs a feltételnek megfelelő előállítása, ezért nem páratlan-összegű számok. Néhány páratlan-összegű szám: $4, 8, 9, 12, 15, 16, 20, 21, 24, 25$ és 27.

Könnyen bizonyítható, hogy minden négyzetszám előáll egymást követő páratlan számok összegeként, mivel $1 + 3 + 5 + 7 + \cdots + (2k - 1) = k^2$ minden k pozitív egész számra teljesül.

1. tétel. *Egy n természetes szám akkor és csak akkor áll elő a*

$$2k + 1, 2k + 3, 2k + 5, \ldots, 2m - 1,$$

egymást követő páratlan számok összegeként, ha $n = m^2 - k^2$, ahol k és m természetes számok, és $m > k + 1$.

Bizonyítás. A tétel következménye annak, hogy minden 0-nál nagyobb természetes szám négyzete előáll egymást követő páratlan számok összegeként.

Ha $n = 2k + 1 + 2k + 3 + 2k + 5 + \cdots + 2m - 1$, akkor az 1. definíció szerint páratlan-összegű szám, ahol $m > k + 1$. A jobb oldali tagok összegzésével kapjuk:

$$\begin{aligned} n &= (2k + 1 + 2m - 1) \cdot (m - k) \cdot \frac{1}{2} = \\ &= 2(m + k) \cdot (m - k) \cdot \frac{1}{2} = (m + k)(m + k) = m^2 - k^2, \end{aligned}$$

ami azt jelenti, hogy $n^2 = m^2 - k^2$ teljesül.

Tegyük fel, hogy $n^2 = m^2 - k^2$, ahol $m > k + 1$. Minden k, m pozitív egész számra teljesül, hogy

$$1 + 3 + 5 + \cdots + (2k - 1) = k^2 \text{ és } 1 + 3 + 5 + \cdots + (2m - 1) = m^2.$$

$$m^2 - k^2 = 2k + 1 + 2k + 3 + 2k + 5 + \cdots + 2m - 1 = n$$

adódik a megfelelő oldalak különbségéből, ami azt jelenti, hogy az így kapott szám páros összegű.

2. tétel. *Egy n természetes szám akkor és csak akkor páratlan-összegű, ha előáll két természetes szám szorzataként $n = a \cdot b$ alakban, ahol $b \geq a > 1$, azonos paritású természetes számok (a és b egyszerre párosak vagy páratlanok).*

Bizonyítás. Tegyük fel, hogy n a $2k + 1, 2k + 3, \ldots, 2m - 1$ egymást követő páratlan számok összege, ahol $m > k + 1$. Ekkor az előző tétel értelmében:

$$n = m^2 - k^2 \text{ és } m^2 - k^2 = (m - k)(m + k)$$

két természetes szám szorzataként előáll. Ha m és k egyszerre páros vagy páratlan, akkor az $m-k$ és $m+k$ is páros számok. Ha az m és k különböző paritásúak, akkor az $m-k$ és $m+k$ is páratlan számok. Az $m>k+1$, ezért $m-k$ és $m+k$ is nagyobb, mint 1.

Ha $n=a\cdot b$, ahol a és b egyszerre párosak vagy páratlanok, akkor az $m+k=b$ és $m-k=a$ egyenletekből az $n=\left(\frac{b+a}{2}\right)^2-\left(\frac{b-a}{2}\right)^2$, és ezért az n páratlan összegű szám az 1. tétel következtében.

Következmény. Az $n>1$ természetes szám akkor és csak akkor nem páratlan összegű, ha prímszám vagy egy páratlan szám kétszerese.

A 2. tétel bizonyítása egy olyan eljáráson alapul, amelynek segítségével meg tudjuk határozni az összegben szereplő egymást követő páratlan természetes számokat.

Algoritmus. Ha $n=a\cdot b$, akkor $n=\left(\frac{b+a}{2}\right)^2-\left(\frac{b-a}{2}\right)^2$, ezért

$$n=(b-a+1)+(b-a+3)+\cdots+(b+a-1).$$

Például. Mivel $105=7\cdot 15, b=15, a=7$,

$$105=(15-7+1)+(15-7+3)+\cdots+(15+7-1),$$

így $105=9+11+\cdots+21$.

A következő tételek segítségével eldönthetjük, hogy egy adott természetes számnak hány különböző reprezentációja létezik. Két előállítást különbözőnek tekintünk, ha az összeadandókban különböznek egymástól, nem tekintjük különbözőnek, ha csak az összeadandók sorrendjében különböznek.

A $105=3\cdot 35=5\cdot 21=7\cdot 15$, ezért a 105-nek 3 különböző páratlan összegű előállítása létezik.

Az n természetes szám osztóinak számától függ a reprezentációk száma.

3. tétel. *Tegyük fel, hogy* $n=p_1^{t_1}\cdot p_2^{t_2}\cdots p_k^{t_k}$, *ahol* $p_1,p_2,\ldots,p_k$ *különböző prímszámok, és* $p_1<p_2<\cdots<p_k$ *és* $t_i>0, \quad i=1,2,\ldots,k$.

3.1. Ha n páratlan és nem négyzetszám, akkor

$$P(n)=\frac{1}{2}\left[(t_1+1)(t_2+1)\cdots(t_k+1)-2\right]$$

reprezentációja létezik.

3.2. Ha n egy páratlan szám négyzete, akkor

$$P(n)=\frac{1}{2}\left[(t_1+1)(t_2+1)\cdots(t_k+1)-1\right]$$

reprezentációja létezik.

3.3. Ha $p_1 = 2$, és n nem négyzetszám, akkor

$$P(n) = \frac{1}{2}\left[(t_1 - 1)(t_2 + 1)\cdots(t_k + 1)\right]$$

reprezentációja létezik.

3.4. Ha $p_1 = 2$, és n négyzetszám, akkor

$$P(n) = \frac{1}{2}\left[(t_1 - 1)(t_2 + 1)\cdots(t_k + 1) + 1\right]$$

különböző reprezentációja létezik.

Bizonyítás. (3.1.) Az n természetes szám összes pozitív osztóinak száma

$$D(n) = (t_1 + 1)\cdot(t_2 + 1)\cdots(t_k + 1).$$

Ha az n páratlan, és nem négyzetszám, akkor minden p_i páratlan. Legalább egy t_i páratlan, mert a szorzat páros szám. Az összes osztók számának fele egyenlő az osztópárok számával:

$$\frac{1}{2}\left[(t_1 + 1)(t_2 + 1)\cdots(t_k + 1)\right].$$

Az osztópárok között van az $1 \cdot n$ is, ami nem felel meg a tételben megfogalmazott feltételnek. Ezért az n szám olyan kéttényezős szorzatainak száma, amelynek mindkét tényezője páratlan és 1-nél nagyobb:

$$\frac{1}{2}\left[(t_1 + 1)(t_2 + 1)\cdots(t_k + 1) - 2\right].$$

Az osztópárok számának meghatározásával és a paritások elemzésével a 3.1.-hez hasonló módon bizonyíthatóak a 3.2., 3.3. és 3.4. állítások, amelytől eltekintünk.

A bizonyítást megelőzően célszerű konkrét számok esetén meghatározni a reprezentációk számát.

Példák. 3.1. Legyen n páratlan és nem négyzetszám $n = 385 = 5 \cdot 7 \cdot 11$, $D(385) = 2 \cdot 2 \cdot 2 = 8$. Az összes pozitív osztó: $1, 5, 7, 11, 35, 55, 77, 385$.
Az osztópárok száma: $\frac{8}{2} = 4$, ezek $1 \cdot 385$, $5 \cdot 77$, $7 \cdot 55$, $35 \cdot 11$.
Az $1 \cdot 385$ nem felel meg a feltételnek, ezért a következő reprezentációt kapjuk: $385 = 5 \cdot 77$, ahol $a = 5, b = 77$, $b - a + 1 = 73$, $b + a - 1 = 81$ adódik, hogy
$385 = 73 + 75 + 77 + 79 + 81$, $385 = 7 \cdot 55$, ahol $a = 7$, $b = 55$,
$b - a + 1 = 49$, $b + a - 1 = 61$, $385 = 49 + 51 + \cdots + 61$, $385 = 11 \cdot 35$, ahol $a = 11, b = 35$, $b - a + 1 = 25$, $b + a - 1 = 45$, $385 = 25 + 27 + \cdots + 45$.

3.2. Legyen n páratlan szám négyzete $n = 441 = 3^2 \cdot 7^2$, $D(441) = 3 \cdot 3 = 9$. Az összes pozitív osztó: 1, 3, 7, 9, 21, 49, 63, 147, 441. A kéttényezős szorzatok száma öt: $1 \cdot 441, 3 \cdot 147, 7 \cdot 63, 9 \cdot 49, 21 \cdot 21$. Az $1 \cdot 441$ nem felel meg a feltételeknek, ezért $441 = 3 \cdot 147$, ahol $a = 3, b = 147, b - 0 + 1 = 145$ és $b + a - 1 = 149$, $441 = 145 + 147 + 149$. $441 = 7 \cdot 63$, ahol $a = 7, b = 63$, $b - a + 1 = 57$, $b + a - 1 = 69$, $441 = 57 + 59 + \cdots + 69$. $441 = 9 \cdot 49$, ahol $a = 9, b = 49, b - a + 1 = 41$, $b + a - 1 = 57, 441 = 41 + 43 + \cdots + 57$. $441 = 21 \cdots 21$, ahol $a = 21, b = 21$, $441 = 1 + 3 + \cdots + 41$, $P(441) = 4$.

3.3. Legyen n páros és nem négyzetszám. Ha $n = 22 = 2 \cdot 11$, akkor nem létezik reprezentációja a 2. tétel következtében, $P(22) = 0$. Ha $n = 48 = 2^4 \cdot 3$, $D(48) = 10$, ami 6 osztópárt jelent, amelyek: $1 \cdot 48, 2 \cdot 24, 3 \cdot 16, 4 \cdot 12, 6 \cdot 8$. Az $1 \cdot 48$ és $3 \cdot 16$ nem felelt meg a 2. tétel feltételeinek, ezért a $2 \cdot 24, 4 \cdot 12, 6 \cdot 8$ alapján a következő reprezentációk lehetnek: $48 = 2 \cdot 24$, ahol $a = 2$, $b = 24$ alapján $b - a + 1 = 23$ és $b + a - 1 = 25$, ezért $48 = 23 + 25$, $48 = 4 \cdot 12$, ahol $a = 4, b = 12$, így $b - a + 1 = 9$ és $b + a - 1 = 15$ ezért a $48 = 9 + 11 + 13 + 15$. A $48 = 6 \cdot 8$, ahol $a = 6, b = 8$, így $b - a + 1 = 3$ és $b + a - 1 = 13$, ezért a $48 = 3 + 5 + 7 + 9 + 11 + 13$ is teljesül. $P(48) = 3$ a 48 összes reprezentációinak száma.

3.4. Legyen n egy páros szám négyzete: $n = 784 = 2^4 \cdot 7^2$, az összes pozitív osztó $D(784) = 15$. A kéttényezős páros számok szorzatai az alábbiak: $2 \cdot 392, 4 \cdot 196, 8 \cdot 98, 14 \cdot 56, 28 \cdot 28$, ami azt jelenti, hogy a $P(784) = 5$.

4. tétel. *Az n természetes szám akkor és csak akkor írható fel egyértelműen egymást követő páratlan számok összegeként, ha n egy prímszám négyzete, vagy egy prímszám köbe, vagy egy prímszám 4-szerese, vagy két különböző páratlan prímszám szorzata.*

Bizonyítás. Tegyük fel, hogy a $P(n) = 1$, vagyis az n előállítása egyértelmű.

Ha n páratlan és nem négyzetszám, akkor a 3. tétel jelöléseivel

$$\frac{1}{2}\left[(t_1 + 1)(t_2 + 1) \cdots (t_k + 1) - 2\right] = 1,$$

amiből az adódik, hogy a szorzat egyenlő 4. Mivel minden $t_i > 0$ vagy $t_i = 1$ és $k = 1$, ezért $n = {p_1}^3$ vagy $t_1 = t_2 = 1$ és $k = 2$, ezért $n = p_1 \cdot p_2$ két különböző páratlan prímszám szorzata.

A 3. tétel alapján hasonlóan bizonyíthatóak a tétel további állításai.

5. tétel. *Van olyan n természetes szám, amelyre $n, n + 1, n + 2$ számok mindegyike páratlan összegű, és létezik olyan n természetes szám is, hogy ezek egyike sem páratlan összegű.*

Bizonyítás. Pl. $P(75) = 1$, $P(76) = 1$, $P(77) = 1$, $P(41) = 0$, $P(42) = 0$, $P(43) = 0$.

6. tétel. *Nem létezik olyan n természetes szám, amelyre az $n, n+1, n+2, n+3$ számok egyike sem páratlan összegű.*

Bizonyítás. Az $n, n+1, n+2$ és $n+3$ között van olyan szám, amelyik a 4-nek többszöröse. Ha 4-nek többszöröse, akkor felírható két páros szám szorzataként. Ez azt jelenti, hogy a 2. tétel alapján páros összegű számnak kell lennie. Négy egymást követő természetes szám között tehát mindig van páros összegű.

A természetes számok egymást követő páratlan számok összegeként való partícióit mutatja az 1. táblázat, ahol n 1 és 50 közötti szám. $P(n)$ jelenti a partíciók számát.

1. táblázat

n	Prímfaktorizáció	Partíciók száma
1	–	0
2	2	0
3	3	0
4	2^2	1
5	5	0
6	$2 \cdot 3$	0
7	7	0
8	2^3	1
9	3^2	1
10	$2 \cdot 5$	0
11	11	0
12	$3 \cdot 2^2$	2
13	13	0
14	$2 \cdot 7$	0
15	$3 \cdot 5$	1
16	$2 \cdot 4$	1
17	17	0
18	$2 \cdot 3^2$	0

n	Prímfaktorizáció	Partíciók száma
19	19	0
20	$2^2 \cdot 5$	1
21	$3 \cdot 7$	1
22	$2 \cdot 11$	0
23	23	0
24	$3 \cdot 2^3$	2
25	5^2	1
26	$2 \cdot 13$	0
27	3^3	1
28	$2^2 \cdot 7$	1
29	29	0
30	$2 \cdot 3 \cdot 5$	0
31	31	0
32	2^5	3
33	$11 \cdot 3$	1
34	$17 \cdot 2$	1
35	$5 \cdot 7$	$\frac{1}{2}(2 \cdot 2 - 2) = 1$
36	$2^2 \cdot 3^2$	$\frac{1}{2}(1 \cdot 3 + 1) = 2$
37	37	0
38	$2 \cdot 19$	0
39	$3 \cdot 13$	$\frac{1}{2}(2 \cdot 2 - 2) = 1$
40	$2^3 \cdot 5$	$\frac{1}{2}(2 \cdot 2) = 2$
41	41	0
42	$2 \cdot 3 \cdot 7$	0
43	43	0
44	$2^2 \cdot 11$	$\frac{1}{2}(1 \cdot 2) = 2$
45	$3^2 \cdot 5$	$\frac{1}{2}(3 \cdot 2 - 2) = 2$
46	$2 \cdot 23$	0
47	47	0
48	$2^4 \cdot 3$	$\frac{1}{2}(3 \cdot 2) = 3$
49	7^2	$\frac{1}{2}(3 - 1) = 1$
50	$2 \cdot 5^2$	0

A hallgatók számára kijelölhetünk további feladatokat újabb tételek megfogalmazására és bizonyítására.

Irodalom

[1] Niven—Zuckerman: *Bevezetés a számelméletbe.* Műszaki Könyvkiadó, Budapest, 1978.

[2] Olson, Melfriend: Sequentially so. *Mathematics Magazin*, (1991), 297—298.

[3] Ray, C. and Harris, S.: An odd sum. *Mathematics Teacher*, Volume 95, Number **3** (2002).

Orosz Gyuláné
Károly Eszterházy College
Department of Mathematics
Leányka Str. 4.
H-3300 Eger, Hungary
E-mail: ogyne@ektf.hu

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 115–124*

MATHEMATICS COMPETITIONS AND THEIR ROLE IN EDUCATION

Erika Gyöngyösi (Debrecen, Hungary)

Abstract. The present paper has two messages: mathematics competitions form an important complementary component of mathematical education, at various levels. They should form an important stimulus to mathematical learning, catalysing discussions which pursue the unknown and mysterious, and in general in many cases catalysing an increased love of learning. Secondly, typical errors in the processes of reasoning can be detected after analysing solutions of different problems given by students participating in mathematics competitions.

Keywords: mathematics competitions, typical errors, reasoning process, preventing and correcting errors, improving education, inspire to learn mathematics

Introduction

In the first chapter benefits and challenges of mathematics competitons will be discussed. In the second chapter, some examples of actual competitions which have been stunningly successful will be considered to illustrate certain typical errors. It is of considerable use to teachers to be aware of these errors, to determine their reasons, to prevent and correct them. Furthermore, all useful related results should be published in order to contribute to the improvement of the effectivity of the teaching practice. In the final chapter a short summary can be read.

Benefits and challenges of mathematics competitions

Competitions: what are they?

The first thing we wish to do is to extend the concept of competition. Competitions ideed form significant supplement to the mathematics learning process. However there are many further activities related to competitions. There are a number of activities which help students develop their knowledge and increase their interest in learning more. According to Professor Peter Taylor, an Australian mathematics professor who gave a lecture at an international conference titled “Mathematics competitions and related activities and their role in education” between 15 and 17 June in 2001 in Toulouse, France, these activities can include:

— mathematical aspects of problem creation and solution, a dynamic branch of mathematics;
— research in mathematics education related or pertaining to competitions or their types of activities listed here;
— enrichment courses and activities in mathematics;
— mathematics clubs or “circles”;
— mathematics camps, including live-in programs in which students solve open-ended or research-style problems over a period of days;
— publication of journals for students and teachers containing problem sections, book review, review articles on historic and contemporary issues in mathematics;
— support for teachers, schools, region and countries who desire to develop local, regional and national competitions.

In the most obvious sense competitions are organized tests with problems which may be new to students and which have to be solved in a given time frame. Whereas the organizers expect students to use normal logical reasoning to solve the problems, sometimes they are multiple choice. Organisations which administer competitions are not normally the schools or their education departments. Usually they are run by independent organizations comprising dedicated teachers. With the help of the participating mathematics professors at the previously mentioned international conference “Mathematics competitions and related activities and their role in education” benefits and challenges have been collected. According to their valuable experiences these objections can be answered as follows.

Benefits and challenges

Advantages
— Competitions are attractive to students of all standard stimulating their interest in mathematics.
— Questions are often set in a real world, rather than pure mathematical environment, with situations to which the sudents can relate.
— These questions automatically test features of mathematics not commonly tested, such as modeling and interaction with language. However underlying mathematical skills are required.
— Competitions promote mathematics in a favourable light and provide teachers with good quality resources.
— A wide numbers of students have access to competitions.
— Competitions fill the gap of the curriculum, providing an opportunity for talented students to appreciate some of the beautiful parts of mathematics, of a more theoretical and structural nature.

— Experience in competitions and related activities will improve the preparation of the student for University study.
— Competitions provide a great wealth of problems. Competition problems usually provoke vigorous discussion and they can often be solved more than one independent way, showing the richness of mathematics.

Challenges
— Some educators argue that competitions are bad because they cause extra pressure on students.
— There are educators who argue that competitions are not egalitarian.
— Are all students treated equally in competition?
— In some competitions there is a penalty for choosing a wrong answer.
— Problems used in competitions are too special and cover difficult topics in mathematics.
— Organizers of multi-choice competitions do not feel totally comfortable with the concept of asking questions in which students do not need to write out an argument.

Answering objections

— Pressure

Why should competitions cause extra pressure on students? We would argue that this is not the case for a number of reasons. First, in most cases, entry is optional. Further, results of competitions do not form part of normal assessment. Therefore competitions should be seen as a positive experience. For most students, competitions are not events in which students compete against other students, either in teams or as individuals (exceptions being in cases of elite students normally). Rather they should be seen as opportunities for individual challenge.

— Egalitarianism

In the past competitions were not egalitarian as they were for the elite only. However, with competitions such as the Hungarian Competitions (Kurschák, Zrínyi, Gordiusz, Arany Dániel, etc.) and the Kangaroo, hopefully this argument no longer applies. These competitions, which are known as “inclusive”, are clearly aimed at students of all standards, and certainly students of average ability.

— Equality

This is a more interesting question. The same rules apply to all participants and judges correcting tests do not know the name of students whose tests they are correcting. In the case of multi-choice tests, answers are unambiguous.

— Risk

In the multi-choice tests there is a penalty for choosing a wrong answer. This is rather historical, and difficult to change, but for our formal reason is to discourage guessing. I am not sure that guessing is necessarily bad. This is a difficult argument. It does however reduce the possibility of many perfect scores, not always for the right reasons, and so makes it easier for the judges to determine the best students.

— Problems with topics

There have been changes in the curriculum and the manner in which mathematics is taught, over the past 20 years. The main result for the changes has been that the syllabus has become less theoretical. The new syllabus is based on "discovery", with students armed at all stages with the latest calculator to assist them make their discoveries. The impact of these changes is meant to broaden the appeal of mathematics to a wider group of students. But there is certainly a vacuum developing in the availability of rigourous mathematics for talented students to learn in the schools. Competition organizers, who are generally volunteers working independently of formal education departments, continue to prepare pedagogical material to fill this gap. The material of competitions, sometimes inspired by material in mathematical Olympiads, is evolving and sometimes takes different forms than material in traditional syllabi.

— Multi-choice competitions

Such competitions can be easily marked, thus freeing themselves up to be more accessible problems to the average student. It is true that students do not need to write out an argument. However it is possible to design such questions so that students reall y need to solve the problem directly, rather than guessing.

Illustration of typical errors in the processes of reasoning

In this chapter we consider some problems revealing typical errors of students participating in a Hungarian Competition.[1]

Observing students' results we may conclude the dominant reason of their errors and thus we can classify typical errors as follows.

[1] The Zrínyi Ilona Mathematics Competition served as a model for the multi-choice mathematics competition organized in February, 1996. Altogether 600 students of secondary education participated in this competition in Baranya county. After its favourable reception a two-round (regional competition and national final) contest called Gordiusz Mathematics Competition was organized in 1997. 2646 competing students from 10 counties solved the problems on the testpapers of the first round. 115 students were invited to the National Final Competition organized in Pécs. In Gordiusz Mathematical Competition each student has to solve 30 problems in 90 minutes. On the testpapers five solutions (A,B,C,D,E) can be found after each problem and only one of them is correct. During the competition, except for a calculat or no other aid (book, ruler, compasses, etc.) can be used. Writing the processes of reasoning is not required. The considerable number of problems makes it possible to realize an overall and complex measure of students' educational standards.

Examples

1. Which formula is equal to

$$(x^{-1}+y^{-1})^{-1}?$$

(A) $x+y$ (B) $\frac{xy}{x+y}$ (C) $x-y$ (D) $(x+y)^{-1}$ (E) $\frac{x+y}{xy}$

Only 29.5% of the participating students chose the right solution (B) to this problem.[2] 39.5% of the students gave the wrong answer (A). 16.4% of them did not solve the problem and the others chose from the other wrong solutions.

The large proportion of students choosing the wrong answer (A) may show that many of them made an **error based on formalism**. Concepts, problems and results of mathematics are often expressed by mathematics signs and formulas. These procedures performed with signs — for example operation mechanisms — will become skills. In such a case content behind mathematics signs is forgotten, the form dominates and the sense of words gets lost. Those who think formalistically recall their memories instead of understanding the essence of problems, try to find a stereotype and consider mathematics as a collection of rules. In this study we confine the concept of formalism to the cases where mathematics forms dominate over the content of it. Certainly, taking a narrow or wide sense of this concept does not change the fact that reasons for errors influence jointly. The method of replacing variables by concrete values proved to be the best way of correcting this type of errors.

2. How many solutions has the following inequality in the set of integers

$$\frac{x^2-5x+6}{x^2-8x+15}<0?$$

(A) infinitely many (B) 3 (C) 2 (D) 1 (E) 0

20.6% of participating students gave the right answer (D) to this problem.[3] 22% of the students chose (E). 24% of them did not give any answer and the others chose from the other wrong solutions.

This type of **error** may be made out **of habit**. Teachers often experience that students observe things and phenomena which are not taught and in such a case students consider things of no importance as being important and think certain false conclusions — on which they do not doubt and so they do never

[2] 14th problem posed to students of age 15–16 in the first round of the Gordiusz Mathematics Competition organized in 1997.

[3] 20th problem posed to students of age 16–17 in the Mathematics Competition organized in 1996.

state them during lessons and thus they remain hidden before their teacher — to be true. These errors are difficult to prevent and correct because it is rather difficult to give up wrong habits. Lots of patience and long training are needed. Therefore it is very important to be aware of this type of errors. Another similar experience is that students consider concepts previously taught as closed systems and they separate them from new concepts without integrating new concepts into the system of the previous ones. Certain concepts are defined at various levels of development of students again and again as their age changes. When teaching a certain concept it is not necessarily important to define it in the widest domain of validity because it can be too complex and difficult for students to understand it for the first sight. So it is more useful to introduce a concept in a simplier way without giving a definitive definition of it. Although, later on when the same concept is to be taught at a higher level in its definitive form teachers should give enough time to understand the enlargement of the concept and to digest the discontinuity between the restricted and enlarged concepts which finally represent the same concept. It is very useful to give more time to practise and to show the application of the concept and to wait until students are able to understand the difference between different concepts and if so, the teacher can go on with their formation. The case of expanding the domain of validity implies the following process: we have a property which is valid for a certain domain A of objects (a statement of the form: $\forall x \in A$, $p(x)$). We expand the domain A to B ($A \subset B$) in such a way that $p(x)$ should have a sense for every x in B. Then we will study if this particular property continues to be true for each object of the domain B (is it true that $\forall x \in B$, $p(x)$?). Briefly, we study if the property contin use to be true in a situation for which it was not established. In the teaching practice this situation occurs very often. In each case when one expands the domain of validity of a concept he or she should study if the properties can be defined in the same way as before the expansion. In this particular case many students made the following error revealing this type of error. They multiplied both sides of the inequality by the expression in the denominator without considering that the order of the inequation changes if one multiplies by a negative number (however in the set of natural numbers this problem does not arise). Thus these students search the solution of the expression in the numerator and consider under which conditions it is negative. In these cases illustration is of considerable importance. Without illustrating figures students will not believe the correct result which seems an absurdity to them. After the illustration and the ensuing understanding, long training and lots of practice may be needed in order to integrate new conceptions in a higher unit.

3. Find the set of roots of the following function:

$$f(x) = \frac{x^2 - 2|x| + 1}{|x| - 1}.$$

(A) 1 (B) -1 (C) $1; -1$ (D) 0 (E) $\emptyset$

16.3% of participating students gave the correct answer (E) to this problem.[4] 20% of the students chose (C). Moreover, 50.2% of them did not give any answer and the others cho se from the other wrong solutions.

This type of errors are made by students **lacking certain preliminary knowledge**. We do not mean to classify errors owing to learning or teaching negligence into this class of errors. In such a case the solution is obvious: it is necessary to fill the gap. But we intend to consider other errors—which are not the fault of the student or the teacher—made owing to the lack of some preliminary knowledge. In mathematics lots of things are regulated by "agreements". It is compulsory to keep them. Mathematicians are familiar with these agreements however others—such as students—do not know them because even if they learnt them they were not emphasized enough thus students may easily forget them. In our particular example one can not divide by zero which means that the function is not defined for the variables when the denominator is zero. Thus the above problem has no solution. In order to prevent these errors it is necessary to emphasize these agreements which may be trivial and obvious to us but not to students and to train students to keep them whenever it is required.

4. The greatest divisor of a number is itself. How many integers have the number 91 as its second greatest divisor?

(A) infinitely many (B) 6 (C) 5 (D) 4 (E) 3

Only 5.1% of participating students gave the right answer (D) to this problem.[5] 23.9% of the students chose (A). 53.2% of them did not give any answer and the others chose from the other wrong solutions.

In our particular case students giving the wrong solution (A) have **the wrong intuition** that infinitely many integers have the number 91 as its second greatest divisor. They are surprised to learn that the solution is not "infinity" in this case. The solution is as follows: $91 = 13 \times 7$. The integers n we want to find are of the form $91k$. They have $13k$ as divisors. We wish to have $13k \leq 91$. Thus, on the one hand it is necessary that $k \leq 7$. On the other hand k must be a prime number since if k is not a prime then k' is the divisor of k and hence $91k'$ will be a "real" divisor of n which is greate r than 91. Thus, k can only be $7, 5, 3$, or 2.

Certain concepts when we study them make the impression that a result should be true. Sometimes, however, the result turns out to be false. If this conviction arises the intuitive concept may mislead us. This type of situation has a subjective characteris tics since on the one hand intuitions vary individually in each person

[4] 27th problem posed to students of age 15–16 in the first round of Gordiusz Mathematics Competition organized in 1997.

[5] 25th problem posed to students of age 16–18 in the "Kangourou Étudiants 2000" French Mathematics Competition oganized in 2000.

on the other hand they depend on how much one is familiar with a concept in question. Giving counter-examples for these preconvinced ideas allows us to rectify this wrong intuition. When teachers correct testpapers of students they often meet this type of situation. Being aware of these false intuition of students teachers can improve the mathematical teaching and learning process if they train students to avoid deliberately these wrong intuitions.

5. Let two numbers x and y be positive integers which has only one common divisor, 1 and $xy = 300$. Which is the smallest possible value for the sum $x + y$?

(A) 30 (B) 35 (C) 37 (D) 56 (E) 79

32.1% of participating students gave the correct answer **(C)** to this problem.[6] 20% and 10.2% of the students chose (A) and (D), respectively and 27.5% of them did not give any answer and the others chose (B).

Students giving wrong answers confused the concept of "common divisor" and that of "one number is divisible by another".

There are **differences between terms of mathematics and those of the everyday language** which may cause difficulties. Mathematical terms may become reasons for errors if their content does not equal to their meaning in the everyday language, or if the term has not other signification apart from a mathematical conception and it is not enough lifelike. Teachers can correct this type of errors by illustrating controversial cases and by giving counter-examples.

6. We know that certain plants are green, red or blue and they may have from 2 to 5 leaves and they may have from 3 to 20 flowers. Minimum how many plants should be selected by accidently so that we could make a bouquet of 11 perfectly identical plants?

(A) 216 (B) 2376 (C) 2160 (D) 2161 (E) 2375

Only 8.9% of participating students gave the correct answer (D) to this problem.[7] 23.3% the students chose (B) and 47.1% of them did not give any answer.

This error reveals that students do not consider the minimum condition of the pigeonhole principle. During lessons when considering different theorems having more conditions, teachers can train students to examine if these **conditions are really necessary conditions**. Thus students should decide if the new theorem derived from the original by suppressing one of the conditions is true or false. In this

[6] 8th problem posed to students of age 16–18 in the "Kangourou Étudiants 2000" French Mathematics Competition oganized in 2000.

[7] 26th problem posed to students of age 16–18 in the "Kangourou Étudiants 2000" French Mathematics Competition oganized in 2000.

way teachers can train students to learn theorems accurately and to understand them.

Remarks

— Formulas tend to hide the real content of concepts and to create stereotypes. Certainly we need to learn and apply formulas however it is inadmissible to let the real content of concepts sink into insignificance. Errors based on formalism can be considerably reduced by performing a good teaching practice.

— If the dominant reason of an error is a wrong habit then it is easier to prevent these wrong habits than to correct them.

— Errors caused by lacking preliminary knowledge — which are not issued from teaching or learning negligence — as well as those caused by the different usage of mathematical and everyday language cannot be prevented. Nor can be prevented errors whose dominant reason is wrong intuition. In these cases we have to concentrate to correct these errors.

— According to the work of researchers if the teaching practice is of high standard and the teacher trains students to think for themselves then the occurance of typical errors in the processes of reasoning can be considerably reduced. It is necessary to emphasize how important it is to perform the formation and enlargement of concepts thoroughly. If teachers find enough time to do so they will save lots of troubles and dissapointments. Thus, new concepts should be integrated into the previous ones forming one unit without separating different "sets".

— Detecting and correcting an error are two different procedures. The former can be made by a striking observation or by a counter-example and the latter usually demands long and patient work. Generally, the most useful method of correcting errors is illustration. Although it takes relatively long time. The previous estimation of certain results often proves to be better in some cases because it takes less time and it teaches students to think for themselves. We should be careful if we wish to correct an error by two different methods because they may confuse students' thinking.

Summary

The main role of mathematics competitions is to enrich the study of mathematics. These competitions can be especially inspiring for the able student, but materials of all standards can be developed, even allowing the average student to realise that mathematics can be done in a relaxing atmosphere and even be fun and useful in everyday life. Students who can face unexpected situations and solve new problems should be and will be in great demand. This is the strength that we have. Correctly used, competitions train students to meet these challenges. Competitions provide a valuable supplement to classroom teaching by providing new ideas on mathematics in an environment with less pressure. Competitions are enjoying and have a greater role in mathematical teaching, as the growth of popular competitions in the past few decades shows, and we expect that one of the next phases in their development will be a clearer understanding and articulation of the values they have for the classroom. On the other hand multi-choice tests are easy to correct and enable us to assess results quickly and impartially. Typical errors in the processes of reasoning can be detected, too. Comparative statistics can be made from results of students and significant statistical data can be obtained. These tests can be used in a class in order to assess the frequency of certain typical errors of students taught by one particular teacher. Moreover, groups of students from different schools can be tested. Thus teachers can detect deficiencies of their own teaching practice which enables them to improve it. Furthermore teachers working in different schools of secondary education can share their experiences and work out projects together in order to prevent and correct typical errors. Hence the effectivity of teaching and learning can be improved.

Note of thanks

The author wishes to express here her sincere gratitude to Professor András Kovács, Professor Sándor Bácsó, Professor André Antibi and Professor Peter Taylor for their valuable advice and help.

References

[1] Sternberg, R. J. and Ben-Zeev, T., The Nature of Mathematical Thinking, (1996), 45–80.

[2] *A matematikatanitás módszertanának néhány kérdése.* (Some questions related to teaching methods of mathematics.) Tankönyvkiadó, Budapest (1972), 114–135.

[3] Teaching Mathematics: The Relationship Between Knowledge Curriculum and Practice, Topiques édition (1996), 35–121.

[4] Középiskolai matematikai versenytesztek. Gordiusz Matematikaverseny 1996–1997. (Mathematics tests for students of secondary education Gordiusz Mathematics Competitions 1996–1997.) Tóth Könyvkereskedés és Kiadó Kft.

[5] Locia Espinoza, E., Les contre-exemples dans l'enseignement des mathématiques (The counter-examples in mathematics education), These d'État, Université Paul Sabatier (Toulouse III), (2000) 73–109.

[6] Weiner, H., *Psychologie der Fehler* (Psychology of Errors), 1929.

[7] Taylor, P., Mathematics Competitions and related activities and their role in education, Colloque International "Rallyes Mathématiques, Jeux, Compétitions, Clubs, ... et leurs retombés sur l'enseignement et l'image des Mathématiques", Conference 15–16–17 Juin 2001, IREM de Toulouse, Université Paul Sabatier, Toulouse, France.

Acta Acad. Paed. Agriensis, Sectio Mathematicae **29** *(2002) 125–133*

MATEMATIKATANULÁSI NEHÉZSÉGEKKEL KÜZDŐ TANULÓK SEGÍTÉSE

Szilák Aladárné (Eger, Hungary)

Kiss Péter professzor emlékére

Abstract. Hilfe für die Schüler (eventuell discalculierischen Schüler), die 5., 6. Klasse besuchen. Wir planten und machten die Beschaftigungen, wonach hilfen Aufschlieıen. Die Essay stellt die Planung, Methoden, Mittel.

1. A téma választásáról

Az Eszterházy Károly Főiskola Matematika Tanszékén az elmúlt években kutatásokat kezdtünk el matematika szakos főiskolai hallgatók közreműködésével szakmódszertanból matematikatanulási nehézségekkel küzdő felső tagozatos tanulók körében. Számos esetben tapasztaltuk, hogy a tanulók egy része (kb. 10%) különböző okok miatt (fejletlen kognitív képességek; a koncentrálóképesség alacsony szintje; szociálisan hátrányos helyzet; diszkalkulia) nem képes a tantervi anyag minimumát sem elsajátítani. A matematika szinte minden témakörének tanítása és tanulása megkívánja, hogy a tanuló biztos számfogalommal rendelkezzen. Ha a természetes számok halmazában nem tud teljes biztonsággal tájékozódni, akkor nem boldogul később az egész számokkal és a törtekkel (racionális számokkal). E számhalmazok a tantervi anyag minimumát teszik ki, és a követelmények a minimális szintet jelentik. A 6. osztályos év végi követelményminimum figyelembevételével összeállítottunk egy olyan szintfelmérő feladatlapot (csak a racionális számokhoz kapcsolódva), melyet több iskolában 6., 7. osztályos, matematikából igen gyenge tanulókkal írattunk meg tanév elején. Az eredmény nagyon lehangoló volt: 3 feladat kivételével a teljesítmény átlag 20% körüli, az egész dolgozatot tekintve 35%. A feladatlapok segítségével a jellemző hibákat jól ki tudtuk szűrni, melyek alapján a következő kategóriákba soroltuk a tanulókat:

(1) *Jellemző hibákat elkövetők.* (Hibák: hibás számolási technikák; előjelek elhagyása; rossz mértékegységváltás; kerekítési hibák; nehéz szövegértelmezés; téves matematikai modellalkotás; stb.)

(2) *Helytelen, rossz matematikai gondolkodásra jellemző hibákat elkövetők.* (Hibák: gyenge analizálás-szintetizálás; rossz analógia; hiányos algoritmus; intuitív gondolkodás; stb.)

(3) *Diszkalkuliára jellemző hibákat elkövetők.* (Hibák a fentieken túl: nem tudják a számokat növekvő vagy csökkenő sorrendbe rendezni; bizonytalan helyiérték-fogalom; iránytévesztés; fáradékonyság; figyelmetlenség.)

E hibák kategorizálásáról és részletezéséről Mesterházi Zsuzsa A matematikai feladatok megoldásának hibái című tanulmányában [3] részletesebben olvashatunk.

2. A fenti kategóriákba tartozó tanulók segítése

Az **(1)**, **(2)** kategóriába tartozók hibáinak korrigálására **Gyakorló munkafüzeteket** állítottunk össze, melyek alkalmazásával tanórán, differenciált önálló munkában pótolhatták hiányosságaikat. Súlyosabb esetekben és a **(3)** kategóriában tanórán kívül **Felzárkóztató, fejlesztő foglalkozások** keretében nyújtottunk segítséget. Olyan egyéni (1-2-3 fős) felzárkóztató, fejlesztő foglalkozásokat terveztünk és próbáltunk ki, melyek egyrészt a hibák megelőzését is szolgálták, másrészt a felzárkóztatást az osztályfoknak megfelelő minimumszintre.

A felzárkóztató, fejlesztő foglalkozások általános elveivel, szervezésével, tartalmával, módszereivel, eszközeivel korábbi cikkünkben [3] már foglalkoztunk. E publikáció eddigi munkánk és eredményeink rövid konkretizálása.

(a) A felzárkóztatás, fejlesztés tartalma (mindegyik kategóriában):

Racionális számok. (A tantervrészletet, mely a számfogalmat, műveletek értelmezését, műveletvégzési algoritmusokat emeli ki, korábbi cikkünkben [3] közöltük.) E tananyag tükrében megvalósítottuk a legalapvetőbb elemi gondolkodási műveletek (analízis-szintézis; analógia) fejlesztését. Előkészítettük az absztrahálás folyamatát, az induktív következtetést, mely tapasztalásból kiinduló, sejtésen alapuló, a tanulók életkorának és képességeinek jól megfelelő módszer. Fontosnak tartottuk a figyelmetlenség, fáradékonyság kiküszöbölését, a rövid távú emlékezet és a kommunikációs képesség fejlesztését.

(b) A fejlesztés során alkalmazott módszerek:

— Olyan **megtanítási eljárásokat** dolgoztunk ki, melyek sok tárgyi tevékenységen, szemléltetésen, önálló tapasztalatszerzésen alapultak. A megtanítási eljárásokat a legfontosabb matematikai tartalmakhoz készítettük el. Ilyenek: áttérés nagyobb számkörre, bővebb számhalmazra; műveletek, inverz műveletek értelmezése; műveletvégzési algoritmusok; mértékátváltások; szöveges feladatok megoldásának előkészítése; egyszerű arányos következtetések; százalékszámítási feladatok.

— Az **ellenőrzést, önellenőrzést, ismétlést, motiválást játékos feladatokkal, a tanulók önálló munkáit munkalapokkal,** mindezeket mint hagyományos módszereket is fontosnak tartottuk alkalmazni.

(c) Taneszközök:

— A tanulók tanórai egyéni munkájához **Gyakorló munkafüzeteket** készítettünk és a továbbiakban is folyamatosan készítjük. (Természetes számok, egész számok, racionális számok témákhoz kapcsolódva 3 füzet készült el 5. osztályos tanulóknak.) Ezek egy részét már kipróbáltuk.

— Külön **munkalapcsomagot** képeztek a **felzárkóztató, fejlesztő foglalkozások munkalapjai.**

— Montessori műveleltáblákkal analóg **összeadó-, kivonó-, szorzó-, osztótáblákat, gyakorlótáblákat** készítettünk az egész számokhoz.

— Az **applikációs modellek, szorobán, számológép, számítógép, számkártyák, számkorongok, képösszerakók stb.,** mint tanórai keretek között jól alkalmazható eszközök itt is alkalmas eszközháttért jelentettek.

(d) Alkalmazott munkaformák:

— A munkalapok az **egyéni munkát** biztosították.

— **Részben irányított munka** a tanár által felváltva egyéni munkával, sok magyarázat, segítés tette lehetővé a fejlődést.

— **Tanár-diák közös munkája** a nehezebb problémák esetében eredményesebb volt.

— **Diák-diák közös munkája** a könnyebb, játékos feladatok megoldása során motiváló volt, és a tanulók egymás közötti megmérettetését is lehetővé tette.

(e) A felzárkóztatáshoz, fejlesztéshez kapcsolódó általános megjegyzéseink:

— A diszkalkulia nem fogyatékosságként, hanem részképességzavarként értelmezett, ezért a *diszkalkuliásoknak is helyük van az általános iskolákban* (1993. évi LXXIX. számú és az 1999. évi LXVIII. számú törvények a közoktatásról). A törvény adta lehetőségek mellett súlyos esetekben nélkülözhetetlen a matematikatanár és a gyógypedagógus (logopédus) együttműködése.

— A tanári képesítés követelményeiről szóló kormányrendelet előírja, hogy a **tanárjelöltek elméleti és gyakorlati képzésében biztosítani kell a tanulók differenciált fejlesztésére való felkészülést.** Mint tanárképző intézmény matematika szakmódszertanból speciálkollégiumon, szakdolgozókkal és speciális iskolákban teljesítjük e feladatainkat.

— Sajnos a matematikatanulási nehézségek teljes megszüntetése fejlesztő, felzárkóztató terápiánk eredményeként sem lehet végleges, így a tartós, folyamatos segítséget, a minimális fejlődést és szinten tartást évről évre biztosítani kellene, sőt még középiskolában is szükséges lenne folytatni.

— Mivel a lemaradások 5. osztályig, sok tanulónál alsó tagozatig is visszavezethetők, így elsősorban 5., 6. osztályos tanulók fejlesztésével, felzárkóztatásával foglalkoztunk. 48 foglalkozás tervét dolgoztuk ki, és egész tanévben folyamatosan fejlesztettünk 1-2-3, matematikából nagyon gyenge (esetleg diszkalkuliás) tanulót. 12 foglalkozás a természetes számok, 12 az egész számok, 12 a törtek, és végül az előző témákat megismételve és összefogva 12 a racionális számokhoz kapcsolódó minimális tananyagot tartalmazta. Ezek a foglalkozások tanórán kívül, heti 1-2 alkalommal 25-30 percig tartottak. A **Gyakorló munkafüzetek** — melyek a foglalkozásokhoz nagyon hasonló feladatokat tartalmaztak — biztosították az otthoni és a tanórai önálló gyakorlást. A fent említett fejlesztéseket, speciális módszereket, megtanítási eljárásokat, taneszközöket folyamatosan terveztük, elkészítettük és alkalmaztuk. Az alábbi terv egy foglalkozás (Egész számok, tematikus terv 5—6. foglalkozása) részletes leírását tartalmazza. A Feladat és a Munkalap között csak formai különbség van, ugyanis a Munkalap a tanuló taneszköze is. Természetesen minden matematikai tartalomra és fejlesztésre (pl. a gondolkodási műveletek terén) egy foglalkozás keretében nem tudunk kitérni. Egy-egy alkalommal a **Vázlatban** megtervezett matematikai tartalmakat és fejlesztéseket erősítjük. Hasonló elveken és szerkesztésen alapulva készült a többi foglalkozás terve is.

3. Egy fejlesztő foglalkozás terve

I. Vázlat

Téma: Az egész számok

A foglalkozás anyaga: Az egész számok ellentettje, abszolút értéke

Javítandó matematikai probléma: Az ellentett és az abszolút érték fogalmának az összekeverése

Fejlesztés:

— Számemlékezet (1. feladat)
— Lényegkiemelés (szöveges feladat értelmezése) (2. feladat)
— Térbeli tájékozódás (3. feladat)
— Analógiás gondolkodás (3. és 4. feladat, 5. és 6. feladat)

Matematika:

— Egész számok a számegyenesen
— A pozitív egész számok ellentettjei
— Negatív egész számok ellentettjei
— Egész számok abszolút értéke

Taneszközök: munkalapok; számegyenes (1 m hosszú, 10 cm széles papírcsíkon a számok -25-től $+25$-ig); kék és piros számkorongok. (Negatív számok kék, pozitív számok piros színűek. Egy számot modellező korongból több is szükséges.)

Módszerek: Tanuló egyéni munkája munkalappal; tanár-diák beszélgetés; tanári irányítás; egyéni játék munkalap segítségével; közös játék (tanár-diák, diák-diák); önellenőrzés.

Munkaformák:

1. feladat: önálló munka munkalappal

2. feladat: tanári segítség; tanár-diák közös munkája, önálló munka munkalappal

3. feladat: tanári segítség, tanár-diák közös munkája

4. feladat: önálló munka munkalappal

5. feladat: közös munka (játék)

6. feladat: otthoni munka (tanórai önálló munka)

II. Kidolgozás

1. feladat: *Emlékező játék*

1. munkalap

Az utasításoknak megfelelően dolgozz! Figyeld meg a I. táblázatot! Az üres helyeken pótold a hiányzó számokat, és jól jegyezd meg őket!

I. táblázat

−23	−22	−21	−20	−19	−18
−17	−16	−15		−13	−12
−11		−9	−8	−7	−6
−5		−3	−2	−1	0
1	2	3	4		6
7	8		10	11	12

A fenti táblázatot takard le, és a II. táblázatban karikázd be a megjegyzett számokat!

II. táblázat

−23	−22	−21	−20	−19	−18
−17	−16	−15	−14	−13	−12
−11	−10	−9	−8	−7	−6
−5	−4	−3	−2	−1	0
1	2	3	4	5	6
7	8	9	10	11	12

A számkorongok közül válaszd ki a bekarikázottakat!

Vedd elő a számegyenest! Rakd a számegyenesen mindegyik korongot a megfelelő helyre!

Fordítsd meg a korongokat!

Ha jól dolgoztál egy dicsérő szót kaptál eredményként.

Írd ide: ÜGYES

2. feladat:

Tanár: Figyeld meg a következő feladat szövegét!

Andris családi házuk pincéjébe 13 lépcsőfokon tud lemenni. Édesapjának segít a téli tüzelőt lehordani. Kosaranként 10 kg fát tud egyszerre levinni. Hány q fát hord le Andris, ha 15-ször fordul?

2. munkalap

Válaszolj a kérdésekre előbb szóban, majd írásban!

— Hány lépcsőfokon lehet a pincébe lejutni?

Válasz: ....

— Hány kg fát tud kosaranként Andris levinni?

Válasz: ....

— Hányszor fordul?

Válasz: ....

— Folytasd!

1. forduló	2. forduló	3. forduló	4. forduló	...
↓	↓	↓	↓	↓
10 kg	+10 kg	+10 kg	+10 kg	+

— Hány q fát hordott le összesen?

Válasz: 10·15 kg = ... kg = ... q

— Van-e a feladatban olyan adat (információ), amelyet nem használtál fel a megoldáshoz?

Válasz: ....

3. feladat:

Tanár: Lépegess a lépcsőn az utasításoknak megfelelően!

3. munkalap

(Egy 15-15 lépcsőfokból álló lépcsősort tartalmaz, amely a Földszintről megy az Emeletre, illetve a Pincébe.)

— *A Földszintről indulj! Lépkedj az Emelet 9. lépcsőfokára!*
— *A számkorongok közül tedd ide az ennek megfelelőt!*
— *Hány lépcsőfokra vagy a Földszinttől?*
— *Keresd meg a válaszodnak megfelelő korongot!*

— *A Földszintről indulj! Lépkedj a Pince 9. lépcsőfokára!*
— *A számkorongok közül tedd ide az ennek megfelelőt!*
— *Hány lépcsőfokra vagy a Földszinttől?*
— *Keresd meg a válaszodnak megfelelő korongot!*

— *Hasonlítsd össze a két megkeresett korongot! Mit tapasztalsz?*

4. feladat:

4. munkalap

Vedd elő a számegyenesmodellt! Lépegess egyesével az utasításoknak megfelelően! Mindig a 0-ról indulj!

— Lépj a (+6)-ra ! A korongok közül tedd ide az ennek megfelelőt!
Hány egységre van a korong a 0-tól?
Válasz: .... egységre van.
Keresd meg a válaszodnak megfelelő korongot!

— Lépj a (−6)-ra! A korongok közül tedd ide az ennek megfelelőt!
Hány egységre van a korong a 0-tól?
Válasz: .... egységre van.
Keresd meg a válaszodnak megfelelő korongot!

— Hasonlítsd össze a két megkeresett korongot! Mit tapasztalsz?

Válasz: ....

Jegyezd meg!

A (+6) **és a** (−6) **ugyanannyi egységre (ugyanolyan távolságra) van a 0-tól. Ezt a távolságot a** (+6) **és a** (−6) **abszolút értékének nevezzük. A** (+6) **abszolút értéke önmaga, a** (−6) **abszolút értéke az ellentettje, azaz** (+6)**.**

5. feladat:

Tanár: Játsszunk együtt!

Az első hiányos mondat egyik kipontozott helyére egy számkorongot teszek. Tedd te is a megfelelő korongokat a többi kipontozott helyre úgy, hogy mindkét mondat igaz legyen! Az 5. munkalap táblázatába írjuk eredményeinket! Felváltva kezdjünk! Aki jól oldja meg a feladatát, (+1)*-es piros korongot kap, aki hibázik,* (−1)*-es kék korongot. Az a játékos dicsérhető meg, akinek nincs kék vagy kevés kék korongja van.*

5. munkalap

A .... ellentettje ....
A .... és a .... abszolút értéke ....

Kezdő játékos										
Másik játékos										
A számok abszolút értéke										

6. feladat:

6. munkalap

Vedd át a hiányzó játékos(ok) szerepét! Töltsd ki a táblázatot!
Ha elfelejtetted a játékot nézd meg az 5. munkalapot!

A .... ellentettje ....
A .... és a .... abszolút értéke ....

Kezdő ját.	(+2)		(−13)	(+14)			0	(−20)
Másik ját.	(−2)	(+10)			(−10)	(+7)		
Absz. ért.	(+2)	(+10)			(+10)	(+7)		

4. További terveink

Mivel a matematikatanulási nehézségekkel küzdő tanulók is sokféle problémát mutatnak, így fejlesztésük, felzárkóztatásuk egyéni módon lehetséges. Ezért statisztikailag is értékelhető eredményekről, átfogó elemzésekről, a fejlesztés eredményeiről, tapasztalatiról csak többszöri kipróbálás után tudunk majd beszámolni.

Az elvárható matematikai alapműveltség megszerzése és az általános iskola sikeres befejezése a matematikából nagyon gyenge tanulókkal is elérhető, ha folyamatos segítséget kapnak. Ezért 7., 8. osztályban is folytatni kell a fejlesztést, felzárkóztatást. A minimális követelmények figyelembevételével a matematikai tartalmat bővítve, a foglalkozásokat megismételjük. Hiszen nagyon fontos, hogy a 8. osztály végére ezek a tanulók is olyan szintre jussanak matematikából, hogy a mindennapi élethelyzetekben és a továbbtanulás során is boldoguljanak.

Irodalom

[1] Czeglédy István—Orosz Gynuláné—Szalontai Tibor—Szilák Aladárné: *Matematika tantárgypedagógia I.* (Főiskolai jegyzet.) Calibra Kiadó, Budapest, 1994.

[2] Grissemann, H.—Weber, A.: *Speciális számolási zavarok, okok és terápia.* Hans Huber Kiadó, Bern, 1982.

[3] Mesterházi Zsuzsa: *Diszkalkuliáról pedagógusoknak.* BGGYTF, Budapest, 1996.

[4] Szilák Aladárné: Matematikatanulási nehézségek, diszkalkulia. *Acta Acad. Paed. Agriensis, Sectio Math.* **27** (2000), 113—123.

[5] Szilák Aladárné: Felső tagozatos diszkalkuliás tanulók segítése. *Acta Acad. Paed. Agriensis, Sectio Math.* **28** (2001), 107—113.

Szilák Aladárné
Károly Eszterházy College
Department of Mathematics
Leányka Str. 4.
H-3300 Eger, Hungary
E-mail: szilakne@ektf.hu