Contents

Methodological papers

ANNALES MATHEMATICAE ET INFORMATICAE 34. (2007)

ANNALES MATHEMATICAE ET INFORMATICAE

TOMUS 34. (2007)

ESZTERHÁZY KÁROLY COLLEGE
EGER • 1774

HUNGARIA, EGER

ANNALES MATHEMATICAE ET INFORMATICAE

VOLUME 34. (2007)

INSTITUTE OF MATHEMATICS AND COMPUTER SCIENCE
ESZTERHÁZY KÁROLY COLLEGE
HUNGARY, EGER

HU ISSN 1787-5021 (Print)
HU ISSN 1787-6117 (Online)

A kiadásért felelős:
az Eszterházy Károly Főiskola rektora
Megjelent az EKF Líceum Kiadó gondozásában
Kiadóvezető: Kis-Tóth Lajos
Felelős szerkesztő: Zimányi Árpád
Műszaki szerkesztő: Tómács Tibor
Megjelent: 2007. december   Példányszám: 50

Készítette: Diamond Digitális Nyomda, Eger
Ügyvezető: Hangácsi József

Annales Mathematicae et Informaticae
34 (2007) pp. 3–8
http://www.ektf.hu/tanszek/matematika/ami

A modification of Graham's algorithm for determining the convex hull of a finite planar set

Phan Thanh An

Institute of Mathematics
Vietnamese Academy of Science and Technology
e-mail: thanhan@math.ac.vn

Submitted 4 September 2007; Accepted 11 October 2007

Abstract

In this paper, in our modification of Graham scan for determining the convex hull of a finite planar set, we show a restricted area of the examination of points and its advantage. The actual run times of our scan and Graham scan on the set of random points shows that our modified algorithm runs significantly faster than Graham's one.

Keywords: Algorithm, computational complexity, convex hull, extreme point, Graham scan

MSC: 52B55, 52C45, 65D18

1. Introduction

The determination of the convex hull of a point set has successfully been applied in application domains such as pattern recognition [2], data mining [3], stock cutting and allocation [4], or image processing [10].

Graham's algorithm [5] is an important sequential algorithm used for determining the convex hull of the set of n points in the plane ($n \geqslant 3$). This algorithm has a complexity of $O(n \log n)$. Take an interior point x of the convex hull and assume without loss of generality that no three points of the given set (including x) are collinear. We will use the phrase "convex hull" to mean "the set of extreme points of the convex hull". The first step of Graham's algorithm is to construct a sequence $\mathcal{P} = \{p_1, \dots, p_n\}$ of the points in polar coordinates ordered about x in terms of increasing angle (see Fig. 1) (note that point p_1 is adjacent to p_n). In this sequence, call a point *reflex* if the interior angle made by it and its adjacent points is greater than π. In Fig. 1, p_1 is nonreflex and p_2 is reflex. Then, a reflex point does not belong to the convex hull. Graham scan in the algorithm examines the points of the sequence in counterclockwise order and deletes those that are reflex; upon termination, only nonreflex points remain, so the rest is the convex hull of $\mathcal{P}$.

Several modifications of Graham's algorithm have been proposed, all having to do with the following. If the first point in $\mathcal{P}$ is guaranteed to be on the convex hull, then it is never reflex (see [1, 6, 9, 10, 11] etc).

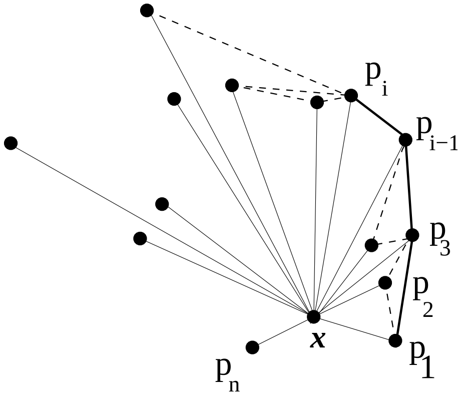


Figure 1: The first step of Graham's algorithm constructs a sequence $\mathcal{P} = \{p_1, \ldots, p_n\}$ of the points in polar coordinates ordered about x.

Determining when the counterclockwise examination of points can stop seems to be the major difficulty, because deleting a reflax point can change its neighbors from nonreflex to reflex. That is one of the reasons why some of modifications of Graham's algorithm contain errors (see [7]). In this note, in our modification of Graham scan, we show a restricted area of the examination of points and its advantage. The actual run times of our scan and Graham scan on the set of random points are given in Table 1, which shows that our modified algorithm runs significantly faster than Graham's one.

2. A modification of the Graham scan

We shall shortly describe a restricted area of the examination of points in Graham scan. Suppose that α is some compact convex set containing $\mathcal{P}$ (see Fig. 2). The first step of Graham's algorithm constructs a sequence $\mathcal{P} = \{p_1, \ldots, p_n\}$ of the points in polar coordinates ordered about the interior point x in terms of increasing angle. After that, let p_{i-1} be nonreflex (i.e., the interior angle made by it and p_i and p_{i-2} is less than π). Let the rays xp_i and $p_{i-1}p_i$ intersect the boundary of α at u_i and v_i, respectively (see Fig. 2). Denote $\widehat{u_i x v_i}$ and $[\widehat{u_i x v_i}]$ the angle at point x and the area, respectively, formed by rays xu_i and xv_i.

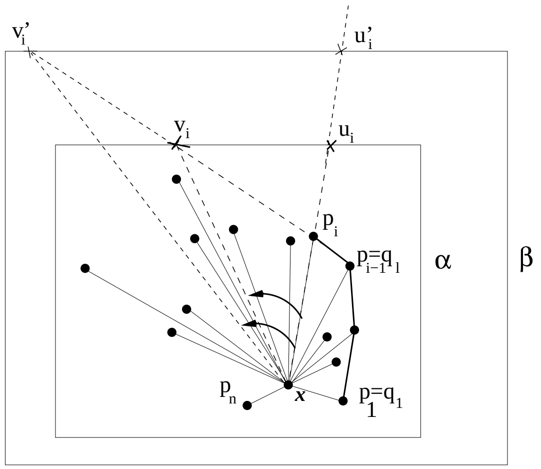


Figure 2: α contains $\mathcal{P}$ and the restricted area at point p_i is $[\widehat{u_i x v_i}]$.
If $\alpha \subset \beta$ then $[\widehat{u_i x v_i}] \subset [\widehat{u_i' x v_i'}]$.

Proposition 2.1. *Let the rays xp_i and $p_{i-1}p_i$ intersect the boundary of α at u_i and v_i, respectively. If p_{i-1} is nonrelfex and all points of $\mathcal{P} \cap [\widehat{u_i x v_i}]$ are nonreflex, then p_i is nonrelfex, too.*

Proof. Assume that $p_{i+1}, \ldots, p_k \in [\widehat{u_i x v_i}]$ and $p_j \notin [\widehat{u_i x v_i}]$ for $k+1 \leqslant j \leqslant n$. Since α is convex, the intersection of α and the closed half-plane bounded by the line $p_{i-1}p_i$ and containing x is convex. It follows that $\widehat{p_{i-1}p_ip_j} < \pi$ for $k+1 \leqslant j \leqslant n$. Therefore, $\widehat{p_{i-1}p_ip_j} < \pi$ for $i+1 \leqslant j \leqslant n$. Since p_{i-1} is nonreflex, p_i is nonreflex, too. □

By Proposition 2.1, to examine if p_i is nonreflex or not, we only need to examine if p_i is nonreflex or not with the points of $\mathcal{P}$ in counterclockwise order beginning from p_{i+1} and belonging to $[\widehat{u_i x v_i}]$. We now present our modification for Graham's algorithm.

Algorithm:

First, find interior point x; label it p_0. Then sort all other points angularly about x; label $p_1, \ldots, p_n$. Set $\mathcal{P} = \{p_1, \ldots, p_n\}$. Take a compact convex set α containing these points. We now determine the convex hull $\mathcal{Q} = \{q_1, \ldots, q_{l+1}\}$.

1. Begin at p_1. Set $l = 1$ and $i = 2$. Because p_1 is on the convex hull, we have $q_1 = p_1$.

2. Consider q_l. If $i = n$, go to **3**. Else, let the rays xq_l and q_lp_i intersect the boundary of α at u_i and v_i, respectively.

2.1 Set $m = 1$.

2.2 If $\widehat{p_i x p_{i+m}} \leqslant \widehat{p_i x v_i}$ (i.e., $p_{i+m} \in \mathcal{P} \cap [\widehat{u_i x v_i}]$) and $\widehat{q_l p_i p_{i+m}} < \pi$, then set $m = m + 1$ and go to **2.2**. Else either

$\widehat{p_i x p_{i+m}} > \widehat{p_i x v_i}$, then by Proposition 2.1, p_i is nonreflex, set $q_{l+1} = p_i$, $i = i + 1$ and $l = l + 1$ go to **2**, or

$\widehat{q_l p_i p_{i+m}} > \pi$, then $\widehat{q_l p_i p_k} < \pi$ for all $p_k \in \mathcal{P}, i < k < i + m$. Set $i = i + m$, go to **2**.

3. Set $q_{l+1} = p_n$. Then, $\mathcal{Q} = \{q_1, \ldots, q_{l+1}\}$ is the convex hull. STOP.

Note that x can be chosen to be a point on the convex hull (see [1, 9]).

Proposition 2.2. *The algorithm computes the convex hull in $n(\log n)$ time.*

Proof. By Proposition 2.1, points of $\mathcal{Q}$ are nonreflex. Hence, the algorithm computes the convex hull.

After sorting points that requires $n(\log n)$ time, the algorithm can only take linear time, since it only advances, never backs up, and the number of steps is therefore limited by the number of points of $\mathcal{P}$. Therefore, the algorithm runs in $n(\log n)$ time. □

Proposition 2.3. *Suppose that α and β are compact convex sets containing $\mathcal{P}$. Let the rays xp_i and $p_{i-1}p_i$ intersect the boundary of α (β, respectively) at u_i and v_i (at u'_i and v'_i, respectively). If $\alpha \subset \beta$ then $[\widehat{u_i x v_i}] \subset [\widehat{u'_i x v'_i}]$.*

Proof. Since α, β are convex and $\alpha \subset \beta$, v_i belongs to the segment $[v'_i, p_i]$. It follows that $[\widehat{u_i x v_i}] \subset [\widehat{u'_i x v'_i}]$. □

Our modification only need to examine the points of $\mathcal{P}$ in counterclockwise order beginning from p_i and belonging to $[\widehat{u_i x v_i}]$ while Jarvis's algorithm [8] and variations of Graham's convex hull algorithm like Akl-Toussaint's algorithm [1], Graham-Yao's algorithm [6], Toussaint-Avis's algorithm [11], etc require that for many points. By Proposition 2.3, the execution time is reduced if the set α is enough small such that it still contains $\mathcal{P}$. So we can choose α to be the smallest rectangle $\mathcal{U}$ enclosing $\mathcal{P}$ and having sides parallel to the coordinate lines.

The algorithm requires to check the condition $\widehat{p_i x p_{i+m}} \leqslant \widehat{p_i x v_i}$. This is implemented in our code as follows: Let xp_{i+m} intersect $u_i v_i$ at $\bar{p}_{i+m}$. Then $\widehat{p_i x p_{i+m}} \leqslant \widehat{p_i x v_i}$ iff x-coordinate of $\bar{p}_{i+m}$ is between x-coordinates of u_i and v_i.

For a given set $\mathcal{P}$ of points randomly positioned in some rectangle $\mathcal{V}$ having sides parallel to the coordinate lines, we can take this rectangle to be α. Based on the "throw-away" principle [1], we can assume that $\mathcal{P}$ includes a finite number of points randomly positioned in the interior of the right-angled triangle abc having sides parallel to the coordinate lines and two points b and c (which form the hypotenuse of the triangle).

Our modified algorithm is implemented in C code. To compare it with Graham's algorithm we use an implementation of Graham's algorithm written by O'Rourke [9]. Codes are compiled by the GNU C Compiler under SuSe Linux 10.0 and are executed on a Pentium IV processor. For the comparison to be meaningful, both implementations use the same code for file reading and rotary sort. The actual run times of the scans in our algorithm and Graham's algorithm on such set $\mathcal{P}$ are given in Table 1, which shows that our modified algorithm runs significantly faster than Graham's one (with integer coordinates). In this case, $\alpha = \mathcal{U} = \mathcal{V}$.

Input size	Number of extreme points	Graham Scan	Our Modified Scan
20000	159	0.0905	0.0638
30000	189	0.1500	0.0946
60000	225	0.3190	0.2068
100000	236	0.5520	0.3611
200000	272	1.2446	0.8503
300000	302	2.0292	1.4025
1000000	376	8.2442	5.7995

Table 1: The actual run times of scans in our algorithm and Graham's algorithm (time in sec) on a finite number of points randomly positioned in the interior of the right-angled triangle *abc* of size 40000 having sides parallel to the coordinate lines and two points *b* and *c*.

References

[1] Akl, S.G. and Toussaint, G.T., A fast convex hull algorithm, *Information Processing Letters*, 7 (1978) 219–222.

[2] Akl, S.G. and Toussaint, G.T., Efficient convex hull algorithms for pattern recognition applications, *Int. Joint Conf. on Pattern Recognition*, Kyoto, Japan, (1978) 483–487.

[3] Böhm, C. and Kriegel, H., Determing the convex hull in large multidimensional databases, *Proceedings of the Third International Conference on Data Warehousing and Knowledge Discovery, Lecture Notes in Computer Science, Springer-Verlag,* 2114 (2001) 294–306.

[4] Freeman, H. and Shapira, R., Determining the minimum-area encasing rectangle for an arbitrary closed curve, *Comm. ACM*, 18(7) (1975).

[5] Graham, R.L., An efficient algorithm for determining the convex hull of a finite planar set, *Information Processing Letters*, 26 (1972) 132–133.

[6] Graham, R.L. and Yao, F.F., Finding the convex hull of a simple polygon, *Journal of Algorithms*, 4 (1983) 324–331.

[7] Gries, D. and Stojmenovic', I., A note on Graham's convex hull algorithm, *Information Processing Letters*, 25 (1987) 323–327.

[8] Jarvis, R.A., On the identication of the convex hull of a finite set of points in the plane, *Information Processing Letters*, 2 (1973) 18–21.

[9] O'Rourke, J., Computational Geometry in C, *Cambridge University Press, Second Edition*, 1998.

[10] Rosenfeld, A., Picture Processing by Computers, *Academic Press, New York*, 1969.

[11] Toussaint, G.T. and Avis, D., On convex hull algorithm for polygons and its application to triangulation problems, *Pattern Recognition*, 15, No. 1 (1982) 23–29.

Phan Thanh An
Institute of Mathematics
Vietnamese Academy of Science and Technology
18 Hoang Quoc Viet Road, 10307 Hanoi, Vietnam

Annales Mathematicae et Informaticae
34 (2007) pp. 9–16
http://www.ektf.hu/tanszek/matematika/ami

Remarks on the Lie derived lengths of group algebras of groups with cyclic derived subgroup

Zsolt Balogh[a], **Tibor Juhász**[b]

[a]Institute of Mathematics and Informatics, College of Nyíregyháza
e-mail: baloghzs@nyf.hu

[b]Institute of Mathematics and Informatics, Eszterházy Károly College
e-mail: juhaszti@ektf.hu

Submitted 20 June 2007; Accepted 10 November 2007

In memoriam Professor Péter Kiss

Abstract

The aim of this paper is to give a new elementary proof for our previous theorem, in which the Lie derived length and the strong Lie derived length of group algebras are determined in the case when the derived subgroup of the basic group is cyclic of odd order.

Keywords: Group algebras, Lie derived length

MSC: 16S34, 17B30

1. Introduction

The group algebra FG of a group G over a field F may be considered as a Lie algebra with the usual bracket operation $[x,y]=xy-yx$. Denote by $[X,Y]$ the additive subgroup generated by all Lie products $[x,y]$ with $x\in X$ and $y\in Y$, and define the Lie derived series and the strong Lie derived series of the group algebra FG respectively, as follows: let $\delta^{[0]}(FG)=\delta^{(0)}(FG)=FG$ and

$$\begin{aligned}\delta^{[n+1]}(FG)&=\big[\delta^{[n]}(FG),\delta^{[n]}(FG)\big],\\ \delta^{(n+1)}(FG)&=\big[\delta^{(n)}(FG),\delta^{(n)}(FG)\big]FG.\end{aligned}$$

We say that FG is Lie solvable if $\delta^{[m]}(FG)=0$ for some m and the number $\mathrm{dl}_L(FG)=\min\{m\in\mathbb{N}\mid\delta^{[m]}(FG)=0\}$ is called the Lie derived length of FG.

Similarly, FG is said to be strongly Lie solvable of derived length $\mathrm{dl}^L(FG) = m$ if $\delta^{(m)}(FG) = 0$ and $\delta^{(m-1)}(FG) \neq 0$. Evidently, $\delta^{[i]}(FG) \subseteq \delta^{(i)}(FG)$ for all i.

For $m \geqslant 0$ let

$$s_l^{(m)} = \begin{cases} 1 & \text{if} \quad l = 0; \\ 2s_{l-1}^{(m)} + 1 & \text{if} \quad s_{l-1}^{(m)} \text{ is divisible by } 2^m; \\ 2s_{l-1}^{(m)} & \text{otherwise.} \end{cases}$$

In [1] we proved the following

Theorem 1.1 (Z. Balogh and T. Juhász [1]). *Let G be a group with cyclic derived subgroup of order p^n, where p is an odd prime, and let F be a field of characteristic p. If $G/C_G(G')$ has order $2^m p^r$, then*

$$\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = d + 1,$$

where d is the minimal integer for which $s_d^{(m)} \geqslant p^n$ holds. Otherwise,

$$\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \lceil \log_2(2p^n) \rceil.$$

This article can be considered as a supplement to [1]. In the original proof of the theorem, at the discussion of the cases when either $G/C_G(G')$ has order $2p^r$, or the order of $G/C_G(G')$ is divisible by some odd prime $q \neq p$, Theorem A and B from [3] play the central role. Two lemmas are shown here, which enable us to construct a new (elementary) proof of Theorem 1.1 avoiding the use of abovementioned results of A. Shalev. For a change, we prove these two lemmas by two different ways (the first was proposed by the referee, whereat we wish to thank him), although both statements could be proved by both methods which will be presented here.

We denote by $\omega(FG)$ the augmentation ideal of FG. It is well-known that $\omega(FG)$ is nilpotent if and only if G is a finite p-group and $\mathrm{char}(F) = p$. The nilpotency index of $\omega(FG)$ will be denoted by $t(G)$. For a normal subgroup $H \subseteq G$ we mean by $\mathfrak{I}(H)$ the ideal $FG \cdot \omega(FH)$. For $x, y \in G$ let $x^y = y^{-1}xy$ and $(x, y) = x^{-1}x^y$, furthermore, denote by $\zeta(G)$ the center of the group G. We shall use freely the identities

$$[x, yz] = [x, y]z + y[x, z], \qquad [xy, z] = x[y, z] + [x, z]y,$$

and for units a, b the equality $[a, b] = ba\big((a, b) - 1\big)$.

2. Proof of Theorem 1.1

Let G be a group with derived subgroup $G' = \langle x \mid x^{p^n} = 1 \rangle$ where p is an odd prime, and let F be a field of characteristic p. As it is well-known, the automorphism group of G' is isomorphic to the unit group $U(\mathbb{Z}_{p^n})$ of $\mathbb{Z}_{p^n}$. Furthermore, $U(\mathbb{Z}_{p^n})$ is cyclic, so the factor group $G/C_G(G')$, which is isomorphic to a subgroup of $U(\mathbb{Z}_{p^n})$, is cyclic, too. We distinguish the following two cases according to the order of $G/C_G(G')$.

2.1. G/C has order $2^m p^r$

Let d be the minimal integer for which $s_d^{(m)} \geqslant p^n$ holds.

First suppose that $m = 0$. Then, as is easy to check (see [1]), the group G is nilpotent, and by [2], $\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \lceil \log_2(p^n + 1) \rceil$. Since

$$2^d - 1 = s_{d-1}^{(0)} < p^n \leqslant s_d^{(0)} = 2^{d+1} - 1,$$

we have $d < \log_2(p^n + 1) \leqslant \lceil \log_2(p^n + 1) \rceil \leqslant d + 1$, thus Theorem 1.1 is proved for the case in point.

Let now $m \geqslant 1$. To prove that $d + 1$ is an upper bound on $\mathrm{dl}^L(FG)$ it is sufficient to show that

$$\delta^{(l+1)}(FG) \subseteq \mathfrak{I}(G')^{s_l^{(m)}} \quad \text{for all} \quad l \geqslant 0.$$

This is clear for $l = 0$. For the induction we need Lemma 2 from [1], which states that

$$[\mathfrak{I}(G')^{i2^m}, \mathfrak{I}(G')^{j2^m}] \subseteq \mathfrak{I}(G')^{i2^m + j2^m + 1}. \tag{2.1}$$

Hence, assuming that $\delta^{(l)}(FG) \subseteq \mathfrak{I}(G')^{s_{l-1}^{(m)}}$, we obtain

$$\begin{aligned}\delta^{(l+1)}(FG) &= [\delta^{(l)}(FG), \delta^{(l)}(FG)]FG \\ &\subseteq [\mathfrak{I}(G')^{s_{l-1}^{(m)}}, \mathfrak{I}(G')^{s_{l-1}^{(m)}}]FG \subseteq \mathfrak{I}(G')^{s_l^{(m)}}.\end{aligned}$$

Therefore, $\mathrm{dl}^L(FG) \leqslant d + 1$. Now, we shall prove that $d + 1 \leqslant \mathrm{dl}_L(FG)$. Let us choose an element $aC_G(G')$ of order 2^m from $G/C_G(G')$ and consider the group $H = \langle x, a \rangle$ and set $x^k = x^a$. In particular, when $m = 1$, we have that $a^2 \in \zeta(H)$, $x^a = x^{-1}$, and the quotient group $\overline{H} = H/\zeta(H)$ is isomorphic to the dihedral group of order $2p^n$. This case is treated in the next lemma.

Lemma 2.1. *Let G be the dihedral group of order $2p^n$ for some odd prime p, and let $\mathrm{char}(F) = p$. Then $\mathrm{dl}_L(FG) \geqslant d + 1$, where d is the minimal integer such that $s_d^{(1)} \geqslant p^n$.*

Proof. Write the group G as $\langle a, x \mid a^2 = x^{p^n} = 1, xa = ax^{-1} \rangle$ and set $s_l = s_l^{(1)}$. We shall show that $(x - x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG)$ if l is odd, and $(x - x^{-1})^{s_{l-1}+1} \in \delta^{[l]}(FG)$ if l is even; further

$$a(x - x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG) \qquad \text{and} \qquad ax(x - x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG).$$

For, if $l = 1$ then $x - x^{-1} = [a, ax] \in \delta^{[1]}(FG)$, $a(x - x^{-1}) = [a, x] \in \delta^{[1]}(FG)$ and $ax(x - x^{-1}) = [ax, x] \in \delta^{[1]}(FG)$.

If l is even then, by induction, the elements

$$(x - x^{-1})^{s_{l-2}}, a(x - x^{-1})^{s_{l-2}}, \; ax(x - x^{-1})^{s_{l-2}}$$

belong to $\delta^{[l-1]}(FG)$. Since $(x-x^{-1})^2$ is central and s_{l-2} is odd,

$$\begin{aligned}[ax(x-x^{-1})^{s_{l-2}}, a(x-x^{-1})^{s_{l-2}}] &= [ax(x-x^{-1}), a(x-x^{-1})](x-x^{-1})^{2s_{l-2}-2}\\ &= a(x-x^{-1})[x, a(x-x^{-1})](x-x^{-1})^{2s_{l-2}-2}\\ &= (x-x^{-1})^{2s_{l-2}+1} = (x-x^{-1})^{s_{l-1}+1}.\end{aligned}$$

Thus $(x-x^{-1})^{s_{l-1}+1} \in \delta^{[l]}(FG)$. Furthermore,

$$\begin{aligned}[\frac{1}{2}a(x-x^{-1})^{s_{l-2}}, (x-x^{-1})^{s_{l-2}}] &= [\frac{1}{2}a, (x-x^{-1})^{s_{l-2}}](x-x^{-1})^{s_{l-2}}\\ &= [\frac{1}{2}a, x-x^{-1}](x-x^{-1})^{2s_{l-2}-1}\\ &= a(x-x^{-1})^{2s_{l-2}} = a(x-x^{-1})^{s_{l-1}},\end{aligned}$$

and hence,

$$\begin{aligned}[\frac{1}{2}ax(x-x^{-1})^{s_{l-2}}, (x-x^{-1})^{s_{l-2}}] &= [\frac{1}{2}a(x-x^{-1})^{s_{l-2}}, (x-x^{-1})^{s_{l-2}}]x\\ &= ax(x-x^{-1})^{s_{l-1}},\end{aligned}$$

so the elements $a(x-x^{-1})^{s_{l-1}}$ and $ax(x-x^{-1})^{s_{l-1}}$ belong to $\delta^{[l]}(FG)$.

Now, if l is odd then s_{l-2} is even, and by the inductive hypothesis

$$(x-x^{-1})^{s_{l-2}+1}\ , a(x-x^{-1})^{s_{l-2}},\ ax(x-x^{-1})^{s_{l-2}} \in \delta^{[l-1]}(FG).$$

As above,

$$\begin{aligned}[a(x-x^{-1})^{s_{l-2}}, ax(x-x^{-1})^{s_{l-2}}] &= [a, ax](x-x^{-1})^{2s_{l-2}}\\ &= (x-x^{-1})^{2s_{l-2}+1}\\ &= (x-x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG),\end{aligned}$$

and

$$\begin{aligned}[\frac{1}{2}a(x-x^{-1})^{s_{l-2}}, (x-x^{-1})^{s_{l-2}+1}] &= [\frac{1}{2}a, x-x^{-1}](x-x^{-1})^{2s_{l-2}}\\ &= a(x-x^{-1})^{2s_{l-2}+1}\\ &= a(x-x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG),\end{aligned}$$

and finally

$$\begin{aligned}[\frac{1}{2}ax(x-x^{-1})^{s_{l-2}}, (x-x^{-1})^{s_{l-2}+1}] &= [\frac{1}{2}a(x-x^{-1})^{s_{l-2}}, (x-x^{-1})^{s_{l-2}+1}]x\\ &= ax(x-x^{-1})^{s_{l-1}} \in \delta^{[l]}(FG).\end{aligned}$$

Induction is complete.

Let d be the minimal integer such that $s_d \geqslant p^n$. Then $s_{d-1} < p^n$ and

$$a(x-x^{-1})^{s_{d-1}} = ax^{-s_{d-1}}(x^2-1)^{s_{d-1}}$$

is nonzero element of $\delta^{[d]}(FG)$ (by the binomial theorem as the order of x^2 is p^n). Thus $\mathrm{dl}_L(FG) > d$ and the statement follows. □

The following line shows the truth of Theorem 1.1 for the case $m = 1$:

$$d + 1 \leqslant \mathrm{dl}_L(F\overline{H}) \leqslant \mathrm{dl}_L(FH) \leqslant \mathrm{dl}_L(FG).$$

Let us turn to the case $m > 1$. Since $(x, a) = x^{-1+k} \in H'$ and $k \not\equiv 1 \pmod p$, we have that H' has order p^n. Moreover, $H/C_H(H')$ has order 2^m. Lemma 4 in [1] forces

$$a\omega^{s_l^{(m)}}(FH') \oplus a^{-1}\omega^{s_l^{(m)}}(FH') \subseteq \delta^{[l+1]}(FH)$$

for all $l \geqslant 0$, therefore $\delta^{[d]}(FH) \neq 0$, so $d + 1 \leqslant \mathrm{dl}_L(FH) \leqslant \mathrm{dl}_L(FG)$, as asserted.

2.2. The order of $G/C_G(G')$ is divisible by some odd prime $q \neq p$

In the proof of the next lemma we will use the well-known congruence

$$x^k - 1 \equiv k(x-1) \pmod{\mathfrak{I}(G')^2} \text{ for all } k \in \mathbb{Z}. \tag{2.2}$$

Set $G/C_G(G') = \langle bC_G(G') \rangle$ and $x^k = x^b$. The congruence

$$[(x-1)^{2^l}, b] \equiv (k^{2^l} - 1)b(x-1)^{2^l} \pmod{\mathfrak{I}(G')^{2^l+1}} \text{ for all } l \geqslant 0 \tag{2.3}$$

can be obtained as a simple consequence of (2.2).

Lemma 2.2. *Let G be a group with cyclic derived subgroup of order p^n and let* $\mathrm{char}(F) = p$. *If the order of $G/C_G(G')$ is divisible by an odd prime $q \neq p$, then* $\mathrm{dl}_L(FG) \geqslant \lceil \log_2(2p^n) \rceil$.

Proof. Let $G' = \langle x \mid x^{p^n} = 1 \rangle$ and let us choose an element $bC \in G/C_G(G')$ of order q and set $x^k = x^b$. Evidently, $k^{2^m} \not\equiv 1 \pmod p$ for all m. Set $H = \langle b, C_G(G') \rangle$. Clearly, $x^{k-1} = (x, b) \in H'$ is of order p^n, so H' has order p^n, too. Since $H' = (b, C_G(G'))$ and the map $c \mapsto (b, c)$ is an epimorphism of $C_G(G')$ onto H', we can choose c from $C_G(G')$ such that $(b, c) = x$. Define the following three series in FG: let

$$u_0 = b, \quad v_0 = c, \quad w_0 = c^{-1}b^{-1},$$

and, for $l \geqslant 0$, let

$$u_{l+1} = [u_l, v_l], \quad v_{l+1} = [u_l, w_l], \quad w_{l+1} = [w_l, v_l].$$

Using induction we show for odd l that

$$\begin{aligned} u_l &\equiv t_u^{(l)} cb(x-1)^{2^{l-1}} \pmod{\mathfrak{I}(G')^{2^{l-1}+1}}; \\ v_l &\equiv t_v^{(l)} c^{-1}(x-1)^{2^{l-1}} \pmod{\mathfrak{I}(G')^{2^{l-1}+1}}; \\ w_l &\equiv t_w^{(l)} b^{-1}(x-1)^{2^{l-1}} \pmod{\mathfrak{I}(G')^{2^{l-1}+1}}, \end{aligned} \tag{2.4}$$

and if l is even then

$$\begin{aligned} u_l &\equiv t_u^{(l)} b(x-1)^{2^{l-1}} \pmod{\Im(G')^{2^{l-1}+1}};\\ v_l &\equiv t_v^{(l)} c(x-1)^{2^{l-1}} \pmod{\Im(G')^{2^{l-1}+1}};\\ w_l &\equiv t_w^{(l)} c^{-1}b^{-1}(x-1)^{2^{l-1}} \pmod{\Im(G')^{2^{l-1}+1}}, \end{aligned} \tag{2.5}$$

where $t_u^{(l)}, t_v^{(l)}, t_w^{(l)}$ are nonzero elements in the field F while $2^{l-1} < p^n$. Evidently, $u_1 = [b,c] = cb(x-1)$, and applying (2.2) we have

$$\begin{aligned} v_1 &= [b, c^{-1}b^{-1}] = c^{-1}\big((x^{-1})^{b^{-1}} - 1\big)\\ &= c^{-1}(x^{-k'} - 1) \equiv -k'c^{-1}(x-1) \pmod{\Im(G')^2}, \end{aligned}$$

and similarly, $w_1 = [c^{-1}b^{-1}, c] \equiv -k'b^{-1}(x-1) \pmod{\Im(G')^2}$, where $x^{k'} = x^{b^{-1}}$. Therefore (2.4) holds for $l = 1$. Now assume that (2.4) is true for some odd l. Then, using the congruences (2.3) and $kk' \equiv 1 \pmod{p}$, we have

$$\begin{aligned} u_{l+1} &\equiv t_u^{(l)} t_v^{(l)} [cb(x-1)^{2^{l-1}}, c^{-1}(x-1)^{2^{l-1}}]\\ &\equiv -t_u^{(l)} t_v^{(l)} [(x-1)^{2^{l-1}}, b](x-1)^{2^{l-1}}\\ &\equiv -t_u^{(l)} t_v^{(l)} (k^{2^{l-1}} - 1) b(x-1)^{2^l} \pmod{\Im(G')^{2^l+1}}, \end{aligned}$$

$$\begin{aligned} v_{l+1} &\equiv t_u^{(l)} t_w^{(l)} [cb(x-1)^{2^{l-1}}, b^{-1}(x-1)^{2^{l-1}}]\\ &\equiv t_u^{(l)} t_w^{(l)} \big(-b^{-1}c[(x-1)^{2^{l-1}}, b](x-1)^{2^{l-1}}\\ &\qquad + cb[(x-1)^{2^{l-1}}, b^{-1}](x-1)^{2^{l-1}} \big)\\ &\equiv t_u^{(l)} t_w^{(l)} k^{2^{l-1}} (k'^{2^l} - 1) c(x-1)^{2^l} \pmod{\Im(G')^{2^l+1}} \end{aligned}$$

and

$$\begin{aligned} w_{l+1} &\equiv t_w^{(l)} t_v^{(l)} [b^{-1}(x-1)^{2^{l-1}}, c^{-1}(x-1)^{2^{l-1}}]\\ &\equiv -t_w^{(l)} t_v^{(l)} c^{-1}[(x-1)^{2^{l-1}}, b](x-1)^{2^{l-1}}\\ &\equiv -t_u^{(l)} t_v^{(l)} (k'^{2^{l-1}} - 1) c^{-1}b^{-1}(x-1)^{2^l} \pmod{\Im(G')^{2^l+1}}. \end{aligned}$$

The assumption on k (see at the beginning of the proof) ensures that the coefficients of the element u_{l+1}, v_{l+1} and w_{l+1} are nonzero in the field F. Supposing that (2.5) is true for some even l we can similarly get the required congruences. So, (2.4) and (2.5) are valid for any $l > 0$.

Assume that $l < \lceil \log_2(2p^n) \rceil$. Then $2^{l-1} < p^n$ and the elements u_l, v_l, w_l are nonzero in $\delta^{[l]}(FH)$, thus $\mathrm{dl}_L(FG) \geqslant \mathrm{dl}_L(FH) \geqslant \lceil \log_2(2p^n) \rceil$. □

The inequality $\mathrm{dl}^L(FG) \leqslant \lceil \log_2(2p^n) \rceil$ is well-known, thus the lemma completes the proof of Theorem 1.1.

3. Remarks on the theorem

(i) If G is a non-nilpotent group with cyclic derived subgroup of order p^n and $\operatorname{char}(F) = p$, then

$$\lceil \log_2(3p^n/2)\rceil \leqslant \mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) \leqslant \lceil \log_2(2p^n)\rceil.$$

In order to prove these inequalities it remains to show that if $G/C_G(G')$ has order $2^m p^r$, then $\lceil \log_2(3p^n/2)\rceil \leqslant \mathrm{dl}_L(FG)$. Since G is not nilpotent, $m > 0$, and, as we have already seen, the dihedral group of order $2p^n$ can be embedded into G. Hence, by Lemma 2.1, we have $d+1 \leqslant \mathrm{dl}_L(FG)$, where d is the minimal integer such that $s_d^{(1)} \geqslant p^n$. At the same time, it is easy to verify that

$$s_l^{(1)} = \begin{cases} (2^{l+2}-1)/3 & \text{if } l \text{ is even;} \\ (2^{l+2}-2)/3 & \text{if } l \text{ is odd.} \end{cases} \tag{3.1}$$

Thus, $(2^{d+2}-1)/3 \geqslant s_d^{(1)} \geqslant p^n$, whence $d+1 \geqslant \lceil \log_2(3p^n/2+1/2)\rceil$ follows. Since $\lceil \log_2(3p^n/2+1/2)\rceil = \lceil \log_2(3p^n/2)\rceil$, the required inequality is guaranteed.

As the difference of the integers $\lceil \log_2(3p^n/2)\rceil$ and $\lceil \log_2(2p^n)\rceil$ is at most one, the values of $\mathrm{dl}_L(FG)$ and $\mathrm{dl}^L(FG)$ are almost uniquely determined by this inequality. In some cases we are able to determine explicitly the values of $\mathrm{dl}_L(FG)$ and $\mathrm{dl}^L(FG)$:

(ii) We claim that if $G/C_G(G')$ has order $2p^r$, then

$$\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \lceil \log_2(3p^n/2)\rceil.$$

Indeed, according to Theorem 1.1, if $l = \mathrm{dl}^L(FG)$ then $s_{l-2}^{(1)} < p^n$. From (3.1) it follows that $(2^l-1)/3 < p^n$. Hence $l < \log_2(3p^n/2+1/2)+1$, and therefore $l \leqslant \lceil \log_2(3p^n/2+1/2)\rceil$. Since $\lceil \log_2(3p^n/2+1/2)\rceil = \lceil \log_2(3p^n/2)\rceil$, the proof is complete.

(iii) Since the order of $G/C_G(G')$ divides the order of $U(\mathbb{Z}_{p^n})$, which is equal to $p^{n-1}(p-1)$, for primes p of the form $4k-1$ the order of $G/C_G(G')$ is either p^r for some r (then $\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \lceil \log_2(p^n+1)\rceil$), or $2p^r$ (then by part *(ii)*, $\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \lceil \log_2(3p^n/2)\rceil$), or it has an odd prime divisor $q \neq p$ (then $\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \lceil \log_2(2p^n)\rceil$).

(iv) Let G be a non-nilpotent group with derived subgroup of order $p > 3$, where p is a Fermat prime (i.e. it can be written in the form $2^{2^s}+1$ for some $s \geqslant 0$), and let $\operatorname{char}(F) = p$. Then

$$\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = \begin{cases} \lceil \log_2(2p)\rceil & \text{if } G/C_G(G') \text{ has order } p-1; \\ \lceil \log_2(3p/2)\rceil & \text{otherwise.} \end{cases}$$

Indeed, let us write p in the form $2^r + 1$ $(r > 1)$. If $G/C_G(G')$ has order $p - 1 = 2^r$, then $s_r^{(r)} = 2^r$, and by Theorem 1.1,

$$\mathrm{dl}_L(FG) = \mathrm{dl}^L(FG) = r + 2 = \lceil \log_2(2p) \rceil,$$

as asserted. In the other case $G/C_G(G')$ has order 2^m for some $0 < m < r$. Since $\lceil \log_2(3p/2) \rceil = r+1$, by Theorem 1.1 it is enough to show that $s_r^{(m)} \geqslant p$. But this is true, because $s_{r-1}^{(r-1)} = 2^{r-1}$, furthermore, for $m = r - 1$ we have

$$s_r^{(m)} = s_r^{(r-1)} = 2s_{r-1}^{(r-1)} + 1 = 2^r + 1 = p,$$

and if $m < r - 1$ then $s_{r-1}^{(m)} > s_{r-1}^{(r-1)}$. This implies

$$s_r^{(m)} \geqslant 2s_{r-1}^{(m)} > 2s_{r-1}^{(r-1)} = 2^r = p - 1$$

and the proof is done.

References

[1] Balogh, Z., Juhász, T., Lie derived lengths of group algebras of groups with cyclic derived subgroup. To appear in *Commun. Alg.*

[2] Juhász, T., On the derived length of Lie solvable group algebras, *Publ. Math. (Debrecen)* Vol. 68/1-2 (2006) 243–256.

[3] Shalev, A., The derived length of Lie soluble group rings. II. *J. London Math. Soc.* (2) 49 (1994), no. 1, 93–99.

Zsolt Balogh
Institute of Mathematics and Informatics
College of Nyíregyháza
H-4410 Nyíregyháza
Sóstói út 31/B
Hungary

Tibor Juhász
Institute of Mathematics and Informatics
Eszterházy Károly College
H-3300 Eger
Leányka út 4
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 17–28
http://www.ektf.hu/tanszek/matematika/ami

The remainder term in Fourier series and its relationship with the Basel problem

V. Barrera-Figueroa[a], A. Lucas-Bravo[a], J. López-Bonilla[b]

[a] Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías Avanzadas,
Departamento de Telemática
e-mail: vbarreraf@ipn.mx, alucasb@ipn.mx

[b] Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica,
Sección de Estudios de Postgrado e Investigación
e-mail: jlopezb@ipn.mx

Submitted 5 September 2007; Accepted 20 November 2007

Abstract

In this paper it is shown several approximation formulae for the remainder term of the Fourier series for a wide class of functions satisfying specific boundary conditions. Also it is shown that the remainder term is related with the Basel problem and the Riemann zeta function, which can be interpreted as the energy of discrete-time signals; from this point of view, their energy can be calculated with a direct formula instead of an infinite series. The validity of this algorithm is established by means several proofs.

Keywords: Fourier series remainder term, discrete-time signal, Basel problem, slow varying-type series.

1. Introduction

Fourier series is a mathematical tool for characterizing the frequency content of a periodic signal which satisfies the Dirichlet conditions [1]. However, the Fourier series is frequently applied to non-periodic functions, made artificially periodic by extending periodically its original domain. In practice, with a sufficiently large number of terms, a finite expansion can be built upon the Fourier series for representing accurately enough the function. Such finite representation carries implicitly a remainder term which must be estimated [2].

The calculation of the remainder term is expressed via a mean square error between the infinite series and the finite expansion, which provides us an enclosed range of values where the error can be found, instead of an exact formula. Such estimations stir up the appearance of slow varying-type series, as in the Basel problem series, which in general are expressed by the Riemann zeta function. This let us establish a relation between it and a discrete-time signal, usually defined for all the natural numbers. Therefore the approximation of the remainder term in Fourier series can be employed as an excellent way for calculating the energy of a discrete-time signal. The energy calculation embraces a small number of terms instead of an infinite number, which brings us accurately enough results whose validity is proved in this paper.

2. Integral approach of slow-varying series

In the calculation of the remainder term in finite Fourier expansion, appears series whose members are expressed as the product of a periodic term and a function which varies slowly between successive values of. This let us get a very good approximation of the series [5]:

$$\sum_{k=1}^{\infty} e^{jk\alpha}\varphi(k). \tag{2.1}$$

Let us integrate the k^{th} term around $k-1/2$ and $k+1/2$:

$$\int_{k-1/2}^{k+1/2} \varphi(\xi)e^{j\xi\alpha}d\xi = \int_{-1/2}^{1/2} \varphi(k+t)e^{j(k+t)\alpha}dt$$

$$= \frac{1}{j\alpha}\varphi(k+t)e^{j(k+t)\alpha}\bigg|_{-1/2}^{1/2} - \frac{1}{j\alpha}\int_{-1/2}^{1/2} \varphi'(k+t)e^{j(k+t)\alpha}dt. \tag{2.2}$$

However, since $\varphi'(k+t)$ tends to zero asymptotically, it is possible to establish the following approximation:

$$\int_{-1/2}^{1/2} \varphi(k+t)e^{j(k+t)\alpha}dt \approx \frac{e^{jk\alpha}}{j\alpha}[\varphi(k+1/2)e^{j\alpha/2} - \varphi(k-1/2)e^{-j\alpha/2}]. \tag{2.3}$$

Because of the slow variation of $\varphi(k)$ we have that $\varphi(k+1/2) \approx \varphi(k-1/2) \approx \varphi(k)$, therefore the integral is:

$$\int_{-1/2}^{1/2} \varphi(k+t)e^{j(k+t)\alpha}dt \approx e^{jk\alpha}\varphi(k)\frac{\sin\alpha/2}{\alpha/2}. \tag{2.4}$$

By changing the integrating variable we have:

$$e^{jk\alpha}\varphi(k) \approx \frac{\alpha}{2\sin\alpha/2}\int_{k-1/2}^{k+1/2} \varphi(\xi)e^{j\xi\alpha}d\xi, \tag{2.5}$$

which transforms the original series into a series of integrals:

$$\sum_{k=1}^{\infty} e^{jk\alpha}\varphi(k) \approx \frac{\alpha}{2\sin\alpha/2}\sum_{k=1}^{\infty}\int_{k-1/2}^{k+1/2}\varphi(\xi)e^{j\xi\alpha}d\xi. \tag{2.6}$$

Since the integration limits are contiguous, the series becomes in just one integral:

$$\sum_{k=1}^{\infty} e^{jk\alpha}\varphi(k) \approx \frac{\alpha}{2\sin\alpha/2}\int_{1/2}^{\infty}\varphi(\xi)e^{j\xi\alpha}d\xi. \tag{2.7}$$

3. The Zeta function as the generalization of the Basel problem

The Basel problem is a famous issue in the Number Theory because of its ingenious solution provided by Leonhard Euler, and its relationship to the distribution of the prime numbers. The problem consists in calculating the exact sum of the following series:

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \lim_{n\to\infty}\left(\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{n^2}\right). \tag{3.1}$$

Euler's method uses the Taylor series for the sine function, which is a polynomial whose roots are $x = k\pi$, $k \in \mathbb{Z}$. Thus, with the Fundamental Theorem of Algebra, the polynomial $\sin x/x$ can be written in terms of its roots [3]:

$$\frac{\sin x}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} + \frac{x^6}{7!} + \cdots = A(x^2-\pi^2)(x^2-4\pi^2)(x^2-9\pi^2)\cdots, \tag{3.2}$$

where A is a proportionality constant. Since each factor has the form $x^2 - n^2\pi^2 = 0$, they can be expressed as $1 - x^2/n^2\pi^2$, transforming the polynomial into:

$$\frac{\sin x}{x} = (1-\frac{x^2}{\pi^2})(1-\frac{x^2}{4\pi^2})(1-\frac{x^2}{9\pi^2})\cdots, \tag{3.3}$$

by multiplying all the factors and gathering the coefficients belonging to x^2, results the series:

$$-\frac{1}{\pi^2}-\frac{1}{4\pi^2}-\frac{1}{9\pi^2}\cdots = -\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}, \tag{3.4}$$

From (3.2) we get the coefficient of x^2 as $-1/3!$, therefore:

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}. \tag{3.5}$$

The same procedure, after being applied in the other resulting powers of the multiplication (3.3), gives a set of impressive series, all of which are based in even powers:

$$\sum_{n=1}^{\infty}\frac{1}{n^4}=\frac{\pi^4}{90},\qquad \sum_{n=1}^{\infty}\frac{1}{n^6}=\frac{\pi^6}{945},$$
$$\sum_{n=1}^{\infty}\frac{1}{n^8}=\frac{\pi^8}{9450},\qquad \sum_{n=1}^{\infty}\frac{1}{n^{10}}=\frac{\pi^{10}}{93555},\qquad \ldots \tag{3.6}$$

The generalization of the Basel problem for real powers is gotten by the Riemann zeta function, defined as [6]:

$$\zeta(x)=\sum_{n=1}^{\infty}\frac{1}{n^x},\qquad x\neq 1. \tag{3.7}$$

The case $x=1$ is avoided since the series becomes divergent, Figure 1. For even powers the function gives exact values, proportional to even powers of π, as shown in (3.6); for odd powers it is not possible to get such an exact representations. The

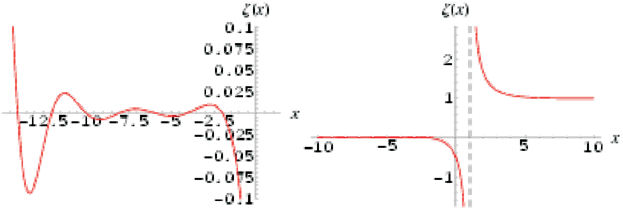


Figure 1: Plot of the Riemann zeta function.

Bernoulli numbers B_n are a set of rational numbers defined by the series [4]:

$$\frac{x}{e^x-1}=\sum_{n=0}^{\infty}\frac{B_n x^n}{n!},$$
$$B_0=1,\quad B_1=-\frac{1}{2},\quad B_2=\frac{1}{6},\quad B_4=-\frac{1}{30},\quad B_6=\frac{1}{42},\quad \ldots \tag{3.8}$$

The zeta function is related with them for integer values of the argument x as:

$$\zeta(n)=\frac{2^{n-1}|B_n|\pi^n}{n!},\quad B_n=(-1)^{n+1}n\zeta(1-n),\qquad n\in\mathbb{N}. \tag{3.9}$$

4. The remainder term of Fourier series

The Fourier series develops a function by means of an infinite series of trigonometric terms; its convergence is assured by Dirichlet conditions. However, in practice, it is not possible to take an infinite number of such orthogonal functions, but a finite number of them for performing a finite Fourier expansion $f_n(x)$, formed by n terms. Fourier series convergence shows that by taking a sufficiently large number of terms, the difference between $f(x)$ and $f_n(x)$, named the remainder term, can be made as small as we desire:

$$\eta_n(x) = f(x) - f_n(x). \tag{4.1}$$

Let us suppose that $f^{(m)}(x)$ exists, although its continuity is not demanded; however, the continuity of $f(x), f'(x), f''(x), \ldots, f^{m-1}(x)$ is required for setting the following boundary conditions:

$$f(\pi) = f(-\pi),\ f'(\pi) = f'(-\pi), \ldots, f^{m-1}(\pi) = f^{m-1}(-\pi). \tag{4.2}$$

The existence of the above conditions let us simplify the integration of the coefficients in Fourier series, performed by parts successively m times. They can be gathered in a complex coefficient:

$$a_k + jb_k = \frac{j^m}{\pi k^m} \int_{-\pi}^{\pi} f^{(m)}(\xi) e^{jk\xi} d\xi, \tag{4.3}$$

where the Fourier series is the real part of the series:

$$f(x) = \sum_{k=1}^{\infty} (a_k + jb_k) e^{-jkx} = \int_{-\pi}^{\pi} f^{(m)}(\xi) \left[\frac{j^m}{\pi} \sum_{k=1}^{\infty} \frac{e^{jk(\xi - x)}}{k^m} \right] d\xi. \tag{4.4}$$

The index $k = 0$ has been omitted since $f(x)$ stands for $f(x) - a_0/2$. Let us change the integrating variable by $\theta = \xi - x$, therefore, $f(x)$ is written in terms of the kernel-type series $G_m(\theta)$:

$$f(x) = \int_{-\pi}^{\pi} f^{(m)}(\theta + x) G_m(\theta) d\theta, \quad G_m(\theta) = \frac{j^m}{\pi} \sum_{k=1}^{\infty} \frac{e^{jk\theta}}{k^m}. \tag{4.5}$$

In the finite expansion $f_n(x)$, the kernel-type series must add only n terms, thus the remainder term is expressed in function of another kernel-type series $g_n^m(\theta)$:

$$\eta_n(x) = \int_{-\pi}^{\pi} f^{(m)}(\theta + x) g_n^m(\theta) d\theta, \quad g_n^m(\theta) = \frac{j^m}{\pi} \sum_{k=n+1}^{\infty} \frac{e^{jk\theta}}{k^m}. \tag{4.6}$$

The simpler method for getting the remainder term is based on Cauchy inequality:

$$\left[\int_a^b f(x) g(x) dx \right]^2 \leqslant \int_a^b f^2(x) dx \int_a^b g^2(x) dx. \tag{4.7}$$

After applied it in (4.6) we get:

$$\eta_n^2(x) \leqslant \int_{-\pi}^{\pi} f^{(m)^2}(\theta + x) d\theta \int_{-\pi}^{\pi} [g_n^m(\theta)]^2 d\theta. \tag{4.8}$$

In this case, we can take advantage of the orthogonality of the members of the series $g_n^m(\theta)$, by taking their real part. The integral of the square of kernel-type series is:

$$\int_{-\pi}^{\pi} [g_n^m(\theta)]^2 d\theta = \frac{1}{\pi^2} \sum_{k=n+1}^{\infty} \int_{-\pi}^{\pi} \frac{\cos k\theta}{k^m} \sum_{l=n+1}^{\infty} \frac{\cos l\theta}{l^m} d\theta = \frac{1}{\pi} \sum_{k=n+1}^{\infty} \frac{1}{k^{2m}}. \tag{4.9}$$

The above series seems to be related with the Riemann zeta function, however, we cannot get an exact result since the series starts from $n+1$. For estimation purposes, we can use the integral approach of a slow varying-type series, whose periodic part is the unitary function, i.e., $\alpha = 0$. The slow varying part is the function $\varphi(k) = 1/k^{2m}$, which varies slowly, since m and n are supposed to be great:

$$\frac{1}{\pi} \sum_{k=n+1}^{\infty} \frac{1}{k^{2m}} \approx \frac{1}{\pi} \int_{n+1/2}^{\infty} \frac{d\xi}{\xi^{2m}} = \frac{1}{\pi(2m-1)(n+1/2)^{2m-1}}. \tag{4.10}$$

The integral of ${f^{(m)}}^2$, should be identified as the norm of the m^{th} derivative of $f(x)$, represented by N_m^2, therefore the remainder term is bounded by:

$$|\eta_n(x)| < \frac{N_m}{\sqrt{\pi(2m-1)}(n+1/2)^{m-1/2}}. \tag{4.11}$$

Another method for getting the remainder term is by evaluating reliably the kernel-type series $g_n^m(\theta)$ with the integral approach of a slow varying-type series, where the slow varying function corresponds with $\varphi(k) = 1/k^m$. With the exception of small values around $\theta = 0$, we can use the asymptotic behavior of the integral:

$$g_n^m(\theta) \approx \frac{j^m \theta}{2\pi \sin\theta/2} \int_{n+1/2}^{\infty} \frac{e^{j\xi\theta}}{\xi^m} d\xi \approx \frac{j^{m+1}}{2\pi \sin\theta/2} \frac{e^{j(n+1/2)\theta}}{(n+1/2)^m}. \tag{4.12}$$

For estimation purposes, the remainder term can be calculated by means the following inequality:

$$|\eta_n(x)| \leqslant \int_{-\pi}^{\pi} |f^{(m)}(\theta+x)||g_n^m(\theta)| d\theta = |f^{(m)}(x)|_{max} \int_{-\pi}^{\pi} |g_n^m(\theta)| d\theta. \tag{4.13}$$

After taking the real part of $g_n^m(\theta)$ and integrating it, we get the following formula:

$$|\eta_n(x)| < \frac{2}{(n+1/2)^{m-1}} \frac{\ln(n+1/2)\pi}{(n+1/2)\pi} |f^m(x)|_{max}. \tag{4.14}$$

5. Mean square error in Fourier series

Frequently the remainder term is known as the error term, for its interpretation is obvious. However, it is more suitable to handle a mean square error for practical issues:

$$\eta^2 = \frac{1}{2\pi} \int_{-\pi}^{\pi} \eta_n^2(x) dx = \frac{1}{2\pi} \int_{-\pi}^{\pi} [f(x) - f_n(x)]^2 dx. \tag{5.1}$$

The orthogonality properties let us express the mean square error in function of the coefficients in Fourier series:

$$\eta^2 = \frac{1}{2}\sum_{k=1}^{\infty}(a_k^2 + b_k^2) - \frac{1}{2}\sum_{k=1}^{n}(a_k^2 + b_k^2) = \frac{1}{2}\sum_{k=n+1}^{\infty}(a_k^2 + b_k^2), \tag{5.2}$$

where the mean square error results equal to the square of the remainder term:

$$\eta^2 = \frac{\eta_n^2}{2\pi}\int_{-\pi}^{\pi} dx = \eta_n^2. \tag{5.3}$$

The above formulae let us find out a relation between the norm of the m^{th} derivative of $f(x)$ and the coefficients of its Fourier series. By substituting (4.9) into (4.8) we have:

$$\eta_n^2 \leqslant \frac{1}{\pi}\sum_{k=n+1}^{\infty}\frac{1}{k^{2m}}\int_{-\pi}^{\pi} f^{(m)^2}(\xi)d\xi, \tag{5.4}$$

from which we get the following inequality:

$$\frac{1}{2}\sum_{k=n+1}^{\infty}(a_k^2 + b_k^2) \leqslant \frac{1}{\pi}\sum_{k=n+1}^{\infty}\frac{1}{k^{2m}}\int_{-\pi}^{\pi} f^{(m)^2}(\xi)d\xi, \tag{5.5}$$

which provides us the wanted relation:

$$a_k^2 + b_k^2 < \frac{1}{\pi k^{2m}}\int_{-\pi}^{\pi} f^{(m)^2}(\xi)d\xi. \tag{5.6}$$

If we consider that in the inequality (5.5) both series start from $k = 1$, we get:

$$\frac{1}{2}\sum_{k=1}^{\infty}(a_k^2 + b_k^2) \leqslant \frac{1}{\pi}\sum_{k=1}^{\infty}\frac{1}{k^{2m}}\int_{-\pi}^{\pi} f^{(m)^2}(\xi)d\xi, \tag{5.7}$$

where the left side is proportional to the integral of $f^2(x)$:

$$\sum_{k=1}^{\infty}(a_k^2 + b_k^2) = \frac{1}{\pi}\int_{-\pi}^{\pi} f^2(x)dx, \tag{5.8}$$

from which the following inequality is gotten:

$$\frac{1}{2}\int_{-\pi}^{\pi} f^2(x)dx \leqslant \sum_{k=1}^{\infty}\frac{1}{k^{2m}}\int_{-\pi}^{\pi} f^{(m)^2}(\xi)d\xi. \tag{5.9}$$

This series is expressed in terms of the zeta function, from which results the following impressive inequality:

$$\int_{-\pi}^{\pi} f^2(x)dx \leqslant \frac{(2\pi)^{2m}}{(2m)!}|B_{2m}|\int_{-\pi}^{\pi} f^{(m)^2}(\xi)d\xi. \tag{5.10}$$

6. Energy of discrete-time signals

A discrete-time signal $x(k)$ is a single value function defined at discrete points of the domain, which represents the samples of a continuous-time function $x_a(t)$, related with the first one by:

$$x(k) = x_a(kT), \quad k \in \mathbb{Z}, \tag{6.1}$$

being T the sampling rate. For discrete-time signals we can define their energy E as that dissipated by a unitary resistance:

$$E = \sum_{k=-\infty}^{\infty} |x(k)|^2. \tag{6.2}$$

For energy signals, the above series converges. However, if the series diverges, the function is said to be a power signal [7]. In general, power signals are periodic functions, where their mean power P, measured in a complete period N, converges:

$$P = \lim_{N\to\infty} \frac{1}{2N+1} \sum_{k=-N}^{N} |x(k)|^2. \tag{6.3}$$

In practice, it is not possible to perform an infinite summation for calculating the energy of a discrete-time signal, since with a representative number of terms we can get an approximation of the series, for the upper terms can be neglected since energy signals show a decreasing behavior; therefore we have the following approximation:

$$E_n = \sum_{k=1}^{n} |x(k)|^2, \tag{6.4}$$

where $x(k)$ is supposed to be a causal signal, i.e., $x(k) = 0$ for $k \leqslant 0$. Therefore, the Riemann zeta function, for even arguments, gives the exact value of the energy of a discrete-time signal:

$$E = \zeta(2m) = \sum_{k=1}^{\infty} \frac{1}{k^{2m}}, \quad m \in \mathbb{N}. \tag{6.5}$$

which is written as a sequence of weighted unitary impulse:

$$x(n) = \sum_{k=1}^{\infty} \frac{\delta(n-k)}{k^m}, \quad \delta(n-k) = \begin{cases} 1, & n = k, \\ 0, & n \neq k. \end{cases} \tag{6.6}$$

The approximation of the energy of the signal is written in terms of its total energy, expressed by the zeta function:

$$E_n = \sum_{k=1}^{n} \frac{1}{k^{2m}} = \zeta(2m) - \sum_{k=n+1}^{\infty} \frac{1}{k^{2m}}. \tag{6.7}$$

In this formula, we can use the integral approach of a slow varying-type series since the second one varies slowly, as is required. Therefore:

$$\sum_{k=n+1}^{\infty} \frac{1}{k^{2m}} \approx \int_{n+1/2}^{\infty} \frac{d\xi}{\xi^{2m}} = \frac{1}{(2m-1)} \frac{1}{(n+1/2)^{2m-1}}. \tag{6.8}$$

Hence, the next formula has the advantage of bring us a very accurate value of the energy of the discrete-time signal without developing the sum until the n^{th} term:

$$E_n \approx \zeta(2m) - \frac{1}{(2m-1)} \frac{1}{(n+1/2)^{2m-1}}. \tag{6.9}$$

The following tables present a comparative analysis which demonstrates the validity of (6.9) as a reliable approximation formula for the finite expansion (6.4). For doing so, we must programming the formula (6.7) by using double precision floating point variables, defined in C++ language like of double type. Figure 2 shows the flow diagram of the main program.

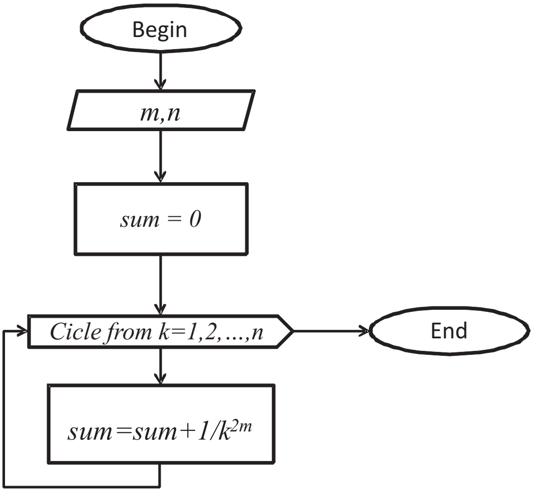


Figure 2: Algorithm for performing the expansion E_n.

7. Conclusions

The formulae used for getting the bounded values of the remainder terms were deduce from the integral approach of a slow varying-type series, which let us calculate the remainder term without performing the infinite sum of the series. In fact, in this work has been proved that the remainder term can be related with the Riemann zeta function, which aroused from the Basel problem.

n	E_n summation	E_n approximation	Absolute Difference
1	1.000000000000000000	0.978267400181559776	0.021732599818440224
10	1.549767731166540760	1.549695971610131060	0.000071759556409701
100	1.634983900184892260	1.634983818092007550	0.000000082092884712
1000	1.643934566681561240	1.643934566598351350	0.000000000083209883
10000	1.644834071848064960	1.644834071847976360	0.000000000000088596
100000	1.644924066898243000	1.644924066898226120	0.000000000000016875

Table 1: Case $m = 1$.

n	E_n summation	E_n approximation	Absolute Difference
1	1.000000000000000000	0.983557801612372495	0.016442198387627505
10	1.082036583493756640	1.082035287844960840	0.000001295648795807
100	1.082322905344472730	1.082322905328218180	0.000000000016254553
1000	1.082323233378305940	1.082323233378304160	0.000000000000001776
10000	1.082323233710861480	1.082323233710804630	0.000000000000056843
100000	1.082323233710861480	1.082323233711137480	0.000000000000276001

Table 2: Case $m = 2$.

n	E_n summation	E_n approximation	Absolute Difference
1	1.000000000000000000	0.991005613424777998	0.008994386575222002
10	1.017341512441431340	1.017341494932115790	0.000000017509315553
100	1.017343061964943730	1.017343061964941290	0.000000000000002442
1000	1.017343061984441020	1.017343061984448570	0.000000000000007550
10000	1.017343061984441020	1.017343061984448790	0.000000000000007772
100000	1.017343061984441020	1.017343061984448790	0.000000000000007772

Table 3: Case $m = 3$.

The Riemann zeta function can be parsed as the energy of a discrete-time energy signal. For calculating accurately its total energy, it is not necessary to perform a large expansion of terms, but to use a formula which is gotten from the study of the remainder term of the Fourier series.

As can be seen from Tables 1– 5, the results demonstrate the virtue of using the formula (6.9) instead of counting n terms. Even if the expansion is formed by only one term, the error involved is in the order of 0.1% for $m = 5$, and 2.1% for $m = 1$. In addition, from the tables we can assure the convergence of the results by taking only ten terms in all of the cases; by taking a large number of terms, the results show that occur a kind of saturation in the results of the program, since there

n	E_n summation	E_n approximation	Absolute Difference
1	1.000000000000000000	0.995716261417096016	0.004283738582903984
10	1.004077346255262570	1.004077346045353590	0.000000000209908979
100	1.004077356197943030	1.004077356197942580	0.000000000000000444
1000	1.004077356197943030	1.004077356197943920	0.000000000000000888
10000	1.004077356197943030	1.004077356197943920	0.000000000000000888
100000	1.004077356197943030	1.004077356197943920	0.000000000000000888

Table 4: Case $m = 4$.

n	E_n summation	E_n approximation	Absolute Difference
1	1.000000000000000000	0.998104320141845691	0.001895679858154309
10	1.000994575058549610	1.000994575056194600	0.000000000002355005
100	1.000994575127818200	1.000994575127817750	0.000000000000000444
1000	1.000994575127818200	1.000994575127817750	0.000000000000000444
10000	1.000994575127818200	1.000994575127817750	0.000000000000000444
100000	1.000994575127818200	1.000994575127817750	0.000000000000000444

Table 5: Case $m = 5$.

exist no variations in the calculations while increasing the number of summands. This can be interpreted as that the first elements have more energy than the upper ones. Therefore, the use of a finite expansion for calculating the energy of the discrete-time signal is justified, since the upper terms can be neglected.

References

[1] Cantor, G., Contributions to the Founding of the Theory of Transfinite Numbers *Dover Publications, Inc.* (1995), 1–82.

[2] Fejér, L., Untersuchen Über Fouriersche Reihen, *Math. Annalen*, Vol. 58 (1904), 51–69.

[3] Kimble, G., Euler's Other Proof, *Mathematics Magazine*, Vol. 60 (1987), 282.

[4] Lanczos, C., Discourse on Fourier Series, *Oliver & Boyd, Edinburgh*, (1996), 45–75, 109.

[5] Lanczos, C., Linear Differential Operators, *Dover Publications, Inc.* (1997), 49–99.

[6] Penrose, R., The Road to Reality, *Jonathan Cape*, (2004), 211.

[7] Proakis, J.G., Manolakis, D.G., Digital Signal Processing. Principles, Algorithms and Applications, *Prentice Hall* (1999), 43–52.

V. Barrera-Figueroa and A. Lucas-Bravo
Av. I.P.N. No. 2580 Col. Barrio La Laguna Ticomán, CP 07340, México D.F.

J. López-Bonilla
UPALM Edif. Z-4, 3er piso, Col. Lindavista CP 07738, México D.F.

Annales Mathematicae et Informaticae
34 (2007) pp. 29–31
http://www.ektf.hu/tanszek/matematika/ami

On a sum involving powers of reciprocals of an arithmetical progression

Hacène Belbachir, Abdelkader Khelladi

USTHB/ Faculté de Mathématiques, Alger
e-mail: hbelbachir@usthb.dz, hacenebelbachir@gmail.com, akhelladi@usthb.dz, akhelladi@wissal.dz

Submitted 25 September 2007; Accepted 9 December 2007

Abstract

Our purpose is to establish the following result: Let a and d be coprime integers and $a, a+d, a+2d, \dots, a+(k-1)\,d$ $(k \geqslant 2)$ be an arithmetical progression. Then for all integers $\alpha_0, \alpha_1, \dots, \alpha_{k-1}$ the rational number $1/a^{\alpha_0} + 1/\left(a+d\right)^{\alpha_1} + \cdots + 1/\left(a+(k-1)\,d\right)^{\alpha_{k-1}}$ is never an integer. This result extends theorems of Taeisinger (1915) and Kürschák (1918), and also generalizes a result of Erdős (1932).

Keywords: Harmonic sums, arithmetical progression, greatest prime factor.

In 1915, Taeisinger proved that the harmonic number $H_n := 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ is never an integer except for H_1. The more general result that the sum of reciprocals of consecutive terms, not necessarily starting with 1, is never an integer was proved by Kürschák in 1918 [3, p.157]. In 1932, Erdős proved that the sum of reciprocals of any integers in arithmetical progression is never a reciprocal and then an integer [2]. Our purpose is to give some extensions of the cited results.

Let n be a positive integer and p be a prime number. We define the p-valuation of n as the unique positive integer $v_p(n)$ satisfying $n = u \cdot p^{v_p(n)}$ with $\gcd(u, p) = 1$.

Our idea relies on the fundamental inequality about the valuation of a sum of two positive integers. Let n and m be integers. It is well known that $v_p(n+m) \geqslant \min\{v_p(n), v_p(m)\}$, with a remarkable implication that if $v_p(n) > v_p(m)$ then $v_p(n+m) = v_p(m)$.

The following Theorem is the key assertion behind all the results of this paper.

Theorem 1.1. *Let $n_1, n_2, \dots, n_k$ be positive integers. Assume that there exists a prime P such that $v_P(n_{j_P})$ is maximal (non zero) for a unique $j_P \in \{1, 2, \dots, k\}$. Then*

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$$

is never an integer.

In fact this result is well-known and simple consequence of elementary properties of valuations (see [1]). However, for the convenience of the reader we give the proof of this statement.

Proof. Let us suppose that $N := \frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$ is an integer. By setting $R := n_1 n_2 \cdots n_k / P^v$, where $v = 1 + \sum\limits_{j \neq j_P} v_P\left(n_j\right)$, one has

$$RN - \sum_{j \neq j_P} \frac{R}{n_j} = \frac{R}{n_{j_P}}.$$

Each term of the left hand side is an integer, while the right hand side is not. It is contradiction, so the statement is proved. □

We get the following as a simple and immediate consequence.

Corollary 1.2. *Let $n_1, n_2, \ldots, n_k$ be positive integers. Assume that there exists a prime P such that $P \mid n_i$ for some i, and $P \nmid n_j$ when $j \neq i$. Then*

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_k}$$

is never an integer.

The first main result of our paper is an extension of Taeisinger's Theorem.

Theorem 1.3. *Let n be an integer $\geqslant 2$ and $\alpha_2, \ldots, \alpha_n$ be positive integers. Then*

$$1 + \frac{1}{2^{\alpha_2}} + \cdots + \frac{1}{n^{\alpha_n}}$$

is never an integer.

Proof. Let P be the greatest prime number $\leqslant n$. By Bertrand's postulate we have $n < 2P$. Thus P is coprime to all $k \in \{1, 2, \ldots, n\} \setminus \{P\}$. The theorem follows then from Corollary 1.2. □

To study the case of an arithmetical progression, we give the following result which is an immediate consequence of a theorem of Shorey and Tijdeman [4].

Theorem 1.4. *Let a, d and k be positive integers, satisfying* $\gcd(a, d) = 1$, $k \geqslant 2$. *By setting $\Delta = \prod\limits_{j=1}^{k} (a + (j-1)\, d)$ and $P := \max\limits_{p \mid \Delta} p$, the greatest prime factor of Δ, then for $d > 1$, we have $P \geqslant k$.*

Now we are able to establish an extension of Erdős theorem, then of Kürschák's Theorem.

Theorem 1.5. *Let a, d and k be positive integers satisfying $k \geqslant 2$, and $a, a+d, a+2d, \ldots, a+(k-1)\,d$ be an arithmetical progression. Then for all positive integers $\alpha_0, \alpha_1, \ldots, \alpha_{k-1}$ the rational number*

$$\frac{1}{a^{\alpha_0}} + \frac{1}{(a+d)^{\alpha_1}} + \cdots + \frac{1}{(a+(k-1)\,d)^{\alpha_{k-1}}}$$

is never an integer.

Proof. Let $\delta := \gcd(a,d)$. Consider the arithmetical progression $(a' + jd')$, $j = 0, \ldots, k-1$, where $a' = a/\delta$ and $d' = d/\delta$. For this progression, let P the prime given by Theorem 1.4. If $P \nmid \delta$, we conclude by using Corollary 1.2. Otherwise, we have

$$\frac{1}{a^{\alpha_0}} + \frac{1}{(a+d)^{\alpha_1}} + \cdots + \frac{1}{(a+(k-1)\,d)^{\alpha_{k-1}}} < \frac{k}{P} \leqslant 1.$$

□

Acknowledgement. The authors are grateful to the referee and would like to thank him/her for comments and several suggestions which improved the quality of this paper.

References

[1] Bachman, G., Introduction to p-adic numbers and valuation theory, *Academic Press, N.Y.* (1964).

[2] Erdős, P., Verallgemeinerung eines elementar-zahlentheoretischen Satzes von Kürschák (Generalization of an elementary number-theoretic theorem of Kürschák.), *Mat. Fiz. Lapok* 39 (1932), 17–24.

[3] Hoffman, P., The man who loved only numbers: The story of Paul Erdős and the search for mathematical truth, *N.Y. Hyperion* (1998).

[4] Shorey, T.N. and Tijdeman, R., On the greatest prime factor of an arithmetical progression, in “A tribute of Paul Erdős”, Edited by A. Baker, B. Bollobas, and A. Hainal. *Cambridge University Press* (1990), 385–389.

Hacène Belbachir
Abdelkader Khelladi
USTHB/ Faculté de Mathématiques
BP 32, El Alia, 16111 Bab Ezzouar, Alger
Algeria

Annales Mathematicae et Informaticae
34 (2007) pp. 33–45
http://www.ektf.hu/tanszek/matematika/ami

Distribution of terms of a logarithmic sequence*

Peter Csiba[a], Ferdinánd Filip[a], János T. Tóth[ab]

[a]Department of Mathematics, J. Selye University

e-mail: csiba.peter@selyeuni.sk
e-mail: filip.ferdinand@selyeuni.sk
e-mail: toth.janos@selyeuni.sk

[b]Department of Mathematics, University of Ostrava
e-mail: janos.toth@osu.cz

Submitted 22 October 2007; Accepted 28 November 2007

Abstract

The number $L(a,b) = \frac{a-b}{\ln a - \ln b}$ for $a \neq b$ and $L(a,a) = a$, is said to be the logarithmic mean of the positive numbers a, b. We shall say that a sequence $(a_n)_{n=1}^{\infty}$ with positive terms is a logarithmic sequence if $a_n = L(a_{n-1}, a_{n+1})$. In the present paper some basic estimations of the terms of logarithmic sequences are investigated.

Keywords: logarithmic mean, power mean, logarithmic sequence.

MSC: Primary 11K31, Secondary 26E60.

1. Introduction

Let a, b be positive real numbers. The logarithmic mean of a, b is defined as follows:

$$L(a,b) = \frac{a-b}{\ln a - \ln b} \quad \text{if} \quad a \neq b \quad \text{and} \quad L(a,a) = a$$

(see [5]).

The logarithmic sequence is defined in paper [2] by means of logarithmic mean in the following way:

*Supported by grants VEGA no. 1/4006/07, GAČR no. 201/07/0191.

Definition 1.1. A sequence $(a_n)_{n=1}^{\infty}$ of positive real numbers is called logarithmic if

$$a_n = L(a_{n-1}, a_{n+1}) \text{ for each } n \geqslant 2.$$

Moreover, in [2] the existence of logarithmic sequence is proved and even it is shown that if a sequence $(a_n)_{n=1}^{\infty}$ is logarithmic and $a_1 < a_2$ then $a_1 < a_2 < \dots < a_n < \cdots$. On the other hand, if $a_1 > a_2$ then $a_1 > a_2 > \dots > a_n > \cdots$ (see [2], Theorem 2.1). Thus we see that the logarithmic sequence is either increasing or decreasing if $a_1 \neq a_2$. In the case $a_1 = a_2$ the logarithmic sequence $(a_n)_{n=1}^{\infty}$ is stationary and $a_n = a_1$ $(n = 1, 2, \dots)$. In the present paper we will consider only the logarithmic sequences $(a_n)_{n=1}^{\infty}$ for which $a_1 \neq a_2$.

The following theorem holds for logarithmic sequences.

Theorem 1.2. ([2; Th. 2.2., Th. 2.3.]) *Let the sequence $(a_n)_{n=1}^{\infty}$ be logarithmic and $a_1 \neq a_2$. Then the following implications hold.*

(i) *If $a_1 < a_2$ then*

$$\lim_{n\to\infty} a_n = \infty.$$

(ii) *If $a_1 > a_2$ then the series*

$$\sum_{n=1}^{\infty} a_n$$

converges.

Now we introduce the power mean of degree $\alpha \in \mathbb{R}$ of two positive numbers a, b as follows:

$$M_\alpha(a,b) = \left(\frac{a^\alpha + b^\alpha}{2}\right)^{\frac{1}{\alpha}} \text{ if } \alpha \neq 0 \ \text{ and } \ M_0(a,b) = \lim_{\alpha\to 0} M_\alpha(a,b).$$

It is well known that $M_0(a,b) = \sqrt{a.b}$ and $M_\alpha(a,b)$ is increasing with respect to α (see [6]).

In paper [3] the following relation between $L(a,b)$ and $M_\alpha(a,b)$ is proved for arbitrary positive numbers a, b:

$$M_0(a,b) \leqq L(a,b) \leqq M_{\frac{1}{3}}(a,b), \tag{1.1}$$

and the equality occurs if and only if $a = b$.

As $M_\alpha(a,b)$ is increasing with respect to α, from (1.1) we have

$$M_0(a,b) \leqq L(a,b) \leqq M_\alpha(a,b) \tag{1.2}$$

for all $a, b > 0$ and $\alpha \geqslant \frac{1}{3}$.

Thus, if the sequence $(a_n)_{n=1}^{\infty}$ is logarithmic then (1.2) implies that for all $n \geqslant 2$ and $\alpha \geqslant \frac{1}{3}$ the inequality

$$\sqrt{a_{n-1}a_{n+1}} \leqslant a_n \leqslant \left(\frac{a_{n-1}^\alpha + a_{n+1}^\alpha}{2}\right)^{\frac{1}{\alpha}}$$

holds. Consequently we have for all $n \geqslant 2$ and $\alpha \geqslant \frac{1}{3}$

$$\frac{a_{n+1}}{a_n} \leqslant \frac{a_n}{a_{n-1}} \quad \text{and} \quad a_n^\alpha - a_{n-1}^\alpha \leqslant a_{n+1}^\alpha - a_n^\alpha. \tag{1.3}$$

From (1.3) we obtain that in the case of increasing logarithmic sequence $(a_n)_{n=1}^\infty$ for each $n \geqslant 2$ the inequalities

$$1 < \frac{a_{n+1}}{a_n} < \frac{a_n}{a_{n-1}} \quad \text{and} \quad 0 < a_n - a_{n-1} < a_{n+1} - a_n \tag{1.4}$$

hold.

A natural question arises. What can be said about the asymptotic behaviour of differences $a_{n+1} - a_n$ and fractions $\frac{a_{n+1}}{a_n}$ if $(a_n)_{n=1}^\infty$ is an increasing logarithmic sequence? More precisely, does it hold

$$\lim_{n\to\infty} (a_{n+1} - a_n) = \infty \quad \text{and} \quad \lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 1\ ? \tag{1.5}$$

In the first part of the present paper, among others, we give the answer to the previous question. We will determine the lower bounds for terms a_n, differences $a_{n+1} - a_n$ and fractions $\frac{a_{n+1}}{a_n}$ if $(a_n)_{n=1}^\infty$ is a logarithmic sequence.

2. Estimates for differences and quotients of consecutive terms of a logarithmic sequence

Theorem 2.1. *Let $(a_n)_{n=1}^\infty$ be a logarithmic sequence. Then the following implications hold.*

(i) *If $(a_n)_{n=1}^\infty$ is increasing then*

$$a_n > \left(\frac{{a_2}^\alpha - {a_1}^\alpha}{2}\right)^{\frac{1}{\alpha}} n^{\frac{1}{\alpha}} \tag{2.1}$$

for every $\alpha \geqslant \frac{1}{3}$ and $n \in \mathbb{N}$.

(ii) *If $(a_n)_{n=1}^\infty$ is decreasing then*

$$a_n < \left(\frac{{a_2}^\beta - {a_1}^\beta}{2}\right)^{\frac{1}{\beta}} n^{\frac{1}{\beta}} \tag{2.2}$$

for every $\beta < 0$ and $n \in \mathbb{N}$.

Proof. (i) Let $(a_n)_{n=1}^\infty$ be an increasing logarithmic sequence. Then (1.3) implies for $\alpha \geqslant \frac{1}{3}$

$$a_n^\alpha - a_{n-1}^\alpha < a_{n+1}^\alpha - a_n^\alpha \quad \text{for} \quad n \geqslant 2.$$

Consequently, for every $n \geqslant 2$ we have

$$a_2^\alpha - a_1^\alpha < a_{n+1}^\alpha - a_n^\alpha, \text{ i.e.}$$

$$(a_n^\alpha + a_2^\alpha - a_1^\alpha)^{\frac{1}{\alpha}} < a_{n+1}. \tag{2.3}$$

Now we will show by induction the inequality

$$((n-1)a_2^\alpha - (n-2)a_1^\alpha)^{\frac{1}{\alpha}} \leqslant a_n \tag{2.4}$$

for every $n \geqslant 2$. For $n = 2$ evidently the equality takes place in (2.4). Suppose that (2.4) holds for some $n = k \geqslant 2$. The we obtain

$$\begin{aligned}(ka_2^\alpha - (k-1)a_1^\alpha)^{\frac{1}{\alpha}} = ((k-1)a_2^\alpha - (k-2)a_1^\alpha + a_2^\alpha - a_1^\alpha)^{\frac{1}{\alpha}} \leqslant \\ \leqslant (a_k^\alpha + a_2^\alpha - a_1^\alpha)^{\frac{1}{\alpha}}.\end{aligned}$$

Consequently, using (2.3) we obtain

$$(ka_2^\alpha - (k-1)a_1^\alpha)^{\frac{1}{\alpha}} \leqslant a_{k+1}$$

proving (2.4) for every $n \geqslant 2$. Finally, for $n \geqslant 2$ we obtain

$$a_n \geqslant ((n-1)(a_2^\alpha - a_1^\alpha) + a_1^\alpha)^{\frac{1}{\alpha}} > (n-1)^{\frac{1}{\alpha}} (a_2^\alpha - a_1^\alpha)^{\frac{1}{\alpha}} \geqslant n^{\frac{1}{\alpha}} \left(\frac{a_2^\alpha - a_1^\alpha}{2}\right)^{\frac{1}{\alpha}}.$$

(ii) Let $(a_n)_{n=1}^\infty$ be a decreasing logarithmic sequence. Then (1.2) and the fact that $M_\alpha(a,b)$ is increasing with respect to α imply the inequality

$$\left(\frac{a_{n-1}^\beta + a_{n+1}^\beta}{2}\right)^{\frac{1}{\beta}} < a_n = L(a_{n-1}, a_{n+1})$$

holding for every real $\beta < 0$. Consequently

$$a_n^\beta - a_{n-1}^\beta < a_{n+1}^\beta - a_n^\beta$$

holds for every $n \geqslant 2$. Especially,

$$a_{n+1}^\beta - a_n^\beta > a_2^\beta - a_1^\beta\ , \quad \text{i.e.}$$

$$a_{n+1} < \left(a_n^\beta + a_2^\beta - a_1^\beta\right)^{\frac{1}{\beta}} \tag{2.5}$$

holds for every $n \geqslant 2$. Now we will show by induction the inequality

$$a_n \leqq \left((n-1)a_2^\beta - (n-2)a_1^\beta\right)^{\frac{1}{\beta}} \tag{2.6}$$

for every $n \geqslant 2$. In the case $n = 2$ the equality takes place in (2.6). Suppose that (2.6) holds for some $n = k \geqslant 2$. The we obtain

$$\left(ka_2^\beta - (k-1)a_1^\beta\right)^{\frac{1}{\beta}} = \left((k-1)a_2^\beta - (k-2)a_1^\beta + a_2^\beta - a_1^\beta\right)^{\frac{1}{\beta}} \geqslant$$

$$\geqslant \left(a_k^\beta + a_2^\beta - a_1^\beta\right)^{\frac{1}{\beta}}.$$

Applying (2.5) we obtain

$$\left(ka_2^\beta - (k-1)a_1^\beta\right)^{\frac{1}{\beta}} \geqslant a_{k+1}$$

proving (2.6) for every integer $n \geqslant 2$. Finally, for every $n \geqslant 2$ we have

$$a_n \leqq \left((n-1)(a_2^\beta - a_1^\beta) + a_1^\beta\right)^{\frac{1}{\beta}} <$$

$$< \left(a_2^\beta - a_1^\beta\right)^{\frac{1}{\beta}} \frac{1}{(n-1)^{-\frac{1}{\beta}}} \leqq \left(\frac{a_2^\beta - a_1^\beta}{2}\right)^{\frac{1}{\beta}} \frac{1}{n^{-\frac{1}{\beta}}}.$$

□

Corollary 2.2. *Let $(a_n)_{n=1}^\infty$ be an increasing logarithmic sequence. Then for every $n \geqslant 2$ the inequality*

$$a_n > \left(\frac{\sqrt[3]{a_2} - \sqrt[3]{a_1}}{2}\right)^3 n^3$$

holds.

Proof. Follows directly from Theorem 2.1 *(i)* for $\alpha = \frac{1}{3}$. □

Corollary 2.3. *If $(a_n)_{n=1}^\infty$ is an increasing logarithmic sequence then the series*

$$\sum_{n=1}^{\infty} \frac{1}{a_n}$$

converges.

Proof. By Corollary 2.2 we have for every $n \geqslant 2$

$$a_n > c.n^3 \quad \text{where} \quad c = \left(\frac{\sqrt[3]{a_2} - \sqrt[3]{a_1}}{2}\right)^3.$$

Evidently the series $\sum\limits_{n=2}^{\infty} \frac{1}{cn^3}$ majorises the series $\sum\limits_{n=2}^{\infty} \frac{1}{a_n}$. Consequently the series $\sum\limits_{n=1}^{\infty} \frac{1}{a_n}$ converges. □

Corollary 2.4. *Let $(a_n)_{n=1}^{\infty}$ be a decreasing logarithmic sequence and let $l > 0$ be a real number. Then the inequality*

$$a_n < c_1 \frac{1}{n^{\frac{1}{l}}}, \quad \textit{where} \quad c_1 = \left(\frac{a_2^{-l} - a_1^{-l}}{2} \right)^{-\frac{1}{l}}$$

holds for every $n \geqslant 2$.

Proof. Follows from Theorem 2.1 (ii) for $\beta = -l,\ l > 0$. □

Corollary 2.5. *If $(a_n)_{n=1}^{\infty}$ is a decreasing logarithmic sequence then the series $\sum\limits_{n=1}^{\infty} a_n$ converges.*

Theorem 2.6. *Let $(a_n)_{n=1}^{\infty}$ be an increasing logarithmic sequence. Then the inequality*

$$a_{n+1} - a_n > (\sqrt{a_2} - \sqrt{a_1})^2 (n+1) \tag{2.7}$$

holds for every $n \geqslant 2$.

Proof. We will proceed by induction. From (1.3) for $\alpha = \frac{1}{2}$ follows the inequality

$$\sqrt{a_n} - \sqrt{a_{n-1}} < \sqrt{a_{n+1}} - \sqrt{a_n}. \tag{2.8}$$

For $n = 2$ we obtain from (2.8)

$$\sqrt{a_3} - \sqrt{a_2} > \sqrt{a_2} - \sqrt{a_1}$$

and

$$a_3 - a_2 > (\sqrt{a_2} - \sqrt{a_1})(\sqrt{a_3} + \sqrt{a_2}) > 3(\sqrt{a_2} - \sqrt{a_1})(\sqrt{a_2} - \sqrt{a_1}).$$

Suppose that (2.7) holds for some $n = k \geqslant 2$. Then from (2.8) for $n = k+1$ we obtain

$$\sqrt{a_{k+2}} - \sqrt{a_{k+1}} > \sqrt{a_{k+1}} - \sqrt{a_k}.$$

Moreover

$$a_{k+2} - a_{k+1} > (a_{k+1} - a_k) \frac{\sqrt{a_{k+2}} + \sqrt{a_{k+1}}}{\sqrt{a_{k+1}} + \sqrt{a_k}} =$$

$$= (a_{k+1} - a_k) + (a_{k+1} - a_k) \frac{\sqrt{a_{k+2}} - \sqrt{a_k}}{\sqrt{a_{k+1}} + \sqrt{a_k}} =$$

$$= (a_{k+1} - a_k) + (\sqrt{a_{k+1}} - \sqrt{a_k})(\sqrt{a_{k+2}} - \sqrt{a_k}) >$$

$$> (a_{k+1} - a_k) + (\sqrt{a_{k+1}} - \sqrt{a_k})^2.$$

As (2.8) implies

$$\sqrt{a_{k+1}} - \sqrt{a_k} > \sqrt{a_2} - \sqrt{a_1}$$

we have

$$a_{k+2} - a_{k+1} > a_{k+1} - a_k + (\sqrt{a_2} - \sqrt{a_1})^2.$$

Finally

$$a_{k+2} - a_{k+1} > (k+2)(\sqrt{a_2} - \sqrt{a_1})^2.$$

□

Theorem 2.7. *Let $(a_n)_{n=1}^{\infty}$ be a logarithmic sequence. Then $\lim\limits_{n\to\infty} \frac{a_{n+1}}{a_n}$ exists and the following implications hold.*

1. *If $(a_n)_{n=1}^{\infty}$ is increasing then*

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 1.$$

2. *If $(a_n)_{n=1}^{\infty}$ is decreasing then*

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n} = 0.$$

Proof. The sequence $(a_n)_{n=1}^{\infty}$ is logarithmic, thus

$$a_n = \frac{a_{n+1} - a_{n-1}}{\ln a_{n+1} - \ln a_{n-1}} \quad \text{for } n \geqslant 2.$$

Consequently

$$\frac{a_n}{a_{n-1}} = \frac{\frac{a_{n+1}}{a_{n-1}} - 1}{\ln \frac{a_{n+1}}{a_{n-1}}}$$

which is equivalent with

$$\frac{a_n}{a_{n-1}} \ln \frac{a_{n+1}}{a_n} \frac{a_n}{a_{n-1}} = \frac{a_{n+1}}{a_n} \frac{a_n}{a_{n-1}} - 1. \tag{2.9}$$

The first relation in (1.3) implies that the sequence $\left(\frac{a_{n+1}}{a_n}\right)_{n=1}^{\infty}$ is decreasing and bounded from below. Consequently the limit $\lim\limits_{n\to\infty} \frac{a_{n+1}}{a_n}$ exists and it is finite. Denote $x = \lim\limits_{n\to\infty} \frac{a_{n+1}}{a_n}$.

If the sequence $(a_n)_{n=1}^{\infty}$ is increasing then obviously $x \geqslant 1$. Taking limit in (2.9) for $n \to \infty$ we obtain

$$x \ln x^2 = x^2 - 1 \quad \text{i.e.} \quad 2x \ln x = x^2 - 1.$$

The above inequality can not hold for $x > 1$ since for all real $x \in (0,1) \cup (1,\infty)$ the inequality $2x \ln x < x^2 - 1$ holds. Thus $\lim\limits_{n\to\infty} \frac{a_{n+1}}{a_n} = 1$.

If the sequence $(a_n)_{n=1}^{\infty}$ is decreasing then obviously $0 \leqslant x < 1$. In the case $0 < x < 1$ again we obtain $2x \ln x = x^2 - 1$ what is impossible. Thus we have $\lim\limits_{n\to\infty} \frac{a_{n+1}}{a_n} = 0$ in the case of a decreasing sequence $(a_n)_{n=1}^{\infty}$. □

Corollary 2.8. *Let $(a_n)_{n=1}^{\infty}$ be a logarithmic sequence. Then*

$$\lim_{n\to\infty} \frac{a_n}{q^n} = 0$$

1. *for every real $q > 1$ if $(a_n)_{n=1}^{\infty}$ is increasing,*
2. *for every real $q > 0$ if $(a_n)_{n=1}^{\infty}$ is decreasing.*

Proof. 1. Consider the power series

$$\sum_{n=1}^{\infty} a_n x^n \, .$$

Then Theorem 2.7 implies that the radius of its convergence is $R = 1$. Thus for every $0 < x < 1$ the series $\sum\limits_{n=1}^{\infty} a_n x^n$ converges. Consequently

$$\lim_{n\to\infty} a_n x^n = 0.$$

Denoting $q = \frac{1}{x}$ we have $q > 1$ arbitrary and $\frac{a_n}{q^n} \to 0 \quad (n \to \infty)$ holds.
2. If $(a_n)_{n=1}^{\infty}$ is decreasing then Theorem 2.7 implies that the radius of convergence R of the considered power series is infinity. Thus for every real $x > 0$ we have $\lim\limits_{n\to\infty} a_n x^n = 0$. □

Corollary 2.9. *If $(a_n)_{n=1}^{\infty}$ is an increasing logarithmic sequence then the set*

$$\left\{ \frac{a_m}{a_n} : \ m, n = 1, 2, \dots \right\}$$

is dense in $(0, \infty)$.

Proof. The proof follows from Theorem 2.7 and the following theorem: If for an unbounded sequence $(a_n)_{n=1}^{\infty}$ of positive real numbers

$$\limsup_{n\to\infty} \frac{a_{n+1}}{a_n} = 1$$

holds then the set $\left\{ \frac{a_m}{a_n} : \ m, n = 1, 2, \dots \right\}$ is dense in $(0, \infty)$ (see Theorem 1.1 of [1]). □

3. Comparison of terms of logarithmic sequence with terms of other sequences

First we will show that the function $L(x, b)$ is increasing in $x > 0$ with fixed $b > 0$. This property of the function $L(x, b)$ will be later used in the proof of Theorem 3.3.

Theorem 3.1. *Let $a, b, c, \in \mathbb{R}^+$. Then*

$$L(c,b) \leqslant L(a,b) \quad \Leftrightarrow \quad c \leqslant a.$$

Proof. For $0 < x \neq b$ we have

$$L(x,b) = b\frac{\frac{x}{b} - 1}{\ln \frac{x}{b}}.$$

Thus $L(x,b)$ is increasing with respect to x if and only if the function

$$f(y) = b\frac{y-1}{\ln y}$$

is increasing with respect to y $(y \neq 1)$, i.e. $\frac{df}{dy} \geqslant 0$ for $y > 0$, $y \neq 1$. This is equivalent to

$$g(y) = \frac{1}{y} + \ln y - 1 \geqslant 0$$

for each $y > 0$. Since $\frac{dg}{dy} = \frac{1}{y} - \frac{1}{y^2} = \frac{y-1}{y^2}$ we obviously have $\frac{dg}{dy} \leqslant 0$ for $0 < y < 1$ and $\frac{dg}{dy} \geqslant 0$ for $y \geqslant 1$. Thus $g(y)$ attains its minimum at $y = 1$, i.e. $g(y) \geqslant g(1) = 0$ for each $y > 0$. □

First we are going to compare the terms of a given logarithmic sequence with terms of another logarithmic sequence.

Theorem 3.2. *Let $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ be such logarithmic sequences that $a_1 = b_1$ and $a_2 \geqslant b_2$. Then*

$$a_n \geqslant b_n \quad \textit{and} \quad \frac{a_n}{a_{n-1}} \geqslant \frac{b_n}{b_{n-1}}$$

hold for every $n \geqslant 2$.

Proof. We will proceed by induction. For $n = 2$ the statement obviously holds. Assume that it holds for some $n = k \geqslant 2$, i.e.

$$a_k \geqslant b_k \quad \text{and} \quad \frac{a_k}{a_{k-1}} \geqslant \frac{b_k}{b_{k-1}}. \tag{3.1}$$

Let us consider the terms a_{k+1}, b_{k+1}. Since both $(a_n)_{n=1}^{\infty}$ and $(b_n)_{n=1}^{\infty}$ are logarithmic sequences, we have

$$a_k = L(a_{k-1}, a_{k+1}) \quad \text{and} \quad b_k = L(b_{k-1}, b_{k+1}).$$

Consequently

$$\frac{a_k}{a_{k-1}} = L\left(\frac{a_{k+1}}{a_{k-1}}, 1\right) \quad \text{and} \quad \frac{b_k}{b_{k-1}} = L\left(\frac{b_{k+1}}{b_{k-1}}, 1\right). \tag{3.2}$$

We will use the notation

$$\alpha_1 = \frac{a_k}{a_{k-1}},\ \alpha_2 = \frac{a_{k+1}}{a_{k-1}},\ \beta_1 = \frac{b_k}{b_{k-1}} \quad \text{and} \quad \beta_2 = \frac{b_{k+1}}{b_{k-1}}$$

in the rest of the proof. Then (3.2) implies

$$\frac{\alpha_1}{\beta_1} = \frac{L(\alpha_2,1)}{L(\beta_2,1)} = \frac{\alpha_2 - 1}{\beta_2 - 1} \cdot \frac{\ln \beta_2}{\ln \alpha_2} = \frac{\alpha_2^{\frac{1}{2}}+1}{\beta_2^{\frac{1}{2}}+1} \cdot \frac{\alpha_2^{\frac{1}{2}}-1}{\beta_2^{\frac{1}{2}}-1} \cdot \frac{\ln \beta_2^{\frac{1}{2}}}{\ln \alpha_2^{\frac{1}{2}}} =$$

$$= \frac{\alpha_2^{\frac{1}{2}}+1}{\beta_2^{\frac{1}{2}}+1} \cdot \frac{\alpha_2^{\frac{1}{4}}+1}{\beta_2^{\frac{1}{4}}+1} \cdot \frac{\alpha_2^{\frac{1}{4}}-1}{\beta_2^{\frac{1}{4}}-1} \cdot \frac{\ln \beta_2^{\frac{1}{4}}}{\ln \alpha_2^{\frac{1}{4}}} = \cdots = \left(\prod_{k=1}^{n} \frac{\alpha_2^{\frac{1}{2^k}}+1}{\beta_2^{\frac{1}{2^k}}+1}\right) \cdot \frac{\alpha_2^{\frac{1}{2^n}}-1}{\beta_2^{\frac{1}{2^n}}-1} \cdot \frac{\ln \beta_2^{\frac{1}{2^n}}}{\ln \alpha_2^{\frac{1}{2^n}}}.$$

Taking into account that $\frac{a+1}{b+1} \leqslant \frac{a}{b}$ holds in the case when $a \geqslant b > 0$, we obtain:

$$\frac{\alpha_1}{\beta_1} \leqslant \left(\frac{\alpha_2}{\beta_2}\right)^{\sum\limits_{k=1}^{n} \frac{1}{2^k}} \cdot \frac{L\left(\alpha_2^{\frac{1}{2^n}}, 1\right)}{L\left(\beta_2^{\frac{1}{2^n}}, 1\right)}.$$

taking limit for $n \to \infty$ we obtain $\frac{\alpha_1}{\beta_1} \leqslant \frac{\alpha_2}{\beta_2}$ as

$$\lim_{n\to\infty} L\left(a^{\frac{1}{2^n}}, 1\right) = 1 \quad \text{where} \quad a > 0.$$

The inequality $\frac{\alpha_1}{\beta_1} \leqslant \frac{\alpha_2}{\beta_2}$ is equivalent with the inequality $\frac{a_{k+1}}{a_k} \geqslant \frac{b_{k+1}}{b_k}$. Since $a_k \geqslant b_k$ using the induction assumption (3.1) we obtain $a_{k+1} \geqslant b_{k+1}$ which completes the proof.

□

The next theorem generalizes the previous one.

Theorem 3.3. *Let $(a_n)_{n=1}^{\infty}$ be a logarithmic sequence and let a sequence $(b_n)_{n=1}^{\infty}$ fulfils the following conditions*

$$b_1 = a_1,\ b_2 \leqslant a_2 \quad \textit{and} \quad b_n \geqslant L(b_{n-1}, b_{n+1}) \quad \textit{for} \quad n \geqslant 2 \tag{3.3}$$

Then for every positive integer n the inequality

$$a_n \geqslant b_n$$

holds.

Proof. Let $k \geqslant 0$ be a given integer. Define the sequence $(a_{k,n})_{n=1}^{\infty}$ as follows:

$$a_{k,1} = b_{k+1},\ a_{k,2} = b_{k+2} \quad \text{and} \quad a_{k,n} = L(a_{k,n-1}, a_{k,n+1}) \quad \text{for} \quad n \geqslant 2. \tag{3.4}$$

Thus the sequence $(a_{k,n})_{n=1}^{\infty}$ is logarithmic for every $k \geqslant 0$.
We will show that

$$a_{k,n} \leqslant a_{k+n} \quad \text{and} \quad b_{k+3} \leqslant a_{k,3} \tag{3.5}$$

holds for every integer $k \geqslant 0$ and positive integer n. We will proceed by induction with respect to k.
For $k = 0$ from (3.3), (3.4) we have

$$a_{0,1} = b_1 = a_1, \quad a_{0,2} = b_2 \leqslant a_2.$$

The assumption that both sequences $(a_n)_{n=1}^{\infty}$ and $(a_{0,n})_{n=1}^{\infty}$ are logarithmic and Theorem 3.2 imply that for every $n \in \mathbb{N}$ the inequality

$$a_{0,n} \leqslant a_n$$

holds. On the other hand, (3.3) and (3.4) imply

$$L(b_3, b_1) \leqslant b_2 = a_{0,2} = L(a_{0,3}, a_{0,1}) = L(a_{0,3}, b_1),$$

and consequently, using Theorem 3.1, we obtain

$$b_3 \leqslant a_{0,3}.$$

Suppose that for some $k = l \geqslant 0$ inequalities (3.5) hold. In the case $k = l + 1$ we obtain

$$a_{l+1,1} = b_{l+2} = a_{l,2} \quad \text{and} \quad a_{l+1,2} = b_{l+3} \leqslant a_{l,3}.$$

By use of Theorem 3.2 and induction assumption we obtain

$$a_{l+1,n} \leqslant a_{l,n+1} \leqslant a_{l+1+n}$$

for every $n \in \mathbb{N}$. On the other hand, (3.3) and (3.4) imply

$$L(b_{l+4}, b_{l+2}) \leqslant b_{l+3} = a_{l+1,2} = L(a_{l+1,3}, a_{l+1,1}).$$

As $b_{l+2} = a_{l+1,1}$, Theorem 3.1 implies

$$b_{l+4} \leqslant a_{l+1,3}.$$

Thus we proved (3.5) by induction. Finally, from (3.5) we obtain

$$b_k \leqslant a_{k-3,3} \leqslant a_k$$

for every $k \geqslant 3$. □

The proof of the following theorem is an application of the previous one.

Theorem 3.4. *Let $(a_n)_{n=1}^{\infty}$ be such a logarithmic sequence that $a_1 < a_2$. Then the series $\sum\limits_{n=1}^{\infty} \frac{1}{a_n}$ converges and*

$$\sum_{n=1}^{\infty} \frac{1}{a_n} < \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{(\sqrt{a_2} - \sqrt{a_1})^2} \frac{\pi^2}{6}$$

holds.

Proof. Define the sequence $(b_n)_{n=1}^{\infty}$ by:

$$b_1 = a_1,\ b_2 = a_2 \quad \text{and} \quad b_n = M_{\frac{1}{2}}(b_{n-1}, b_{n+1}) \quad \text{for} \quad n \geqslant 2.$$

As

$$M_{\frac{1}{2}}(b_{n-1}, b_{n+1}) \geqslant L(b_{n-1}, b_{n+1}),$$

we have $b_n \geqslant L(b_{n-1}, b_{n+1})$. Thus the sequence $(b_n)_{n=1}^{\infty}$ fulfils the assumptions of Theorem 3.2.
Consequently $b_n \leqslant a_n$ for every $n \in \mathbb{N}$. Using ([2] Th.1.1) we have

$$b_n = \left((n-1)\sqrt{b_2} - (n-2)\sqrt{b_1}\right)^2,$$

i.e. for every $n > 2$

$$b_n = \left((n-2)(\sqrt{b_2} - \sqrt{b_1}) + \sqrt{b_2}\right)^2 > (n-2)^2 \left(\sqrt{b_2} - \sqrt{b_1}\right)^2 =$$
$$= (n-2)^2 \left(\sqrt{a_2} - \sqrt{a_1}\right)^2$$

holds. Finally we obtain

$$\sum_{n=1}^{\infty} \frac{1}{a_n} \leqslant \sum_{n=1}^{\infty} \frac{1}{b_n} < \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{(\sqrt{a_2} - \sqrt{a_1})^2} \frac{\pi^2}{6}.$$

□

References

[1] Andrica, D. and Buzeteanu, S., Relatively dense universal sequences for the class of continuous periodical functions of period T, *L'analyse Numérique et la Théorie de L'approximation*, Vol. 16 (1987) no. 1, 1–9.

[2] Bukor, J., Šalát, T., Tóth, J. and Zsilinszky, L., Means of positive numbers and certain types of series, *Acta Mathematica et Informatica Nitra*, Vol. 1 (1992) 49–57.

[3] Bukor, J., Tóth, J. and Zsilinszky, L., The logarithmic mean and the power mean of positive numbers *Octogon (Brasov)* Vol. 2 (1994) 19–24.

[4] Carlson, B.C., Algorithms involving arithmetic and geometric means *Amer. Math. Monthly* Vol. 78 (1971) 496–505.

[5] Carlson, B.C., The logarithmic mean *Amer. Math. Monthly* Vol. 79 (1972) 615–618.

[6] Pólya, G. and Szegő, G., Problems and Theorems in Analysis, I *Springer–Verlag, Berlin, Heidelberg* (1962).

Peter Csiba, **Ferdinánd Filip**, **János T. Tóth**
Department of Mathematics,
J. Selye University,
P.O.Box 54,
945 01 Komárno,
Slovakia

János T. Tóth
Department of Mathematics,
University of Ostrava,
30. dubna 22,
701 03 Ostrava,
Czech Republic

Annales Mathematicae et Informaticae
34 (2007) pp. 47–49
http://www.ektf.hu/tanszek/matematika/ami

On group rings with restricted minimum condition

Bertalan Király

Institute of Mathematics and Informatics, Eszterházy Károly College
e-mail: kiraly@ektf.hu

Submitted 28 September 2007; Accepted 18 December 2007

Abstract

In this paper we investigate the group rings RG satisfying the restricted minimum condition.

Keywords: restricted minimum condition, group ring

MSC: 16S34

1. Results

Let R be an associative ring with unit element. R is said to satisfy the left restricted minimum condition, if for each nontrivial ideal J of R the ring R/J is left artinian. In this paper we consider the group rings with left restricted minimum condition, in the case when RG itself is not left artinian.

We prove the following:

Theorem 1.1. *Let G be a group with non-trivial center and let R be a commutative ring with unit element. If the group ring RG satisfies the left restricted minimum condition, then R is left artinian and either G is finite, or G is the infinite cyclic group.*

For group algebras the converse assertion is also true.

Theorem 1.2. *Let G be a group with non-trivial center and let R be a field. The group algebra RG satisfies the left restricted minimum condition if and only if either G is finite, or G is the infinite cyclic group.*

By $A(RG)$ we mean the augmentation ideal of RG, that is the kernel of the ring homomorphism $\phi : RG \to R$ sending each group element to 1. It is easy to see that

$A(RG)$ is a free R-module in which the set of the elements $g-1$ with $1 \neq g \in G$ form a basis. For a normal subgroup H of G we denote by $I(H)$ the ideal of RG generated by all elements of the form $h-1$ with $h \in H$. As it is well-known, $I(H)$ is the kernel of the natural epimorphism $\overline{\phi} : RG \to R[G/H]$ induced by the group homomorphism ϕ of G onto G/H, furthermore

$$RG/I(H) \cong R[G/H], \tag{1.1}$$

and $I(G) = A(RG)$.

The commutator subgroup and the center of the group G will be denoted by G' and $\zeta(G)$, respectively.

2. Proof of Theorems

We need the following two statements.

Proposition 2.1 (Theorem 4.12 in [2]). *If G is a group whose center has finite index n, then G' is finite and $(G')^n = 1$.*

Proposition 2.2 (Theorem 4.33 in [2]). *An infinite group has each non-trivial subgroup of finite index if and only if it is infinite cyclic.*

Proof of Theorem 1.1. It is well-known that the group ring RG is left artinian if and only if R is left artinian and G is finite. Assume that RG satisfies the left restricted minimum condition. According to (1.1) for every normal subgroup H the factor group G/H is finite and from the isomorphism $RG/A(RG) \cong R$ it follows that R is left artinian. Furthermore, $RG/I(\zeta(G))$ is left artinian and therefore, by (1.1), $G/\zeta(G)$ is finite. Then Proposition 2.1 guarantees that G' is finite. If $G' \neq 1$ then, by (1.1) G/G' is finite, and so G is finite. On the other hand, if G is abelian and infinite, then by (1.1) we have that every non-trivial subgroup of G has finite index. But then Proposition 2.2 states that G is the infinite cyclic group and the proof of the theorem is complete. □

Let R be an euclidean ring with the euclidean norm φ such that $\varphi(ab) \geqslant \varphi(a)$ for all $a \neq 0$, $b \neq 0$ $(a, b \in R.)$ Then R is a principal ideal ring. Let $I = (r)$ and $J = (s)$ be the ideals of R generated by the element r and s respectively, and assume that $I \supseteq J$. Then $s = rt$ for a suitable $t \in R$, and $\varphi(s) = \varphi(rt) \geqslant \varphi(r)$. It is easy to see that $\varphi(e) = 1$ if and only if e is an unit in R and that $I = J$ if and only if $\varphi(r) = \varphi(s)$.

Let $J = (s)$ be an arbitrary ideal of an euclidean ring R and let

$$\overline{R} \supseteq \overline{J}_1 \supseteq \overline{J}_2 \supseteq \ldots \supseteq \overline{J}_n \supseteq \ldots \supseteq \bigcap_{i=1}^{\infty} \overline{J}_i = \overline{J}_\omega \tag{2.1}$$

a sequence of ideals, where $\overline{R} = R/J$ and ω the first limit ordinal. Denote by J_k the inverse image of $\overline{J}_k$ in R ($k = 1, 2, \ldots$ or $k = \omega$). Then J_k's are principal ideals and, in view of (2.1) we have that

$$R \supseteq J_1 \supseteq J_2 \supseteq \ldots \supseteq J_n \supseteq \ldots \supseteq J_\omega \supseteq J = (s). \tag{2.2}$$

Suppose that $J_k = (s_k)$. Since $J_k \supseteq J = (s)$, so $\varphi(s) \geqslant \varphi(s_k)$ for all k $(k = 1, 2, \ldots$ and $k = \omega)$ But $\varphi(s)$ and $\varphi(s_k)$ are non-negative integers, therefore there exists a natural number n such that $\varphi(s_n) = \varphi(s_{n+1}) = \ldots = \varphi(s)$. Thus the sequence (2.2) has finite length and consequently, the sequence (2.1) is finite, too. It follows that for each ideal J of R the ring R/J is artinian, and we have

Lemma 2.3. *Euclidean rings satisfy the restricted minimum condition.*

It was prowed in [1] that the group algebra of the infinite cyclic group over a field is an euclidean ring. Hence, Theorem 1.2 is a direct consequence of Lemma 2.3 and Theorem 1.1.

References

[1] Király, B., Orosz, Gyuláné, Egy euklideszi gyűrű, *Acad. Paed. Agriensis, Sect. Math.* (1998), 71–76.

[2] Robinson, J.S., Finiteness Conditions and Generalized Soluble Groups, Part 1, *Springer-Verlag New York Heildelberg Berlin*, 1972.

Bertalan Király
Institute of Mathematics and Informatics
Eszterházy Károly College
H-3300 Eger
Leányka út 4
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 51–59
http://www.ektf.hu/tanszek/matematika/ami

On the shape parameter and constrained modification of GB-spline curves*

Yajuan Li[a], Miklós Hoffmann[b] and Guozhao Wang[c]

[a]School of Science, Hangzhou Dianzi University, Hangzhou, China

[b] Department of Mathematics, Károly Eszterházy College, Eger, Hungary

[c]Department of Mathematics, Zhejiang University, Hangzhou, China

Submitted 25 April 2007; Accepted 10 October 2007

Abstract

GB-spline curves can be considered as the generalization of B-spline curve incorporating a shape parameter into the polynomial basis functions. The geometric effect of the alteration of the shape parameter is discussed in this paper, including constrained shape control of the curve.

Keywords: GB-spline curves, shape parameter, paths, shape control, constrained modification

MSC: 68U05

1. Introduction

Although B-spline curve still plays central role in computer aided geometric design, the recently developed generalizations of this curve are also in the forefront of research. The well-known result of this attempt is the NURBS curve (c.f. [9]), but this curve has rational coefficient functions, yielding computational stability problems. Some recently developed methods tried to incorporate shape parameters into the original, polynomial basis functions. One of the earliest methods in this way is β-spline curve with two global parameters ([1, 2]). Further methods have been provided by direct generalization of B-spline curves as αB-splines in [8] and [10] and recently as GB-splines in [3]. Some alternative spline curves with shape parameters can be found in [4, 5, 6].

*Research supported by the Hungarian National Scientific Fund (OTKA No. T048523) and the National Office of Research and Technology (Project CHN-37/2005).

In this paper we examine the GB-spline curves. At first we study the effect of the shape parameter on the points of the curve, extending the method we applied for trigonometric CB-spline curves in [7]. In Section 2 we study the paths obtained by altering the shape parameter of the curve, and prove that points of the curve move along straight line segments. Applying this fact in Section 5 linear blending is used for constrained shape control, where the shape parameter is modified in a way that the new GB-spline curve passes through a given point.

2. GB-spline curve and its λ-paths

In [3] the GB-spline curve as a generalization of the classical uniform cubic B-spline curve with shape parameter has been introduced. The definition of an arc of a GB-spline curve with shape parameter λ is as follows.

Definition 2.1. Given a sequence of control points $P_i, (i = 0, \ldots, 3)$ the arc of the GB-spline curve is

$$C(\lambda, t) = \sum_{i=0}^{3} P_i b_i(\lambda, t), \quad \lambda \in [-8, \infty), \quad t \in [0, 1], \tag{2.1}$$

where the GB-spline basic functions are

$$\begin{aligned} b_0(\lambda, t) &= \frac{2}{12+\lambda}(1-t)^3 \\ b_1(\lambda, t) &= \frac{1}{12+\lambda}\left(2\,(3+\lambda)\,t^3 - 3\,(4+\lambda)\,t^2 + 8 + \lambda\right) \\ b_2(\lambda, t) &= \frac{1}{12+\lambda}\left(-2\,(3+\lambda)\,t^3 + 3\,(2+\lambda)\,t^2 + 6t + 2\right) \\ b_3(\lambda, t) &= \frac{2}{12+\lambda}t^3. \end{aligned} \tag{2.2}$$

This arc can simply be extended to a multi-arc non-uniform cubic GB-spline curve in a usual way, using four consecutive control points and applying the substitution

$$t = \frac{u - u_i}{u_{i+1} - u_i}$$

at each arc, where $u \in [u_i, u_{i+1})$. Since the shape parameter has the same effect on each arc, we will focus on the single arc (2.1) in this paper.

Now we consider the paths $P(\lambda, t_0)$ of the point $C(t_0)$ of the curve as the parameter λ has been changed. Note, that in these paths λ is the running parameter and t is the family parameter. Throughout this paper these paths are called λ-paths.

Theorem 2.2. *The limit points of the λ-paths $P(\lambda, t_0)$ at $\lambda \to \infty$ are fixed points of the control leg P_1P_2 and have symmetrical positions for the midpoint of the leg.*

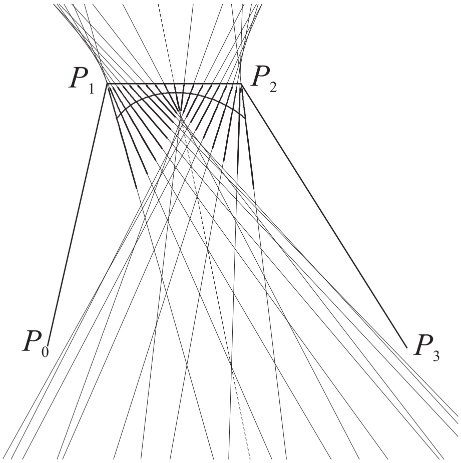


Figure 1: GB-spline curve and its λ-paths

Proof. By simple calculation

$$\begin{aligned}
\lim_{\lambda\to\infty} b_0(\lambda,t) &= \lim_{\lambda\to\infty} b_3(\lambda,t) = 0\\
\lim_{\lambda\to\infty} b_1(\lambda,t) &= 2t^3 - 3t^2 + 1\\
\lim_{\lambda\to\infty} b_2(\lambda,t) &= -2t^3 + 3t^2.
\end{aligned}$$

Denoting the latter limits by $b_1(\infty,t)$ and $b_2(\infty,t)$, and observing, that $b_2(\infty,t) = 1 - b_1(\infty,t)$ it is obvious, that the limit points of the paths are

$$\lim_{\lambda\to\infty} P(\lambda,t) = L(t) = b_1(\infty,t)P_1 + (1 - b_1(\infty,t))P_2 \tag{2.3}$$

while at $t = 0.5$ we obtain $0.5P_1 + 0.5P_2$ and this completes the proof. □

Theorem 2.3. *The λ-paths are straight line segments.*

Proof. We prove that for any fixed $t \in [0,1]$ the points of the path $P(\lambda,t)$ can be described as barycentric combination of the two endpoints $P(-8,t)$ and $P(\infty,t) = \lim_{\lambda\to\infty} P(\lambda,t)$. The blending functions at $P(-8,t)$ are

$$\begin{aligned}
b_0(-8,t) &= \frac{1}{2}(1-t)^3\\
b_1(-8,t) &= \frac{-5}{2}t^3 + 3t^2\\
b_2(-8,t) &= \frac{1}{2}(5t^3 - 9t^2 + 3t + 1)
\end{aligned}$$

$$b_3(-8,t) = \frac{1}{2}t^3.$$

We can observe that

$$\frac{b_0(\lambda,t)}{b_0(-8,t)} = \frac{b_3(\lambda,t)}{b_3(-8,t)} = \frac{4}{12+\lambda} \tag{2.4}$$

and denoting this quotiens by $q(\lambda)$, after some calculation we obtain that

$$b_1(\lambda,t) = q(\lambda)b_1(-8,t) + (1-q(\lambda))\, b_1(\infty,t)$$
$$b_2(\lambda,t) = q(\lambda)b_2(-8,t) + (1-q(\lambda))\, b_2(\infty,t),$$

thus finally for any point of the path we get

$$P(\lambda,t) = q(\lambda)P(-8,t) + (1-q(\lambda))\, P(\infty,t) \tag{2.5}$$

and this was to be proved. □

Theorem 2.4. *Considering the symmetric λ-paths $P(\lambda,t_0)$ and $P(\lambda,1-t_0)$, these lines may intersect each other. These intersection points are on the path of the point associated to the parameter value $t=1/2$, that is at the line $P(\lambda,1/2)$, if the lines P_0P_3 and P_1P_2 are parallel* (see Fig. 2).

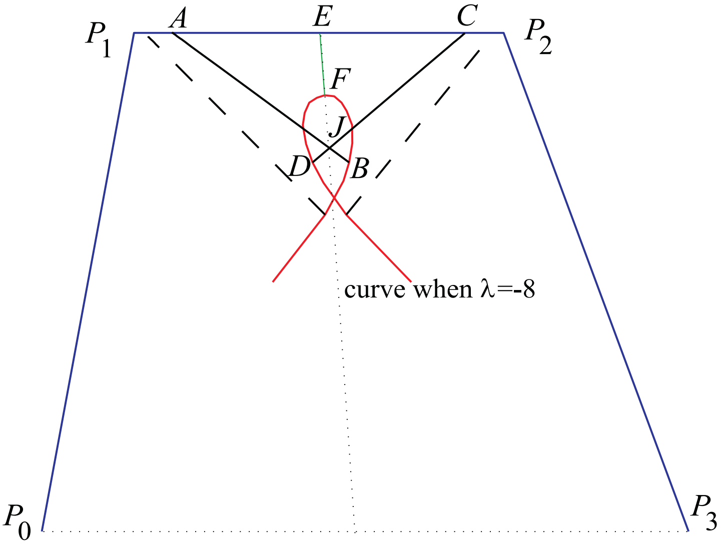


Figure 2: Symmetric paths intersect each other at a path associated to $t=1/2$

Proof. It is easy to prove that the shape of a GB-spline curve is independent of the choice of coordinates, i.e. (2.2) satisfies the following two equations:

$$C(\lambda, t, P_0{*}T{+}r, P_1{*}T{+}r, P_2{*}T{+}r, P_3{*}T{+}r) \equiv C(\lambda, t, P_0, P_1, P_2, P_3){*}T{+}r \quad (2.6)$$

where r is an arbitrary vector, and T is an arbitrary 3×3 matrix. From above we know that the GB-spline curve, the symmetric lines and the midpoint of the segments are all preserved by an affine transformation, so we can prove the result in a special case using the coordinate system given in Fig. 2.

For arbitrary parameter t, let the symmetric paths $P(\lambda, t_0)$ and $P(\lambda, 1 - t_0)$ intersect the control leg P_1P_2 and the curve $C(-8, t)$ at the point A, B, C, D respectively, and the middle path corresponding to $t = 0.5$ is on the line segment EF with E, F are midpoints of P_0P_3 and P_1P_2 respectively. Then using the definition of GB-spline curve, the coordinates of these points can be computed as follows:

$$\begin{aligned}
A &= ((3t^2 - 2t^3)a, 1)\\
B &= 1/2((5t^3 - 9t^2 + 3t + 1)a + t^3, 1 + 3t - 3t^2)\\
C &= ((1 - 3t^2 + 2t^3)a, 1)\\
D &= 1/2((6t^2 - 5t^3)a + (1 - t)^3, 1 + 3t - 3t^2)\\
E &= (a/2, 1)\\
F &= (7/16a + 1/16, 7/8)
\end{aligned}$$

Thus we obtain the coordinates of intersection point J of the line AB and CD:

$$J = \left(\begin{array}{c} \dfrac{(3t^4 - 6t^3 - 2t^2 + 3t + 1)a^2 + (-3t^4 + 6t^3 - 3t^2)a}{(9t^2 - 9t - 3)a + t^2 + 1}, \\ \dfrac{(6t^4 - 12t^3 - 4t^2 + 10t + 2)a + (-t^2 + t - 1)}{(9t^2 - 9t - 3)a + t^2 + 1} \end{array} \right). \quad (2.7)$$

To prove that the symmetric paths intersect each other at the path of the point associated to the parameter value $t = 0.5$, we can prove that the point J is on the line segment EF. The reciprocal of slope of EF is

$$\frac{1}{k_{EF}} = \frac{a - 1}{2} \quad (2.8)$$

Connecting the points EJ, the reciprocal of slope of EJ is $\frac{a-1}{2}$ too. So the point J is located on the line EF (or located on its extending part). That completes the proof. □

3. Passing through a given point

For practical applications, we would like to find a GB-spline curve passing through a given point among the family curves with the same control polygon. Of course, the given point should be in a constrained region filled by the family of curves with running parameter λ. For $\lambda \geqslant 0$ this region is bounded by the B-spline curve, the control leg P_1P_2 and the paths when $\lambda = 0, 1$ (See Fig. 3.a). If we let $\lambda > -8$ then the shape of the constrained region is a bit more complex. For a convex polygon, the region includes two parts in general. There is only one curve passing through a given point in one region, while there are two curves passing through a given point in another. Definitely, for every point in this region, we can find no less than one curve passing through it. By the property of the given convex control polygon $P_i, i = 0, \ldots, 3$, we can give the shape of the constrained region:

1) If two legs P_0P_1, P_2P_3 contend outside, the region $H \oplus G$ is circled by leg P_1P_2, paths when $\lambda = 0, 1$ and the curve when $\lambda = -8$ as shown in Fig. 3. b.

2) When control polygon is a parallelogram, this region $H \oplus G$ is a triangle (See Fig. 3. c).

3) Otherwise this region is circled by leg P_1P_2, paths when $\lambda = 0, 1$ and the curve when $\lambda = -8$ as shown in Fig. 3. d.

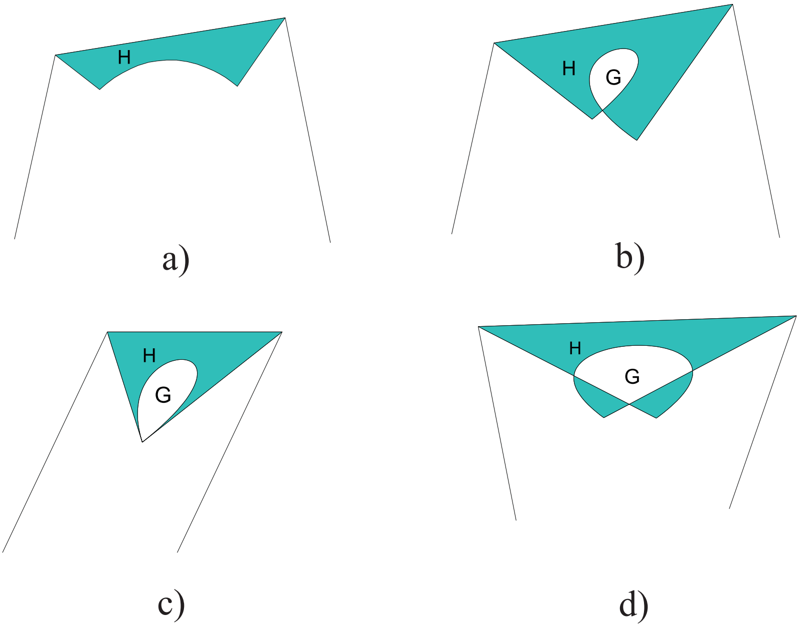


Figure 3: Different cases of constrained region for shape control. At each point in region H exactly one curve passes through, while in region G there are two solutions for each point.

Then for every point P in this region, we should find two parameter values λ_0 and t_0 for which $C(\lambda_0, t_0) = P$. As we have mentioned before, when $\lambda < 0$, the GB-spline curve is “below” the standard B-spline curve and in this case the variation diminishing property does not necessarily fulfilled. Thus in the following we restrict ourselves for the case $\lambda \geqslant 0$, however the described method works for $\lambda < 0$ as well.

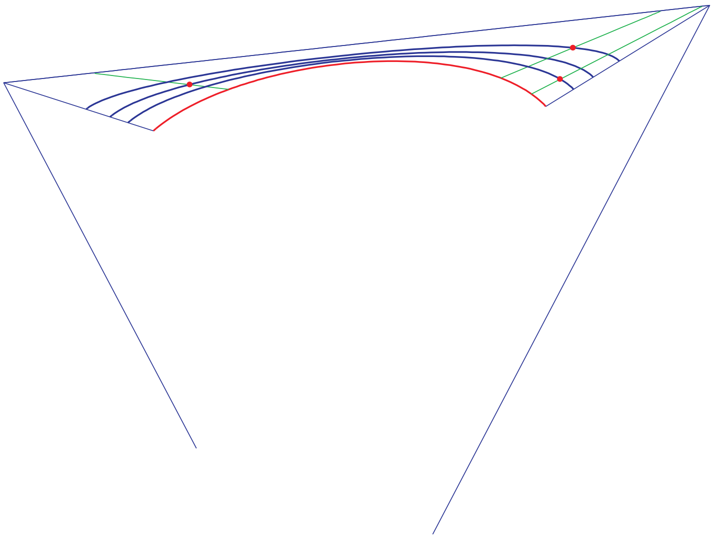


Figure 4: Given three points in the constrained region ($\lambda \geqslant 0$) the shape parameter is modified in a way that the curves pass through at the given points

We know that GB-spline paths are all lines, so we can find the value of t_0 by the following dichotomy method.

Let $first = 0, last = 1$:

a) Let $t^* = (first + last)/2$ and compute two endpoints $C(0, t^*)$ and $C(\infty, t^*)$ of path line $C(\lambda, t^*)$.

b) If P is just on the path line $C(\infty, t^*)$ within an allowed error, we get $t_0 = t^*$. The algorithm ends.

c) Otherwise we let $last = t^*$ (when P and b_0 are on the same side of path line) or $first = t^*$ (when P and b_3 are on the same side of path line). Then we return to step a).

After obtaining the value of t_0, we can get the value of λ_0 by the following calculation. From (2.5) one can get

$$P(\lambda_0, t_0) = q(\lambda_0)P(-8, t_0) + (1 - q(\lambda_0))\,P(\infty, t_0)$$

which yields

$$q(\lambda_0) = \frac{P - P(\infty, t_0)}{P(-8, t_0) - P(\infty, t_0)}$$

for each coordinates of the points $P, P(\infty, t_0)$ and $P(-8, t_0)$. Choosing for example the x coordinates of these points, one can find

$$\lambda_0 = \frac{4(P(-8,t_0) - P_x(\infty,t_0))}{P_x - P_x(\infty,t_0)} - 12.$$

By the above algorithm the curve $C(\lambda_0,t)$ passes through the given point P at the parameter value t_0 (Fig. 4).

4. Conclusion and further research

GB-spline curves has been studied in the paper with special emphasis on the numerical and geometrical effects of the alteration of its shape parameter λ. The curve has also been described in a linear blending way, where a cubic blending function was used to combine the classical B-spline curve and its control polygon leg. This approach may worth for further examination to study other curves with shape parameters as linear blending curves to give an overall view and comparison of these curve types.

References

[1] Barsky, B.A. and Beatty, J.C., Local control of bias and tension in β-splines, *ACM Transactions on Graphics*, 2 (1983) 109–134.

[2] Barsky, B.A., Computer graphics and geometric modeling using $\beta-$splines, *Springer-Verlag*, Berlin, 1988.

[3] Guo, Q., Cubic GB-spline curves, *Journal of Information and Computational Science*, 3 (2005) 465–471.

[4] Habib, Z., Sakai, M. and Sarfraz, M., Interactive Shape Control with Rational Cubic Splines, *International Journal of Computer-Aided Design & Applications*, 1 (2004) 709–718.

[5] Habib, Z., Sarfraz, M. and Sakai, M., Rational cubic spline interpolation with shape control, *Computers & Graphics*, 29 (2005) 594–605.

[6] Han, X., Piecewise quartic polynomial curves with a local shape parameter, *Journal of Computational and Applied Mathematics*, 195 (2006) 34–45.

[7] Hoffmann, M., Li, Y. and Wang, G., Paths of C-Bézier and CB-spline curves, *Computer Aided Geometric Design*, 23 (2006) 463–475.

[8] Loe, K.F., αB-spline: a linear singular blending spline, *The Visual Computer*, 12 (1996) 18–25.

[9] Piegl, L. and Tiller, W., The NURBS book, *Springer Verlag*, Berlin, 1995.

[10] Tai, C.L. and Wang, G.J., Interpolation with slackness and continuity control and convexity preservation using using singular blending, *Journal of Computational and Applied Mathematics*, 172 (2004) 337–361.

Yajuan Li
School of Science, Hangzhou Dianzi University, Hangzhou 310027, China

Miklós Hoffmann
Department of Mathematics, Károly Eszterházy College, H-3300 Eger, Hungary

Guzhao Wang
Institute of Computer Graphics and Image Processing, Department of Mathematics, Zhejiang University, Hangzhou 310027, China

Annales Mathematicae et Informaticae
34 (2007) pp. 61–70
http://www.ektf.hu/tanszek/matematika/ami

Cryptographycal protocols in the Egerfood Information System[*]

Kálmán Liptai, Gábor Kusper, Tibor Radványi

EKF, Institute of Mathematics and Informatics
e-mail: liptaik@ektf.hu, gkusper@aries.ektf.hu, dream@aries.ektf.hu

Submitted 28 September 2007; Accepted 16 November 2007

Abstract

In this article we present the cryptography of the food safety tracking system of the Regional Knowledge Center (EGERFOOD), which can be found in Eger, Hungary at the Eszterházy Károly College. We analyzed its requirements for the underlying information system. To build a user friendly system, which serves quickly and cost effectively the costumers, the providers, and the effected authorities by information, is a complex task. Furthermore, the system has to fulfill the strict requirements which one put up for data-safety and -encryption in case of a tracking system. We considered also these ones by setting up the EGERFOOD information model.

Keywords: food safety, tracking, information systems, cryptography, AES-128, RSA, .NET, framework

MSC: 94A60, 68P30, 68N15, 68P25

1. Introduction

In the focus of the research-service activities nowadays stays the environment protection and the food analytical research, from which the most attractive (from viewpoint of R+D, economy, and society) works deal with the food analytical and food safety.

We have understood this at the Eszterházy Károly College and we have decided to setup a food safety and analytical monitoring center.

[*]Research supported by the Hungarian National Foundation for Scientific Research Grant. No. T 048945 MAT.

Before that in Hungary there were only segregated attempts to boost the safety some well-known products. However, these detached examinations could not achieve a new quality. There was no new quality- or safety-parameter introduction. However, there were some results but these ones were not yet integrated in a coherent and comprehensive food tracking system. In Hungary there is so far only one food tracking system, which is for red pepper. There was not nearly any attempt to adapt this system for other products.

Our goal regarding informatics: Building a system, which sits the costumer in the center, and which is able to process and send food safety information (firstly) to the costumers and (secondly) to the food producers and to the effected authorities in a fast, cost effective, and reliable way.

The information technology is a really important tool in every aspects of the project. From the communication that exists between the collaborating partners, through the food tracking system, to the food safety communication with the customers. There will be tasks for both the device developers (for example for solving the signal transferring problems) and the software developers (for example the internet based framework of the food tracking system).

Tasks of information technology are: Create and support continuously the web system, which operates the inner communication of the project. Its goal is to ensure the information-flow between those who work in the project.

Determine the structure of the food tracking database and create the hardware and software sides of the data transmission system. The backbone of the informatics system is the database of the food tracking system. We analyzed the collected data and requirements, and by that, we created the data model of the information system. [8]

We keep the connection with the customers through WAP and Internet. Install the data-collector hardware devices at the involved food provider companies. We connect the new gauging devices - which are in experimental stage - into the communication network of the project.

2. The construction of the information system

Now the system follows the lifecycle of 1-1 product of 6 companies and connects the results of the laboratory of the knowledgecenter into the system. These are the data sources. The main aims can be seen in Figure 1.

The side of outgoing data is layered. The public competence level can be reached through the internet or WAP. It is used to give information about the production and the origin of the product using an identification code. The protected competence level gives information to the participants of the project, whose ring is much narrower than the data of the public competence level. These data are useable in research and in the development of the production of the product. The inner competence level shows the companies' exclusive, inner used data. These data can be used by an ERP system.

Now let us see the construction of the system. So called bufferservers are

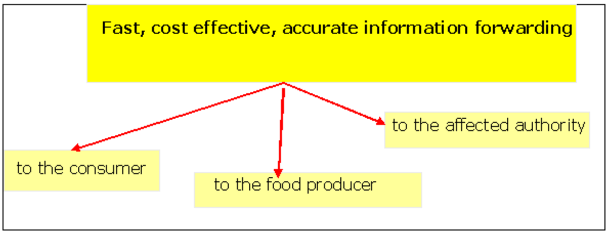

Fast, cost effective, accurate information forwarding
to the affected authority
to the consumer
to the food producer

Figure 1: Information forwarding

installed in every outer company and in research laboratory. Their tasks are the followings:

- store the members' data that belongs to the Egerfood project (e.g. corpus, meaning results, etc.)
- decode the incoming data
- process and store the incoming data
- encrypt the data and send it to the central data storehouse (through VPN connection)
- store backup copies.

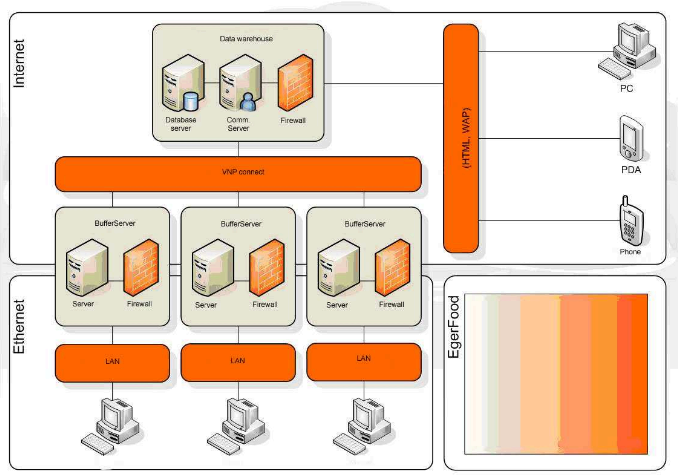


Figure 2: The informatical system

When we developed the information system of the project, the insurance of the suitable data security got a stressed function. For this reason, a three-storied encryption system came to development. In this way, starting from the creation of the data, every data is encoded by the algorithm AES-128. [1] (We shall detail the selection later.) When we send data we use the most modern method used in software technology, called Windows Communication Foundation, which makes encrypted communication. [4] The network data communication happens through a VPN network, so we can exploit the encryption provided by the VPN routers.

The base of the software system is the database developed by the researchers of this project, which make it possible that we can easily integrate any product of any company into the system.

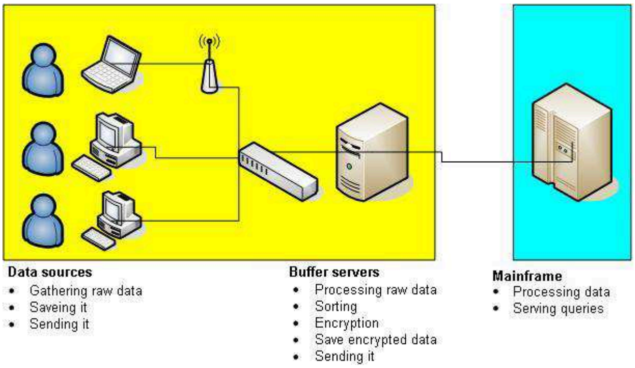


Figure 3: Puffer server

We made a program, called working process graph maker and analyser program, which output is a mass of data which generate the user surface of the clientprogram automatically. As a result of it, later enlarging can be done faster and smoothly, and the maintenance can perform with universal methods.

3. About the Encryption

Public networks such as the Internet do not provide a means of secure communication between entities. Communication over such networks is susceptible to being read or even modified by unauthorized third parties. In addition to file encryption and encryption on a local disk, cryptography helps you to create a secure means of communication over (otherwise insecure) channels, providing data integrity and authentication.

3.1. Possibility of the developer environment, the Microsoft's .NET 3.0

Cryptographic primitive	**Use**
a. Secret-key encryption (symmetric cryptography)	Performs a transformation on data, keeping the data from being read by third parties. This type of encryption uses a single shared, secret key to encrypt and decrypt data.
b. Public-key encryption (asymmetric cryptography)	Performs a transformation on data, keeping the data from being read by third parties. This type of encryption uses a public/private key pair to encrypt and decrypt data.
c. Cryptographic signing	Helps verify that data originates from a specific party by creating a digital signature that is unique to that party. This process also uses hash functions.
d. Cryptographic hashes	Maps data from any length to a fixed-length byte sequence. Hashes are statistically unique; a different two-byte sequence will not hash to the same value.

a. Symmetric cryptography

DESCryptoServiceProvider This algorithm supports a key length of 64 bits.

RC2CryptoServiceProvider The RC2CryptoServiceProvider implementation supports key lengths from 40 bits to 128 bits in increments of 8 bits.

RijndaelManaged This algorithm supports key lengths of 128, 192, or 256 bits.

TripleDESCryptoServiceProvider This algorithm supports key lengths from 128 bits to 192 bits in increments of 64 bits.

b. Asymmetric cryptography

DSACryptoServiceProvider You can use the DSACryptoServiceProvider class to create digital signatures and protect the integrity of your data. To use a public-key system to digitally sign a message, the sender first applies a hash function to the message to create a message digest. This algorithm supports key lengths from 512 bits to 1024 bits in increments of 64 bits.

RSACryptoServiceProvider This is the default implementation of RSA. The RSACryptoServiceProvider supports key lengths from 384 bits to 16384 bits in increments of 8 bits if you have the Microsoft Enhanced Cryptographic Provider installed. It supports key lengths from 384 bits to 512 bits in increments of 8 bits if you have the Microsoft Base Cryptographic Provider installed.

4. Why did we choose the AES?

We paid our attention the Advanced Encryption Standard (AES) announced in 2001 published by Joan Daemen and Vincent Rijmen [1] and the other was RSA published in 1976 by Ron Rivest, Adi Shamir and Leonard Adleman at MIT.

The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt in blocks of 128 bits. Usually an implementation of AES algorithm supports least one of the three key lengths. The algorithm specified in this standard has been implemented in different languages. In bibliographies there are lots of suggestions on how to efficiently implement the AES algorithms on a variety of platforms. We have a 32 bit system so we chose the AES-128 version to try. In this paper we don't want to detail the whole process, but we mention the main steps. When we use the AES standard we follow the following main steps.

1. A non-linear substitution step where each byte is replaced with another according to a given table (SubBytes).

2. A transposition step where each row of the state is shifted cyclically a certain number of steps (ShiftRows).

3. A mixing operation which operates on the columns of the state, combining the four bytes in each column (MixColumns).

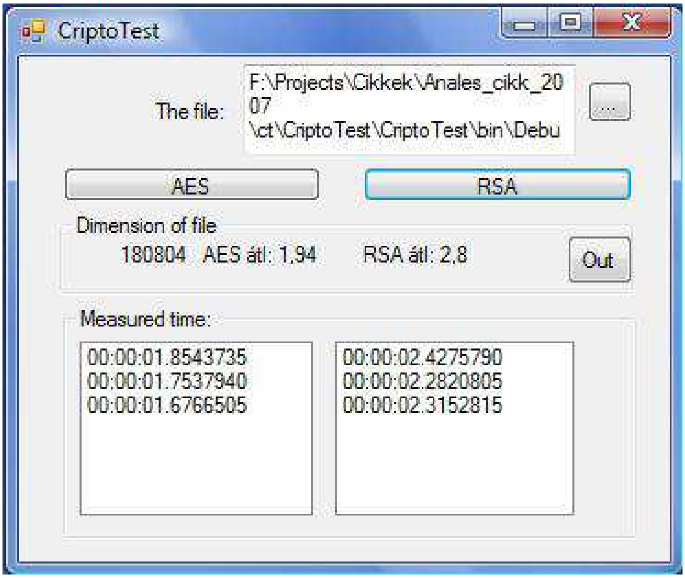
4. Each byte of the state is combined with the round key, each round key is derived from the cipher key using a key schedule (AddRoundKey).

These points are completed with an Initial Round and a Final Round, where we use the previous steps with slightly modification. In our case we repeat the rounds ten times (one of them is the Final Round).

The RSA cryptosystem is based on two mathematical problems, the problem of factoring large numbers and discrete logarithm problem. It is known that RSA is much slower than DES and other symmetric cryptosystem, but we investigated this fact in our case.

We analysed our choice with a program. [5] We wanted to know how long does it take to encrypt files with different size in one hand with the algorithm AES, on the other hand with algorithm RSA. Both of the algorithms are implemented in the system of framework 2.0 and 3.0. the surface of the test program is easy to use.

On this picture can be seen that after a file is selected the program execute three times both the AES and RSA encryptions, and measures the passed time. [7] Than calculates the arithmetic mean of it. The measured results can be saved into a file with one only click. A size of the file and the averaged times belongs to it.[2][3] This program was used in computer with following configuration:



The file: F:\Projects\Cikkek\Anales_cikk_2007\ct\CriptoTest\CriptoTest\bin\Debu

Dimension of file
180804 AES átl: 1,94 RSA átl: 2,8

Measured time:

```
00:00:01.8543735     00:00:02.4275790
00:00:01.7537940     00:00:02.2820805
00:00:01.6766505     00:00:02.3152815
```

Figure 4: The test program

Intel i915G; Pentium4 530 (3GHz, 1Mb L2 cache, 800MHz FSB) processzor; 512Mb (2x256Mb) 400MHz dual channel DDR RAM; 160Gb SATA HDD, MS Windows XP Home operation system.

We got this table as a result of measure. The items are represented in a diagram. [8] It can be seen very well that the curve belongs to the RSA stays above the curve belongs to the AES during the time of measuring. It can be clearly seen that the algorithm RSA needs more time to encrypt the same sized file.

The results got approached with a power function. Let f be a function which shows how many time need to encrypt a file the function of file size in the case of algorithm RSA. Let g be a function which shows how many time need to encrypt the function of file size in the case of algorithm AES. We get

$$f(x) = 1,340686 \cdot 10^{-10} \cdot x^{2,003325}$$
$$g(x) = 1,518159 \cdot 10^{-10} \cdot x^{1,975274}$$

We got the result that we expected beforehand so that the symmetrical key algorithm AES is more efficient in our case and with the growth of the size of the encrypted file is more conspicuous. We found substantial differences so we gave up applying RSA in our system because the quickness is very important point of view of the companies. We remark that we had chance to chose the key in AES-128 but we left this for the implemented program. Our data can be seen in following table and figures:

Size (byte)	AES (sec)	RSA (sec)
116362	2,01	2,307
136356	2,125	2,244
156352	2,229	3,322
176346	3,208	4,302
196342	4	5,265
216336	5,223	6,52
236332	6,255	7,229
256326	7,104	9,14
276320	8,317	10,244
296316	9,234	12
316328	11,328	14,307
326444	12,26	15,276
326444	12,62	15,156
345474	13,71	17,584
365470	15,32	18,834
405460	18,312	23,297
445450	22,148	28,1

Table 1: Measured data

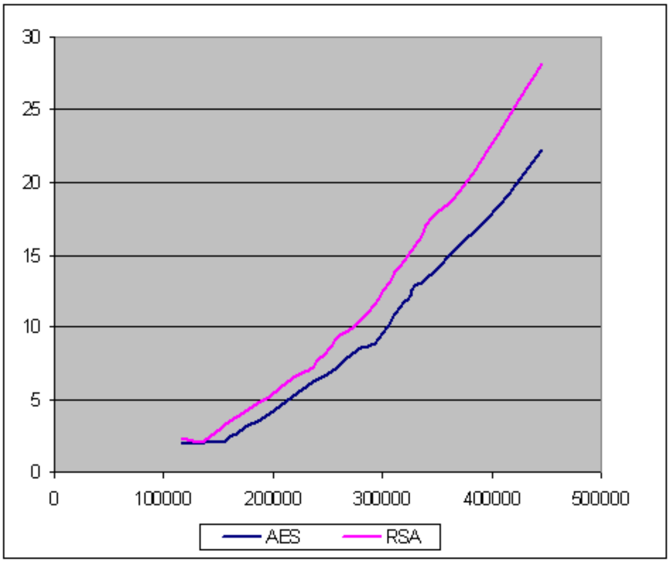


Figure 5: Measured data on the graph

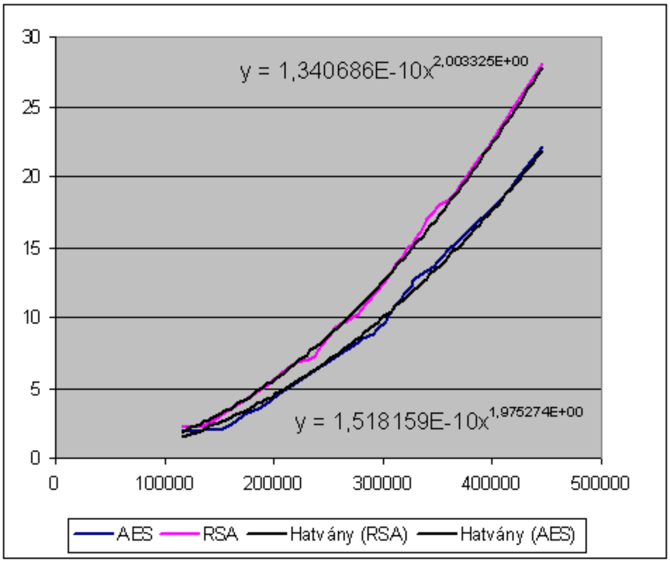


Figure 6: The interpolated curves

References

[1] Announcing the Advanced encryption standard (AES), *Federal Information Processing Standards Publication* 197, 2001.

[2] Schneier, B., Applied Cryptography, *John Wiley & Sons*, 1996.

[3] Menezes, A.J., van Oorschot, P.C., Vanstone, S.A., Handbook of Applied Cryptography, *CRC Press* 1996.

[4] Microsoft: Improving .NET Application Performance and Scalability, (2004), 639–682.

[5] Tsai, M., Kulkarni, C., Sauer, C., Shah, N., Kurt Keutzer University of California, Berkeley, Infineon Technologies, CPR ST, Munich A Benchmarking Methodology for Network Processors 1st Network Processor Workshop, 8th Int. Symp. on High Performance Computer Architectures (HPCA), Feb. 3rd 2002 Boston, MA.

[6] Radványi, T., Kusper, G., Requirement Analyses and a Database Model for the Project EGERFOOD Food Safety Knowledge Center, *ICAI2007*, Eger Hungary.

[7] Baraani-Dastjerdi, A., Pieprzyk, J., Safavi-Naini, R., Getta, J.R., Using Cryptographic Hash Functions for Discretionary Access Control in Object-Oriented Databases, *Journal of Universal Computer Science*, vol. 3, no. 6 (1997), 730–753.

[8] Radványi, T., Examination of the MSSQL Server from the user'point of view considering data insertion, *Acta Academiae Paedagogicae Agriensis, Sec. Mathematicae* (2004), 69–77.

Kálmán Liptai
Gábor Kusper
Tibor Radványi
Eszterházy Károly College
Institute of Mathematics and Informatics
P.O. Box 43
H-3300 Eger
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 71–75
http://www.ektf.hu/tanszek/matematika/ami

On the generalization of the Fibonacci-coefficient polynomials*

Ferenc Mátyás

Institute of Mathematics and Informatics, Eszterházy Károly College
e-mail: matyas@ektf.hu

Submitted 8 September 2007; Accepted 27 November 2007

Abstract

In this note we deal with the zeros of polynomials defined recursively, where the coefficients of these polynomials are the terms of a given second order linear recursive sequence of integers. Some results on the Fibonacci-coefficient polynomials obtained by D. Garth, D. Mills and P. Mitchell will be generalized.

Keywords: Fibonacci numbers, polynomials defined recursively, bounds for zeros

MSC: 11C08, 13B25

1. Introduction

Let $R_0 = 0$, $R_1 = 1$, A and B be fixed positive integers and let R_n denote the nth term of the second order linear recursive sequence

$$R = \{R_n\}_{n=0}^{\infty},$$

where for $n \geqslant 2$

$$R_n = AR_{n-1} + BR_{n-2}. \tag{1.1}$$

According to the known Binet-form, for $n \geqslant 0$

$$R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta},$$

where α and β are the zeros of the characteristic polynomial $x^2 - Ax - B$ of the sequence R. We can suppose that $\alpha > 0$ and $\beta < 0$.

*Research has been supported by the Hungarian OTKA Foundation No. T048945.

In the special case $A = B = 1$ we can get the Fibonacci-sequence, that is, with the usual notation

$$F_0 = 0,\ F_1 = 1,\ F_n = F_{n-1} + F_{n-2} \quad (n \geqslant 2).$$

We can similarly define the most known second order linear recursive sequences of polynomials, such as the Chebishev-polynomials

$$\{U_n(x)\}_{n=0}^{\infty}$$

of the second kind and the Fibonacci-polynomials

$$\{F_n(x)\}_{n=0}^{\infty},$$

where

$$U_0(x) = 0,\ U_1(x) = 1,\ U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x) \quad (n \geqslant 2)$$

and

$$F_0(x) = 0,\ F_1(x) = 1,\ F_n(x) = xF_{n-1}(x) + F_{n-2}(x) \quad (n \geqslant 2). \tag{1.2}$$

It is well-known that for $n \geqslant 2$, $U_n(z) = 0$ if and only if $z = \cos\frac{k\pi}{n}$ for $k = 1, 2, \dots, n-1$ and so $z \in \mathbf{R}$ and $|z| < 1$, while for $n \geqslant 2$ $\;F_n(z') = 0$ if and only if $z' = 2i\cos\frac{k\pi}{n}$ for $k = 1, 2, \dots, n-1$ and so z's are purely imaginary complex numbers except 0 if n is even, and $|z'| < 2$.

According to D. Garth, D. Mills and P. Mitchell [1] the definition of the Fibonacci-coefficient polynomial $p_n(x)$ is the following:

$$p_n(x) = \sum_{k=0}^{n} F_{k+1}x^{n-k} = F_1x^n + F_2x^{n-1} + \cdots + F_nx + F_{n+1}. \tag{1.3}$$

It is worth mentioning that (1.3) is not a suitable (linear) transformation of (1.2).

The aim of this paper is to investigate the zeros of the polynomials $q_n(x)$, where

$$q_n(x) = \sum_{k=0}^{n} R_{k+1}x^{n-k} = R_1x^n + R_2x^{n-1} + \cdots + R_nx + R_{n+1}, \tag{1.4}$$

that is, our results concern to a family of the linear recursive sequences of second order instead of the only one Fibonacci-sequence.

Naturally, with the notation

$$q_n^{\star}(x) = x^n q_n(1/x) = R_1 + R_2x + R_3x^2 + \cdots + R_{n+1}x^n \tag{1.5}$$

we can find information on the zeros of the polynomials $q_n^{\star}(x)$.

2. Preliminary and known results

At first we mention that the polynomials $q_n(x)$ can easily be rewritten in a recursive manner. That is, if $q_0(x) = 1$ then for $n \geqslant 1$

$$q_n(x) = xq_{n-1}(x) + R_{n+1}.$$

Lemma 2.1. *Let for $n \geqslant 1$, $g_n(x) = (x^2 - Ax - B)q_n(x)$. Then*

$$g_n(x) = x^{n+2} - R_{n+2}x - BR_{n+1}. \tag{2.1}$$

Proof. Using (1.4) we get $q_1(x) = R_1x + R_2$ and by (1.1) $g_1(x) = (x^2 - Ax - B)q_1(x) = (x^2 - Ax - B)(R_1x + R_2) = \cdots = x^3 - R_3x - BR_2$. Continuing the proof with induction on n, we suppose that the statement is true for $n-1$ and we prove it for n. Applying (1.4) and (1.1), after some numerical calculations one can get that

$$g_n(x) = (x^2 - Ax - B)q_n(x) = (x^2 - Ax - B)(R_1x^n + R_2x^{n-1} + \cdots + R_nx + R_{n+1})$$

$$= \cdots = x^{n+2} - R_{n+2}x - BR_{n+1}.$$

□

Lemma 2.2 (Theorem of S. Kakeya [3]). *If every coefficients of the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ are positive numbers and the roots of equation $f(x) = 0$ are denoted by $z_1, z_2, \ldots, z_n$, then*

$$\gamma \leqslant |z_i| \leqslant \delta$$

holds for every $1 \leqslant i \leqslant n$, where γ is the minimal, while δ is the maximal value in the sequence

$$\frac{a_0}{a_1}, \frac{a_1}{a_2}, \ldots, \frac{a_{n-1}}{a_n}.$$

The following lemma can be found in [2].

Lemma 2.3. *Let us consider the sequence R defined by* (1.1). *The increasing order of the elements of the set*

$$\left\{ \frac{R_{i+1}}{R_i} \ : \ 1 \leqslant i \leqslant n \right\}$$

is

$$\frac{R_2}{R_1}, \frac{R_4}{R_3}, \frac{R_6}{R_5}, \ldots, \frac{R_7}{R_6}, \frac{R_5}{R_4}, \frac{R_3}{R_2}.$$

3. Results and proofs

At first we deal with the number of the real zeros of the polynomials $q_n(x)$ defined in (1.4).

Theorem 3.1. a) *If $n \geqslant 2$ and even, then the polynomial $q_n(x)$ has not any real zero, that is, every zeros are non-real complex numbers.*

b) *If $n \geqslant 3$ and odd, then the polynomial $q_n(x)$ has only one real zero and this is negative. That is, every but one zeros are non-real complex numbers.*

Proof. Because of the definition (1.1) of the sequence R the coefficients of the polynomials $q_n(x)$ are positive ones, thus positive real root of the equation $q_n(x) = 0$ does not exist. That is, it is enough to deal with only the existence of negative roots of the equation $q_n(x) = 0$.

a) Since n is even, by (2.1), the coefficients of the polynomial $g_n(-x) = (-x)^{n+2} - R_{n+2}(-x) - BR_{n+1} = x^{n+2} + R_{n+2}x - BR_{n+1}$ have only one change of sign, thus according to the Descartes' rule of signs, the polynomial $g_n(x)$ has exactly one negative real zero. But $g_n(x) = (x^2 - Ax - B)q_n(x)$ implies that $g_n(\beta) = 0$, where $\beta < 0$, and so the polynomial $q_n(x)$ can not have any negative real zero.

b) Since $n \geqslant 3$ is odd, thus the existence of at least one negative real zero is obvious. We have only to prove that exactly one negative real zero exists. The polynomial

$$g_n(-x) = (-x)^{n+2} - R_{n+2}(-x) - BR_{n+1} = -x^{n+2} + R_{n+2}x - BR_{n+1}$$

shows that among its coefficients there are two changes of signs, thus according to the Descartes' rule of signs, the polynomial $g_n(x)$ has either two negative real zeros or no one. But $g_n(x) = (x^2 - Ax - B)q_n(x)$ implies that for $\beta < 0$ $g_n(\beta) = 0$. Although, $g_n(\alpha) = 0$ also holds, but $\alpha > 0$. That is, an other negative real zero of $g_n(x)$ must exist. Because of $g_n(x) = (x^2 - Ax - B)q_n(x)$ this zero must be the zero of the polynomial $q_n(x)$.

This terminated the proof of the theorem. □

In this part of the paper we deal with the localization of the zeros of the polynomials $q_n(x)$ defined in (1.4).

Theorem 3.2. *Let $z \in \mathbf{C}$ denote an arbitrary zero of the polynomial $q_n(x)$. For $n \geqslant 1$*

$$A \leqslant |z| \leqslant A + \frac{B}{A},$$

where A and B are positive integers from (1.1).

Proof. To apply Lemma 2.2 for the polynomial $q_n(x)$ we have to determine the minimal and maximal values in the sequence

$$\frac{R_{n+1}}{R_n}, \frac{R_n}{R_{n-1}}, \dots, \frac{R_2}{R_1}.$$

According to Lemma 2.3, these are $\frac{R_2}{R_1}$ and $\frac{R_3}{R_2}$, respectively. But by (1.1), $\frac{R_2}{R_1} = A$ and $\frac{R_3}{R_2} = \frac{A^2+B}{A} = A + \frac{B}{A}$, which match the statement of the theorem. □

Remarks. 1) If $n \geqslant 3$ and is odd then for the only one negative real zero z_n of the polynomial $q_n(x)$

$$-A - \frac{B}{A} \leqslant z_n \leqslant -A. \tag{3.1}$$

2) If we know the exact value of A and B then the estimation in (3.1) can be improved. E.g. in the case of the Fibonacci-sequence ($A = B = 1$) (see in [1])

$$-2 < -\frac{1+\sqrt{5}}{2} < z_n \leqslant -1.$$

3) For arbitrary zero $z^\star$ of the polynomial $q_n^\star(x)$ (1.5)

$$\frac{1}{A + \frac{B}{A}} \leqslant |z^\star| \leqslant \frac{1}{A}$$

holds.

References

[1] Garth, D., Mills, D. and Mitchell, P., Polynomials Generated by the Fibonacci Sequence, *Journal of Integer Sequences*, Vol. 10 (2007), Article 07.6.8.

[2] Mátyás, F., On the quotions of the elements of linear recursive sequences of second order, *Matematikai Lapok*, 27 (1976-1979), 379–389 (Hungarian).

[3] Zemyan, S.M., On the zeros of the n^{th} partial sum of the exponential series, *The American Mathematical Monthly*, 112 (2005), No. 10, 891–919.

Ferenc Mátyás
Institute of Mathematics and Informatics
Károly Eszterházy College
P.O. Box 43
H-3301 Eger
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 77–87
http://www.ektf.hu/tanszek/matematika/ami

On the resolution of simultaneous Pell equations[*]

László Szalay

Institute of Mathematics and Statistics, University of West Hungary
e-mail: laszalay@ktk.nyme.hu

Submitted 16 May 2007; Accepted 29 October 2007

Abstract

We descibe an alternative procedure for solving automatically simultaneous Pell equations with relatively small coefficients. The word “automatically” means to indicate that the algorithm can be implemented in Magma. Numerous famous examples are verified and a new theorem is proved by running simply the corresponding Magma procedure requires only the six coefficients of the system

$$\begin{aligned} a_1x^2 + b_1y^2 &= c_1, \\ a_2x^2 + b_2z^2 &= c_2. \end{aligned}$$

Keywords: Simultaneous Pell equations, to compute all solutions, Thue equations

MSC: 11D09, 11D25, 11Y50

1. Introduction

In this paper an alternative method is presented for solving the simultaneous Pell equations

$$a_1x^2 + b_1y^2 = c_1, \tag{1.1}$$
$$a_2x^2 + b_2z^2 = c_2, \tag{1.2}$$

in non-negative integers x, y and z, where the coefficients are given integers satisfying the natural conditions

$$a_1b_1 < 0, \quad a_2b_2 < 0, \quad c_1c_2 \neq 0, \quad a_1c_2 - a_2c_1 \neq 0.$$

[*]Research supported by János Bolyai Scholarship of HAS and Hungarian National Foundation for Scientific Research Grant No. T 048945 MAT and K 61800 FT2.

The algorithm depends on the combination of (1.1) and (1.2), which leads to Thue equations of degree four can be solved, for example, by the computer package MAGMA. Further, if (1.2) is replaced by

$$a_2x^2 + b_2z^2 = c_2y^2, \tag{1.3}$$

then the method still works. Unfortunately, the number and the coefficients of the Thue equations need to be solved may increase if a_i, b_i, c_i $(i = 1, 2)$ are getting larger. Nevertheless, applying the new idea, the classical examples have been handled before by different methods were verified in a short time (see Appendix). One of the examples gives a new result by showing that there is no Lucas balancing number.

The first paper concerning simultaneous Pell equations is due to Boutin and Teilhet [8]. In 1904, they proved the unsolvability (in positive integers α, β, γ) of the system $6\beta^2 + 1 = \alpha^2$, $\gamma^2 - 3\beta^2 = 1$. In Appendix there are given some more papers from the early period. Ljunggren [20] has a remarkable result from the first part of the twentieth century. Using the properties of the units of quadratic fields, he showed that the equations $x^2 - Dy^2 = 1$ and $y^2 - D_1z^2 = 1$ with fixed D and D_1 have only finitely many solutions, and he was able to solve the case $D = 2$, $D_1 = 3$. Generally, the finiteness of the number of solutions of (1.1), (1.2) (or (1.1), (1.3) or (1.4), (1.5)) follows from the works of Thue [27] or Siegel [26].

In 1969, Baker and Davenport discovered that the theory of linear forms in logarithm can be also applied to solve simultaneous Pell equations. Their famous paper [3] provided the number 120 as a unique extension of the Diophantine triple $\{1, 3, 8\}$ to quadruple. A set of positive integers is called Diophantine m-tuple if the product of any two elements increased by one is a perfect square. Following them, many authors applied the Baker-Davenport method to investigate similar problems (see Appendix). Taking t_{12}, t_{13}, $t_{23} \in \mathbb{Z}$ the set $S = \{a_1, a_2, a_3\}$ is called Diophantine triple with t_{12}, t_{13}, t_{23} if each $a_ia_j + t_{ij}$ equals a perfect square. Can S be extended to Diophantine quadruple by some integer $x = a_4$ with the new integers t_{14}, t_{24}, t_{34}? This question leads to the equations

$$\begin{aligned} a_1x + t_{14} &= x_1^2, \\ a_2x + t_{24} &= x_2^2, \\ a_3x + t_{34} &= x_3^2, \end{aligned}$$

or, equivalently, to an (1.1), (1.2)-type system of the form

$$\begin{aligned} a_2x_1^2 - a_1x_2^2 &= a_2t_{14} - a_1t_{24}, \\ a_3x_1^2 - a_1x_3^2 &= a_3t_{14} - a_1t_{34}. \end{aligned}$$

Clearly, starting from an Diophantine quadruple with fixed six integers t_{ij} $(1 \leqslant i < j \leqslant 4)$, one can make efforts to solve the problem of Diophantine quintuple with the new integers t_{i5} $(i = 1, \ldots, 4)$.

Pinch [23] generalized the procedure of Baker and Davenport, and his approach was applied by Gaál, Pethő and Pohst [13]. They reduced the resolution of index form equations to the resolution of certain simultaneous Pell equations.

Although Kedlaya [18] described an elementary method to solve the generalization

$$\begin{aligned} x^2 - ay^2 &= b, && (1.4)\\ P(x,y) &= z^2 && (1.5)\end{aligned}$$

of (1.1), (1.3), where $P(x,y)$ is a polynomial with integer coefficients, it is fact, that in his examples P is univariate with degree at most two.

Tzanakis [28] suggests the elliptic logarithm method. The procedure provides a corresponding elliptic curve and then determines all rational points on it. But his algorithm requires an initial non-trivial rational solution, and it may cause difficulties. This idea has been partially described by Katayama [16] as well.

An other direction is to study the number of solutions of simultaneous Pell equations. In [5] Bennett proved that if a and b are distinct nonzero integers then the simultaneous equations $x^2 - az^2 = 1 = y^2 - bz^2$ possess at most three solutions in positive integers (x,y,z). Further, he also gave an upper bound for the cardinality of positive triplets (x,y,z) satisfying $x^2 - az^2 = u$, $y^2 - bz^2 = v$.

In the end of this section we quote two preliminary result required by our method. First we recall a criterion due to Legendre for the existence of a nonzero integer solution (x,y,z) to the diophantine equation

$$ax^2 + by^2 + cz^2 = 0, \tag{1.6}$$

where a, b and c are nonzero integers. (See, for example, in [7].)

Theorem 1.1. *Let a, b, c be three squarefree integers, $a > 0$, $b < 0$, $c < 0$ which are pairwise coprime. Then there exists a nonzero integer solution (x,y,z) to the diophantine equation (1.6) if and only if all three congruences*

$$t^2 \equiv -ab \pmod{c} \qquad t^2 \equiv -ac \pmod{b} \qquad t^2 \equiv -bc \pmod{a}$$

are solvable. Furthermore, if a nonzero solution exists, then there exists a nonzero solution (x_0,y_0,z_0) of equation (1.6) satisfying the inequality

$$\max\{x_0,y_0,z_0\} \leqslant \sqrt{abc}.$$

By applying the next statement (see [21]), if (1.6) has a non-zero solution, one can determine all (x,y,z) satisfying (1.6).

Theorem 1.2. *Assume that (x_0,y_0,z_0) is an integer solution of equation (1.6) with $z_0 \neq 0$. Then, all integer solutions (x,y,z) with $z \neq 0$ of equation (1.6) are of the form*

$$\begin{aligned} x &= \pm\frac{D}{d}\left(-ax_0s^2 - 2by_0rs + bx_0r^2\right),\\ y &= \pm\frac{D}{d}\left(ay_0s^2 - 2ax_0rs - by_0r^2\right),\end{aligned}$$

$$z = \pm\frac{D}{d}\left(az_0s^2 + bz_0r^2\right),$$

where r and $s > 0$ are coprime integers, D is a nonzero integer, and $d \mid 2a^2bcz_0^3$ is a positive integer.

2. The algorithm

Consider the aforesaid system of two diophantine equations

$$a_1x^2 + b_1y^2 = c_1, \tag{2.1}$$
$$a_2x^2 + b_2z^2 = c_2, \tag{2.2}$$

in non-negative integers x, y and z, where the coefficients are given integers satisfying the conditions $a_1b_1 < 0$, $a_2b_2 < 0$, $c_1c_2 \neq 0$ and $a_1c_2 - a_2c_1 \neq 0$.

After multiplying (2.1) by c_2 and (2.2) by c_1 and subtracting the second equation from the first, we obtain

$$(a_1c_2 - a_2c_1)x^2 + b_1c_2y^2 - b_2c_1z^2 = 0. \tag{2.3}$$

Note that none of the coefficients in (2.3) is zero. We should achieve that the conditions of Legendre's theorem be fulfilled. Therefore we divide (2.3) by $\gcd(a_1c_2 - a_2c_1, b_1c_2, b_2c_1)$ and we get $a_3x^2 + b_3y^2 + c_3z^2 = 0$, further if $a_3b_3c_3 < 0$ then even multiply $a_3x^2 + b_3y^2 + c_3z^2 = 0$ by (-1). Moreover, let this new equation be multiplied by $\gcd(a_3, b_3) \cdot \gcd(a_3, c_3) \cdot \gcd(b_3, c_3)$ and let assimilate the squarefull part of the coefficients into the corresponding variables, relabelling them, and we have

$$aX^2 + bY^2 + cZ^2 = 0, \tag{2.4}$$

where X, Y, Z is a permutation of c_xx, c_yy, c_zz with some suitable positive integers c_x, c_y and c_z, moreover $a > 0$, $b < 0$ and $c < 0$ are pairwise coprime, squarefree integers. Clearly, the choice of X is unique, but the role of Y and Z can be switched. By the theorem of Legendre, we need a basic solution (X_0, Y_0, Z_0).

If (2.4) is not solvable then the system (2.1), (2.2) has no solution. Otherwise, let (X_0, Y_0, Z_0) with $Z_0 \neq 0$ satisfy (2.4), and possibly $d(2a^2bcZ_0^3) \leqslant d(2a^2bcY_0^3)$, where $d(\ )$ denotes the number of divisors function. Such a triplet can easily be found by a simply search in the intervals $0 \leqslant X_0, Y_0, Z_0 \leqslant \sqrt{abc}$.

Now, applying Theorem 1.2, X, Y and Z can be expressed by

$$\begin{aligned} X &= \pm\frac{D}{d}(\alpha_1s^2 + \beta_1sr + \gamma_1r^2), \\ Y &= \pm\frac{D}{d}(\alpha_2s^2 + \beta_2sr + \gamma_2r^2), \\ Z &= \pm\frac{D}{d}(\alpha_3s^2 + \beta_3sr + \gamma_3r^2), \end{aligned}$$

where $s > 0$ and r are coprime, D is an arbitrary integer, $d \mid h_d = 2a^2bcZ_0^3$ is a positive integer and $\beta_3 = 0$. Consequently,

$$\begin{aligned} x &= \pm\frac{D}{c_x d}(\alpha_{i_1}s^2 + \beta_{i_1}sr + \gamma_{i_1}r^2), \\ y &= \pm\frac{D}{c_y d}(\alpha_{i_2}s^2 + \beta_{i_2}sr + \gamma_{i_2}r^2), \\ z &= \pm\frac{D}{c_z d}(\alpha_{i_3}s^2 + \beta_{i_3}sr + \gamma_{i_3}r^2), \end{aligned}$$

where i_1, i_2, i_3 is a permutation of the subscripts 1, 2, 3 of α, β and γ.

These results can be applied to return with x, y and z, for instance, to (2.1), and we obtain

$$a_1\left(\frac{D}{c_x d}(\alpha_{i_1}s^2 + \beta_{i_1}sr + \gamma_{i_1}r^2)\right)^2 + b_1\left(\frac{D}{c_y d}(\alpha_{i_2}s^2 + \beta_{i_2}sr + \gamma_{i_2}r^2)\right)^2 = c_1,$$

which implies

$$a_1c_y^2\left(\alpha_{i_1}s^2 + \beta_{i_1}sr + \gamma_{i_1}r^2\right)^2 + b_1c_x^2\left(\alpha_{i_2}s^2 + \beta_{i_2}sr + \gamma_{i_2}r^2\right)^2 = c_1c_x^2c_y^2\left(\frac{d}{D}\right)^2.$$

Note that the left hand side is a homogenous form of degree 4 in s and r, denote it by $T_1(s,r)$. Simplify the latest equation by the greatest common divisor of $c_1c_x^2c_y^2$ and the coefficients of T_1. Hence we obtain $T(s,r) = c_4(d/D)^2$. On the right hand side, let c_0 be the squarefree part of c_4. Thus there exist a positive integer c_6 such that $c_4 = c_0c_6^2$. Then the above equation is equivalent to

$$T(s,r) = c_0\left(\frac{c_6 d}{D}\right)^2. \tag{2.5}$$

(2.5) means finitely many Thue equations of order 4, because $T(s,r)$ is given, $0 < d$ is a divisor of $h_d = 2a^2bcZ_0^3$ and $j = \frac{c_6 d}{D}$ must be integer. To determine all solutions of equations (2.5) we use MAGMA system. Suppose that (s_j, r_j) is a solution of $T(s,r) = c_0j^2$ for some eligible j. We reject (s_j, r_j) if $s_j \leqslant 0$ or $\gcd(s_j, r_j) > 1$, otherwise we get

$$\begin{aligned} x &= \pm\frac{c_6}{c_x j}(\alpha_{i_1}s_j^2 + \beta_{i_1}s_jr_j + \gamma_{i_1}r_j^2), \\ y &= \pm\frac{c_6}{c_y j}(\alpha_{i_2}s_j^2 + \beta_{i_2}s_jr_j + \gamma_{i_2}r_j^2), \\ z &= \pm\frac{c_6}{c_z j}(\alpha_{i_3}s_j^2 + \beta_{i_3}s_jr_j + \gamma_{i_3}r_j^2). \end{aligned}$$

If all x, y and z are non-negative integers then a solution of the system (2.1), (2.2) is found.

3. Examples

Example 3.1. A positive integer y is called balancing number with balancer $r \in \mathbb{N}^+$ if

$$1 + 2 + \cdots + (y - 1) = (y + 1) + \cdots + (y + r). \tag{3.1}$$

The problem of determining balancing numbers leads to the solutions of the Pell equation $z^2 - 8y^2 = 1$, where y can be described by the recurrence $y_n = 6y_{n-1} - y_{n-2}$, $y_0 = 1$, $y_1 = 6$ (see Behera and Panda, [4]). Note that $y = y_0 = 1$ is not a balancing number in the sense of equation (3.1).

In [19], Liptai showed that there are no Fibonacci balancing numbers, i.e. neither of balancing numbers y is a term of the Fibonacci sequence $\{F\}$ defined by the initial values $F_0 = 0$, $F_1 = 1$ and by the recurrence relation $F_n = F_{n-1} + F_{n-2}$, $(n \geqslant 2)$. Liptai used the Baker-Davenport method to have the solution of the simultaneous Pell equation $x^2 - 5y^2 = \pm 4$, $z^2 - 8y^2 = 1$.

Now we show that no Lucas balancing number exists. Lucas sequence is defined by the recurrence relation $L_n = L_{n-1} + L_{n-2}$, $(n \geqslant 2)$ and $L_0 = 2$, $L_1 = 1$. It is well known that the terms of Lucas and Fibonacci sequences satisfy $L_n^2 - 5F_n^2 = \pm 4$.

Theorem 3.2. *There is no Lucas balancing number.*

Proof. We are showing that the system

$$\begin{aligned} x^2 - 5y^2 &= \pm 4, & (3.2)\\ z^2 - 8x^2 &= 1. & (3.3) \end{aligned}$$

has only the positive integer solution $(x, y, z) = (1, 1, 3)$, consequently there exists no Lucas balancing number x.

Taking the case $+4$, with the notation $X := x$, $Y := y$ and $Z := 2z$, we have

$$33X^2 - 5Y^2 - Z^2 = 0.$$

By Theorem 1.1, it has no nonzero solution, because $t^2 \not\equiv 33 \pmod{-5}$.

The case of -4 with $X := 2z$, $Y := y$, $Z := x$ provides

$$X^2 - 5Y^2 - 31Z^2 = 0.$$

The coefficients suggest the solution $(X_0, Y_0, Z_0) = (6, 1, 1)$. Applying Theorem 1.2, it follows that

$$\begin{aligned} x &= Z = \pm\frac{D}{d}(s^2 - 5r^2),\\ y &= Y = \pm\frac{D}{d}(s^2 - 12sr + 5r^2),\\ z &= \frac{X}{2} = \pm\frac{D}{2d}(-6s^2 + 10sr - 30r^2) = \pm\frac{D}{d}(-3s^2 + 5sr - 15r^2). \end{aligned}$$

Substitute x and z to (3.3) to have

$$(-3s^2+5sr-15r^2)^2-8(s^2-5r^2)^2=\left(\frac{d}{D}\right)^2,$$

where, by Theorem 1.2 again, $0<d\mid 310$. Obviously, $\frac{d}{D}$ is integer, therefore we have to solve the Thue equations

$$s^4-30s^3r+195s^2r^2-150sr^3+25r^4=\left(\frac{d}{D}\right)^2 \tag{3.4}$$

for some positive integers $j=d/D\mid 310$. There are only three values of j when the solution (s_j,r_j) satisfies the condition $s_j>0$ and $\gcd(s_j,r_j)=1$, these are $j=1,\ 31$ and 155. All the three triplets $(j,s_j,r_j)=(1,1,0),\ (31,6,1),\ (155,5,6)$ provide the same solution $(x,y,z)=(1,1,3)$. Hence, we conclude that there are no Lucas balancing number. □

Example 3.3 (Brown [9]). The system

$$x^2-8y^2 \ = \ 1 \tag{3.5}$$

$$z^2-5y^2 \ = \ 1 \tag{3.6}$$

leads to the equation $X^2-3Y^2-Z^2=0$, where $X:=x,\ Y:=y,\ Z:=z$. The coefficients of the Legendre equation and the basic solution $(X_0,Y_0,Z_0)=(1,0,1)$ imply $d\leqslant 6$. Theorem 2 gives $x=X=\pm\frac{D}{d}(-s^2-3r^2)$, $y=Y=\pm\frac{D}{d}(-2sr)$, $z=Z=\pm\frac{D}{d}(s^2-3r^2)$, which together with the first equation of the system leads to

$$s^4-26s^2r^2+9r^4=\left(\frac{d}{D}\right)^2. \tag{3.7}$$

Since $d\mid 6$, we have to solve only four Thue equations. Only one of them have solution satisfying the conditions, namely if $j=(d/D)=1$ then $(s_j,r_j)=(1,0)$. It gives $(x,y,z)=(1,0,1)$.

Example 3.4. To determine all the non-negative solutions of the system

$$3x^2-10y^2 \ = \ -13, \tag{3.8}$$

$$x^2-3y^2 \ = \ z^2, \tag{3.9}$$

first we consider (3.9), which has already been solved in the previous example. Applying $x=X=\pm\frac{D}{d}(-s^2-3r^2)$, $y=Y=\pm\frac{D}{d}(-2sr)$, $d\mid 6$ and (3.8), we obtain

$$3s^4-22s^2r^2+27r^4=-13\left(\frac{d}{D}\right)^2. \tag{3.10}$$

These Thue equations has eight solutions in coprime $s_j>0$ and r_j providing $(x,y,z)=(7,4,1)$ and $(73,40,23)$.

In the next section we enumerate chronologically several systems of Pell equations in order to illustrate experiences and statistical data regarding the MAGMA program on my average home computer. The last coloumn shows the running time of the algorithm. Then we notify four more examples.

4. Appendix

Year	**Cit.**	**Author(s)**	**System(s)**	$\mathbf{(x,y,z)}$	$\mathbf{h_d}$	$\mathbf{d(h_d)}$	**Time**
1904	[8]	Boutin, Teilhet	$x^2-6y^2=1$ $z^2-3y^2=1$	$(1,0,1)$	6	4	1 sec
1918	[25]	Rignaux	$x^2-2z^2=1$ $y^2-3z^2=1$	$(1,1,0)$	2	2	1 sec
1922	[2]	Arwin	$x^2-2y^2=1$ $y^2-3z^2=1$	$(3,2,1)$	6	4	2 sec
1941	[20]	Ljunggren (see Arwin)	$x^2-2y^2=1$ $y^2-3z^2=1$	$(3,2,1)$	6	4	2 sec
1949	[12]	Gloden (see Rignaux)	$2x^2+1=y^2$ $3x^2+1=z^2$	$(0,1,1)$	2	2	1 sec
1969	[3]	Baker, Davenport (details below)	$3x^2-y^2=2$ $8x^2-z^2=7$	$(1,1,1)$ $(11,19,31)$	980	18	20 sec
1975	[15]	Kanagasabapathy Ponnudurai	$y^2-3x^2=-2$ $z^2-8x^2=-7$	$(1,1,1)$ $(11,19,31)$	980	18	20 sec
1978	[14]	Grinstead	$x^2-8y^2=1$ $3z^2-2y^2=1$	$(3,1,1)$	36	9	5 sec
1980	[29]	Vellupilai	$z^2-3y^2=-2$ $z^2-6x^2=-5$	$(1,1,1)$ $(29,41,71)$	50	6	2 sec
1984	[22]	Mohanty Ramasamy	$x^2-5y^2=-20$ $z^2-2y^2=1$	$(0,2,3)$	10	4	3 sec
1985	[9]	Brown	$x^2-8y^2=1$ $z^2-5y^2=1$	$(1,0,1)$	6	4	1 sec
1987	[30]	Zheng	$y^2-2x^2=1$ $z^2-5x^2=4$	$(0,1,2)$	6	4	2 sec
1987	[30]	Zheng	$y^2-5x^2=4$ $z^2-10x^2=9$	$(0,2,3)$	80	10	3 sec
1988	[23]	Pinch (example)	$x^2-2y^2=-1$ $x^2-10z^2=-9$	$(1,1,1)$ $(41,29,13)$	10	4	1 sec
1995	[13]	Gaál, Pethő Pohst (example)	$2x^2-y^2=\pm1$ $5x^2-z^2=\pm4$	$(0,1,2)$ $(1,1,1)$ $(5,7,11)$	6, 2704 2704, 6	4, 15	Σ : 16 sec
1996	[24]	Riele (details below)	$2x^2-y^2=1$ $y^2-3z^2=1$	$(1,1,0)$ $(5,7,4)$	96	12	1 sec
1996	[10]	Chen (details below)	$5x^2-3y^2=2$ $16y^2-5z^2=11$	$(1,1,1)$	7436	18	13.5 min
1996	[1]	Anglin (example)	$x^2-11y^2=1$ $z^2-56y^2=1$	$(1,0,1)$ $(199,60,449)$	10	4	26 sec
1997	[11]	Chen	$x^2-7y^2=2$ $z^2-32y^2=-23$	$(3,1,3)$ $(717,271,1533)$	92	6	40 sec
1998	[18]	Kedlaya (example)	$x^2-2y^2=-1$ $3z^2-4y^2=-1$	$(1,1,1)$	36	9	2 sec
1995	[17]	Katayama, Levesque Nakahara (example)	$x^2-3y^2=1$ $y^2-2z^2=-1$	$(1,1,1)$	8	4	2 sec
2004	[6]	Bennett (example)	$x^2-2y^2=1$ $9z^2-3y^2=-3$	$(3,2,1)$	54	8	1 sec
2004	[19]	Liptai (details below)	$x^2-5y^2=\pm4$ $z^2-8y^2=1$	$(2,0,1)$ $(3,1,3)$ $(1,1,3)$	6, 2738	4, 6	Σ : 40 sec
2005		Szalay	$x^2-5y^2=\pm4$ $z^2-8x^2=1$	$(1,1,3)$	–, 310	8	4 sec
2005		Szalay	$3x^2-10y^2=-13$ $x^2-3y^2=z^2$	$(7,4,1)$ $(73,40,23)$	6	4	—

1. Baker and Davenport, [3].
$3x^2 - y^2 = 2$, $8x^2 - z^2 = 7 \Longrightarrow 7X^2 - 5Y^2 - 2Z^2 = 0$,
$X := y$, $Y := x$, $Z := z$, $(X_0, Y_0, Z_0) = (1, 1, 1)$,
$d \mid 980$,
$49s^4 - 224s^3r + 314s^2r^2 - 160sr^3 + 25r^4 = (d/D)^2$.

2. Riele. [24]
$2x^2 - y^2 = 1$, $y^2 - 3z^2 = 1 \Longrightarrow X^2 - Y^2 - 6Z^2 = 0$,
$X := 2y$, $Y := 2x$, $Z := z$, $(X_0, Y_0, Z_0) = (5, 1, 2)$,
$d \mid 96$,
$23s^4 + 20s^3r - 150s^2r^2 + 20sr^3 + 23r^4 = -(2d/D)^2$.

3. Chen, [10].
$5x^2 - 3y^2 = 2$, $16y^2 - 5z^2 = 11 \Longrightarrow 13X^2 - 2Y^2 - 11Z^2 = 0$,
$X := y$, $Y := x$, $Z := z$, $(X_0, Y_0, Z_0) = (1, 1, 1)$,
$d \mid 7436$,
$169s^4 - 1534s^3r + 1718s^2r^2 - 236sr^3 + 4r^4 = (d/D)^2$.

4. Liptai, [19].
$x^2 - 5y^2 = \pm 4$, $z^2 - 8z^2 = 1 \Longrightarrow X^2 - 3Y^2 - Z^2 = 0$ and $37X^2 - Y^2 - Z^2$,
$X := 2z$, $Y := 3y$, $Z := x$, $(X_0, Y_0, Z_0) = (1, 0, 1)$ and
$X := y$, $Y := x$, $Z := 2z$, $(X_0, Y_0, Z_0) = (1, 6, 1)$
$d \mid 6$ and $d \mid 2738$
$9s^4 - 74s^2r^2 + 81r^4 = (6d/D)^2$ and
$42439s^4 - 28416s^3r + 7050s^2r^2 - 768sr^3 + 31r^4 = -(2d/D)^2$.

Acknowledgements. The author would like to thank Sz. Tengely for introducing him to Magma system, and A. Bérczes for implementing the algorithm toMAGMA. Moreover the author finished this paper during his very enjoyable visit to UNAM, Morelia, Mexico, and thanks the Institute of Mathematics for their kind hospitality.

References

[1] Anglin, W.S., Simultaneous Pell equations, *Math. Comp.*, 65 (1996), 355–359.

[2] Arwin, A., Common solution to simultaneous Pell equations, *Ann. Math.*, 52 (1922), 307–312.

[3] Baker, A. and Davenport, H., The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford*, 20 (1969), 129–137.

[4] Behera, A. and Panda, G., On the square roots of triangular numbers, *Fibonacci Quart.*, 37 (1999), 98–105.

[5] Bennett, M.A., On the number of solutions of simultaneous Pell equations, *J. Reine Angew. Math.*, 498 (1998), 173–199.

[6] Bennett, M.A., Products of consecutive integers, *Bull. London Math. Soc.*, 36 (2004), 683–694.

[7] Borevich, Z.I. and Shafarevich, I.R., Number Theory, *Academic Press, New York and London*, 1966.

[8] Boutin, A. and Teilhet, P.F., The form $6\beta^2 + 1$ is not a square if β is a root of $\gamma^2 - 3\beta^2 = 1$, *L' Intermédiare des mathématiciens*, XI (1904), 68, 182.

[9] Brown, E., Sets in which $xy + k$ is always a square, *Math. Comp.*, 45 (1985), 613–620.

[10] Chen, Z.Y., The Diophantine system of equations $5x^2 - 3y^2 = 2$, $16y^2 - 5z^2 = 11$, *J. Central China Normal Univ. Natur. Sci.*, 30 (1996), 381–384 (in Chinese).

[11] Chen, Z.Y., Upper bounds for positive integer solutions of the indeterminate equations $x^2 - 7y^2 = 2$, $z^2 - 32y^2 = -23$, *J. Central China Normal Univ. Natur. Sci.*, 31 (1997), 253–256 (in Chinese).

[12] Gloden, A., Impossibilités Diophantiennes, *Euclides, Madrid*, 9 (1949), 476.

[13] Gaál, I., Pethő, A. and Pohst, M., On the resolution of index form equations in biquadratic number fields III. The bicyclic biquadratic case, *J. Number Theory*, 53 (1995), 100–114.

[14] Grinstead, C.M., On a method of solving a class of Diophantine equations, *Math. Comp.*, 32 (1978), 936–940.

[15] Kanagasabapathy, P. and Ponnudurai, T., The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$, *Quart. J. Math. Oxford*, 26 (1975), 275–278.

[16] Katayama, S., Several methods for solving simultaneous Fermat-Pell equations, *J. Math. Tokushima Univ.*, 33 (1999), 1–14.

[17] Katayama, S., Levesque, C. and Nakahara, T., On the unit group and the class number of certain composita of two real quadratic field, *Manuscripa Math.*, 105 (2001), 85–101.

[18] Kedlaya, K.S., Solving unconstrained Pell equations, *Math. Comp.*, 67 (1998), 833–842.

[19] Liptai, K., Fibonacci balancing numbers, *Fibonacci Quart.*, 42 (2004), 330–340.

[20] Ljunggren, W., A note on simultaneous Pell equations, *Norsk Mat. Tidsskr.*, 23 (1941), 132–138 (in Norvegian).

[21] Luca, F. and Szalay, L., Consecutive binomial coefficients satisfying a quadratic relation, *Publ. Math. Debrecen*, 69 (2006), 185–194.

[22] Mohanty, S.P. and Ramasamy, A.M.S., The simultaneous Diophantine equations $5y^2 - 20 = x^2$ and $2y^2 + 1 = z^2$, *J. Number Theory*, 18 (1984), 356–359.

[23] Pinch, R.G.E., Simultaneous Pell equations, *Math. Proc. Camb. Phil. Soc.*, 103 (1988), 35–46.

[24] te Riele, J.J., CNTA5, *Problem Session*, 1996.

[25] Rignaux, M., L'intermédiarie des math., 25 (1918), 94–95.

[26] Siegel, C.L., Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.*, (1929), 1.

[27] Thue, A., Über Annäherungenswerte algebraischen Zahlen, *J. Reine Angew. Math.*, 135 (1909), 284–305.

[28] Tzanakis, N., Effective solution of two simultaneous Pell equations by the elliptic logarithm method, *Acta Arithm.*, 103 (2002), 119–135.

[29] Vellupilai, M., The equations $z^2-3y^2=-2$ and $z^2-6x^2=-5$, in: A Collection of Manuscripts Related to the Fibonacci sequence, V. E. Hoggatt, M. Bicknell-Johnson (eds.), *The Fibonacci Association, Santa Clara*, 1980, 71–75.

[30] Zheng, D.X., On the system of Diophantine equations $y^2-2x^2=1$, $z^2-5x^2=4$ and $y^2-5x^2=4$, $z^2-10x^2=9$, *Sichuan Daxue Xuebao*, 24 (1987), 25–29 (in Chinese).

László Szalay
Institute of Mathematics and Statistics
University of West Hungary
H-9400, Sopron, Erzsébet utca 9.
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 89–95
http://www.ektf.hu/tanszek/matematika/ami

Triangles with two integral sides*

Szabolcs Tengely

Institute of Mathematics, University of Debrecen
e-mail: tengely@math.klte.hu

Submitted 26 July 2007; Accepted 2 November 2007

Abstract

We study some Diophantine problems related to triangles with two given integral sides. We solve two problems posed by Zoltán Bertalan and we also provide some generalization.

Keywords: Diophantine equations, Elliptic curves

MSC: Primary 11D61; Secondary 11Y50

1. Introduction

There are many Diophantine problems arising from studying certain properties of triangles. Most people know the theorem on the lengths of sides of right angled triangles named after Pythagoras. That is $a^2 + b^2 = c^2$.

An integer $n \geqslant 1$ is called congruent if it is the area of a right triangle with rational sides. Using tools from modern arithmetic theory of elliptic curves and modular forms Tunnell [10] found necessary condition for n to be a congruent number. Suppose that n is a squarefree positive integer which is a congruent number.

(a) If n is odd, then the number of integer triples (x, y, z) satisfying the equation $n = 2x^2+y^2+8z^2$ is just twice the number of integer triples (x, y, z) satisfying $n = 2x^2 + y^2 + 32z^2$.

(b) If n is even, then the number of integer triples (x, y, z) satisfying the equation $\frac{n}{2} = 4x^2+y^2+8z^2$ is just twice the number of integer triples (x, y, z) satisfying $\frac{n}{2} = 4x^2 + y^2 + 32z^2$.

*Research supported in part by the Magyary Zoltán Higher Educational Public Foundation

A Heronian triangle is a triangle having the property that the lengths of its sides and its area are positive integers. There are several open problems concerning the existence of Heronian triangles with certain properties. It is not known whether there exist Heronian triangles having the property that the lengths of all their medians are positive integers [6], and it is not known whether there exist Heronian triangles having the property that the lengths of all their sides are Fibonacci numbers [7]. Gaál, Járási and Luca [5] proved that there are only finitely many Heronian triangles whose sides $a, b, c \in S$ and are reduced, that is $\gcd(a, b, c) = 1$, where S denotes the set of integers divisible only by some fixed primes.

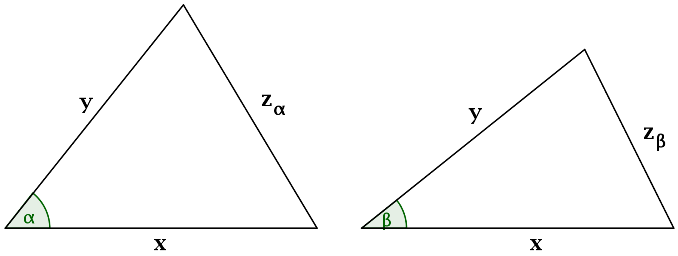
Petulante and Kaja [9] gave arguments for parametrizing all integer-sided triangles that contain a specified angle with rational cosine. It is equivalent to determining a rational parametrization of the conic $u^2 - 2\alpha uv + v^2 = 1$, where α is the rational cosine.

The present paper is motivated by the following two problems due to Zoltán Bertalan.

(i) How to choose x and y such that the distances of the clock hands at 2 o'clock and 3 o'clock are integers?

(ii) How to choose x and y such that the distances of the clock hands at 2 o'clock and 4 o'clock are integers?

We generalize and reformulate the above questions as follows. For given $0 < \alpha, \beta < \pi$ we are looking for pairs of triangles in which the length of the sides (z_α, z_β) opposite the angles α, β are from some given number field $\mathbb{Q}(\theta)$ and the length of the other two sides (x, y) are rational integers. Let $\varphi_1 = \cos(\alpha)$ and $\varphi_2 = \cos(\beta)$.



By means of the law of cosine we obtain the following systems of equations

$$x^2 - 2\varphi_1 xy + y^2 = z_\alpha^2,$$
$$x^2 - 2\varphi_2 xy + y^2 = z_\beta^2,$$

After multiplying these equations and dividing by y^4 we get

$$\mathcal{C}_{\alpha,\beta} : X^4 - 2(\varphi_1 + \varphi_2)X^3 + (4\varphi_1\varphi_2 + 2)X^2 - 2(\varphi_1 + \varphi_2)X + 1 = Y^2,$$

where $X = x/y$ and $Y = z_\alpha z_\beta / y^2$. Suppose $\varphi_1, \varphi_2 \in \mathbb{Q}(\theta)$ for some algebraic number θ. Clearly, the hyperelliptic curve $\mathcal{C}_{\alpha,\beta}$ has a rational point $(X, Y) = (0, 1)$, so it is isomorphic to an elliptic curve $\mathcal{E}_{\alpha,\beta}$. The rational points of an elliptic curve form a finitely generated group. We are looking for points on $\mathcal{E}_{\alpha,\beta}$ for which the first coordinate of its preimage is rational. If $\mathcal{E}_{\alpha,\beta}$ is defined over $\mathbb{Q}$ and the rank is 0, then there are only finitely many solutions, if the rank is greater than 0, then there are infinitely many solutions. If the elliptic curve $\mathcal{E}_{\alpha,\beta}$ is defined over some number field of degree at least two, then one can apply the so-called elliptic Chabauty method (see [2, 3] and the references given there) to determine all solutions with the required property.

2. Curves defined over $\mathbb{Q}$

2.1. $(\alpha, \beta) = (\pi/3, \pi/2)$

The system of equations in this case is

$$\begin{aligned} x^2 - xy + y^2 &= z^2_{\pi/3}, \\ x^2 + y^2 &= z^2_{\pi/2}. \end{aligned}$$

The related hyperelliptic curve is $\mathcal{C}_{\pi/3,\pi/2}$.

Theorem 2.1. *There are infinitely many rational points on* $\mathcal{C}_{\pi/3,\pi/2}$.

Proof. In this case the free rank is 1, as it is given in Cremona's table of elliptic curves [4] (curve 192A1). Therefore there are infinitely many rational points on $\mathcal{C}_{\pi/3,\pi/2}$. □

Corollary 2.2. *Problem* (i) *has infinitely many solutions.*

Few solutions are given in the following table.

x	y	$z_{\pi/3}$	$z_{\pi/2}$
8	15	13	17
1768	2415	2993	3637
10130640	8109409	9286489	12976609
498993199440	136318711969	517278459169	579309170089

2.2. $(\alpha, \beta) = (\pi/2, 2\pi/3)$

The system of equations in this case is

$$\begin{aligned} x^2 + y^2 &= z^2_{\pi/2}, \\ x^2 + xy + y^2 &= z^2_{2\pi/3}. \end{aligned}$$

The hyperelliptic curve $\mathcal{C}_{\pi/2,2\pi/3}$ is isomorphic to $\mathcal{C}_{\pi/3,\pi/2}$, therefore there are infinitely many rational points on $\mathcal{C}_{\pi/2,2\pi/3}$.

2.3. $(\alpha,\beta)=(\pi/3,2\pi/3)$

We have

$$x^2-xy+y^2=z^2_{\pi/3},$$
$$x^2+xy+y^2=z^2_{2\pi/3}.$$

After multiplying these equations we get

$$x^4+x^2y^2+y^4=(z_{\pi/3}z_{2\pi/3})^2. \tag{2.1}$$

Theorem 2.3. *If* (x,y) *is a solution of* (2.1) *such that* $\gcd(x,y)=1$, *then* $xy=0$.

Proof. See [8] at page 19. □

Corollary 2.4. *Problem* (ii) *has no solution.*

In the following sections we use the so-called elliptic Chabauty's method (see [2], [3]) to determine all points on the curves $\mathcal{C}_{\alpha,\beta}$ for which X is rational. The algorithm is implemented by N. Bruin in MAGMA [1], so here we indicate the main steps only, the actual computations can be carried out by MAGMA. The MAGMA code clock.m which were used is given below. It requires three inputs, a,b as members of some number fields and p a prime number.

3. Curves defined over $\mathbb{Q}(\sqrt{2})$

3.1. $(\alpha,\beta)=(\pi/4,\pi/2)$

The hyperelliptic curve $\mathcal{C}_{\pi/4,\pi/2}$ is isomorphic to

$$\mathcal{E}_{\pi/4,\pi/2}:\quad v^2=u^3-u^2-3u-1.$$

The rank of $\mathcal{E}_{\pi/4,\pi/2}$ over $\mathbb{Q}(\sqrt{2})$ is 1, which is less than the degree of $\mathbb{Q}(\sqrt{2})$. Applying elliptic Chabauty (the procedure "Chabauty" of MAGMA) with $p=7$, we obtain that $(X,Y)=(0,\pm 1)$ are the only affine points on $\mathcal{C}_{\pi/4,\pi/2}$ with rational first coordinates. Since $X=x/y$ we get that there does not exist appropriate triangles in this case.

3.2. $(\alpha,\beta)=(\pi/4,\pi/3)$

The hyperelliptic curve $\mathcal{C}_{\pi/4,\pi/3}$ is isomorphic to

$$\mathcal{E}_{\pi/4,\pi/3}:\quad v^2=u^3+(\sqrt{2}-1)u^2-2u-\sqrt{2}.$$

The rank of $\mathcal{E}_{\pi/4,\pi/2}$ over $\mathbb{Q}(\sqrt{2})$ is 1 and applying elliptic Chabauty's method again with $p=7$, we obtain that $(X,Y)=(0,\pm 1)$ are the only affine points on $\mathcal{C}_{\pi/4,\pi/3}$ with rational first coordinates. As in the previous case we obtain that there does not exist triangles satisfying the appropriate conditions.

Algorithm 1 MAGMA code clock.m

```
clock:=function(a,b,p)
P1:=ProjectiveSpace(Rationals(),1);
K1:=Parent(a);
K2:=Parent(b);
if IsIntegral(a) then
   K1:=RationalField();
end if;
if IsIntegral(b) then
   K2:=RationalField();
end if;
if Degree(K1)*Degree(K2) eq 1 then
   K:=RationalField();
else
   if Degree(K1) gt 1 and Degree(K2) gt 1 then
      K:=CompositeFields(K1,K2)[1];
   else
      if Degree(K1) eq 1 then
         K:=K2;
      else
         K:=K1;
      end if;
   end if;
end if;
P<X>:=PolynomialRing(K);
ka:=K!a;
kb:=K!b;
C:=HyperellipticCurve($X^4-2*(ka+kb)*X^3+(4*ka*kb+2)*X^2-2*(ka+kb)*X+1$);
pt:=C![0,1];
E,CtoE:=EllipticCurve(C,pt);
Em,EtoEm:=MinimalModel(E);
umap:=map<C->P1|[C.1,C.3]>;
U:=Expand(Inverse(CtoE*EtoEm)*umap);
RB:=RankBound(Em);
print Em,RB;
if RB ne 0 then
   success,G,mwmap:=PseudoMordellWeilGroup(Em);
   NC,VC,RC,CC:=Chabauty(mwmap,U,p);
   print success,NC,#VC,RC;
   if NC eq #VC then
      print {EvaluateByPowerSeries(U,mwmap(gp)): gp in VC};
      print forall{pr: pr in PrimeDivisors(RC)|IsPSaturated(mwmap,pr)};
   end if;
else
   success,G,mwmap:=PseudoMordellWeilGroup(Em);
   print #G,#TorsionSubgroup(Em);
   print {EvaluateByPowerSeries(U,mwmap(gp)): gp in G};
end if;
return K,C;
end function;
```

4. Curves defined over $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{5})$

In the following tables we summarize some details of the computations, that is the pair (α, β), the equations of the elliptic curves $\mathcal{E}_{\alpha,\beta}$, the rank of the Mordell-Weil group of these curves over the appropriate number field ($\mathbb{Q}(\sqrt{3})$ or $\mathbb{Q}(\sqrt{5})$), the rational first coordinates of the affine points and the primes we used.

(α, β)	$\mathcal{E}_{\alpha,\beta}$	Rank	X	p
$(\pi/6, \pi/2)$	$v^2 = u^3 - u^2 - 2u$	1	$\{0, \pm 1\}$	5
$(\pi/6, \pi/3)$	$v^2 = u^3 + (\sqrt{3} - 1)u^2 - u + (-\sqrt{3} + 1)$	1	$\{0\}$	7
$(\pi/5, \pi/2)$	$v^2 = u^3 - u^2 + 1/2(\sqrt{5} - 7)u + 1/2(\sqrt{5} - 3)$	1	$\{0\}$	13
$(\pi/5, \pi/3)$	$v^2 = u^3 + 1/2(\sqrt{5} - 1)u^2 + 1/2(\sqrt{5} - 5)u - 1$	1	$\{0, 1\}$	13
$(\pi/5, 2\pi/5)$	$v^2 = u^3 - 2u - 1$	1	$\{0\}$	7
$(\pi/5, 4\pi/5)$	$v^2 = u^3 + 1/2(-\sqrt{5} + 1)u^2 - 4u + (2\sqrt{5} - 2)$	0	$\{0\}$	-

In case of $(\alpha, \beta) = (\pi/5, \pi/3)$ we get the following family of triangles given by the length of the sides

$$(x, y, z_\alpha) = \left(t, t, \frac{-1 + \sqrt{5}}{2} t\right) \text{ and } (x, y, z_\beta) = (t, t, t),$$

where $t \in \mathbb{N}$.

References

[1] Bosma, W., Cannon, J., and Playoust, C., The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4) (1997) 235–265. Computational algebra and number theory (London, 1993).

[2] Bruin, N.R., Chabauty methods and covering techniques applied to generalized Fermat equations, volume 133 of CWI Tract, *Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam*, 2002. Dissertation, University of Leiden, Leiden, 1999.

[3] Bruin, N., Chabauty methods using elliptic curves, *J. Reine Angew. Math.*, 562 (2003) 27–49.

[4] Cremona, J.E., Algorithms for modular elliptic curves, *Cambridge University Press*, New York, NY, USA, 1992.

[5] Gaál, I., Járási, I. and Luca, F., A remark on prime divisors of lengths of sides of Heron triangles. *Experiment. Math.*, 12(3) (2003) 303–310.

[6] Guy, R.K., Unsolved problems in number theory, *Problem Books in Mathematics, Springer-Verlag*, New York, second edition, 1994. Unsolved Problems in Intuitive Mathematics, I.

[7] Harborth, H., Kemnitz, A. and Robbins, N., Non-existence of Fibonacci triangles, *Congr. Numer.*, 114 (1996) 29–31. Twenty-fifth Manitoba Conference on Combinatorial Mathematics and Computing (Winnipeg, MB, 1995).

[8] Mordell, L.J., Diophantine equations, *Pure and Applied Mathematics*, Vol. 30. Academic Press, London, 1969.

[9] Petulante, N. and Kaja, I., How to generate all integral triangles containing a given angle, *Int. J. Math. Math. Sci.*, 24(8) (2000) 569–572.

[10] Tunnell, J.B., A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.*, 72(2) (1983) 323–334.

Szabolcs Tengely
Institute of Mathematics
University of Debrecen
and the Number Theory Research Group
of the Hungarian Academy of Sciences
P.O. Box 12
4010 Debrecen
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 97–102
http://www.ektf.hu/tanszek/matematika/ami

A general method to obtain the rate of convergence in the strong law of large numbers

Tibor Tómács

Department of Applied Mathematics, Eszterházy Károly College
e-mail: tomacs@ektf.hu

Submitted 28 September 2007; Accepted 9 November 2007

Abstract

A general approach to the rate of convergence in the strong law of large numbers is given. It is based on the Hájek–Rényi type method presented in Sung, Hu and Volodin [5].

Keywords: strong law of large numbers, Hájek–Rényi maximal inequality, rate of convergence

MSC: 60F15

1. Introduction

The Hájek–Rényi inequality (see Hájek and Rényi [3]) is a useful tool to prove the strong law of large numbers (SLLN). There are several generalizations of that inequality. In Fazekas and Klesov [1] a unified approach is given to obtain SLLN's. Their method is based on a Hájek–Rényi type inequality for the moments. Then the general method is applied to prove SLLN's for various dependent sequences. It turned out that by their method the normalizing constants in the SLLN's can be improved. Hu and Hu in [4] strengthened the method of Fazekas and Klesov [1] by adding the rate of convergence in the SLLN.

Sung, Hu and Volodin [5] found a new method for obtaining the strong growth rate for sums of random variables by using the method of Fazekas and Klesov [1]. This result generalizes and sharpens the method of Hu and Hu [4].

Tómács and Líbor in [6] gave a version of the approach in Fazekas and Klesov [1] by using Hájek–Rényi type inequality for the probabilities instead of the moments.

In this paper we give a general method to obtain the rate of convergence in an SLLN by using a Hájek–Rényi type inequality for the probabilities (see Theorem 3.4). This result generalizes the method of Sung, Hu and Volodin [5].

We use the following notation. Let $\mathbb{N}$ be the set of the positive integers and $\mathbb{R}$ the set of real numbers. If $a_1, a_2, \ldots \in \mathbb{R}$ then in case $A = \emptyset$ let $\max_{k \in A} a_k = 0$ and $\sum_{k \in A} a_k = 0$. Let Ψ denote the set of functions $f\colon (0,\infty) \to (0,\infty)$, that are nonincreasing and

$$\sum_{n=1}^{\infty} n^{-2} f(n^{-1}) < \infty.$$

2. Lemmas

Lemma 2.1. *If $f \in \Psi$ then $\sum_{k=0}^{\infty} 2^{-k} f(2^{-k}) < \infty$.*

Proof. It is easy to see that

$$\sum_{n=1}^{\infty} n^{-2} f(n^{-1}) = \sum_{k=0}^{\infty} \sum_{n=2^k}^{2^{k+1}-1} n^{-2} f(n^{-1})$$

$$\geqslant \sum_{k=0}^{\infty} f(2^{-k}) \sum_{n=2^k}^{2^{k+1}-1} \left(\frac{1}{n} - \frac{1}{n+1} \right) = \frac{1}{2} \sum_{k=0}^{\infty} 2^{-k} f(2^{-k}).$$

This inequality implies the statement. □

The following lemma generalizes Dini's theorem (see Fikhtengolts [2], §375.5 or Lemma 1 in Hu and Hu [4]).

Lemma 2.2. *Let $\{a_k,\ k \in \mathbb{N}\}$ be a sequence of nonnegative numbers such that $a_k > 0$ for infinitely many k. Let $f \in \Psi$. If $\sum_{k=1}^{\infty} a_k < \infty$ then*

$$\sum_{k=1}^{\infty} a_k f\left(\sum_{i=k}^{\infty} a_i \right) < \infty.$$

Proof. Let $v_k = \sum_{i=k}^{\infty} a_i$. Then $\{v_k,\ k \in \mathbb{N}\}$ is a nonincreasing sequence of positive numbers and $\lim_{k\to\infty} v_k = 0$.

Let $A_i = \{k \in \mathbb{N} \ :\ 2^{-i-1} < v_k \leqslant 2^{-i}\}$, $i = 0, 1, 2, \ldots$, and $k_0 = \min \bigcup_{i=0}^{\infty} A_i$.

If $A_i \neq \emptyset$, then with notation $m_i = \min A_i$, we have

$$\sum_{k \in A_i} a_k \leqslant \sum_{k=m_i}^{\infty} a_k = v_{m_i} \leqslant 2^{-i}.$$

So we get

$$\sum_{k=k_0}^{\infty} a_k f(v_k) = \sum_{i=0}^{\infty} \sum_{k \in A_i} a_k f(v_k) \leqslant \sum_{i=0}^{\infty} f(2^{-i-1}) \sum_{k \in A_i} a_k$$

$$\leqslant \sum_{i=0}^{\infty} 2^{-i} f(2^{-i-1}) = 2\sum_{i=1}^{\infty} 2^{-i} f(2^{-i})$$

which is less then ∞ by Lemma 2.1. Thus the statement is proved. □

Lemma 2.3. *Let* $\{Y_k,\ k \in \mathbb{N}\}$ *be a sequence of random variables defined on a fixed probability space* $(\Omega, \mathcal{F}, \mathrm{P})$*. Then*

$$\mathrm{P}\Big(\sup_k Y_k > x\Big) = \lim_{n\to\infty} \mathrm{P}\Big(\max_{k\leqslant n} Y_k > x\Big) \ \ \textit{for all} \ \ x \in \mathbb{R}.$$

Proof. It is easy to see that

$$\Big\{\sup_k Y_k > x\Big\} = \bigcup_{n=1}^{\infty} \Big\{\max_{k\leqslant n} Y_k > x\Big\} \ \text{ for all } \ x \in \mathbb{R},$$

hence, using continuity of probability, we get the statement. □

Lemma 2.4. *Let* $\{Y_k,\ k \in \mathbb{N}\}$ *be a sequence of random variables defined on a fixed probability space* $(\Omega, \mathcal{F}, \mathrm{P})$ *and* $\{\varepsilon_n,\ n \in \mathbb{N}\}$ *a nondecreasing sequences of real numbers. If*

$$\lim_{n\to\infty} \mathrm{P}\Big(\sup_k Y_k > \varepsilon_n\Big) = 0,$$

then

$$\sup_k Y_k < \infty \ \ \textit{almost surely (a.s.)}.$$

Proof. Using continuity of probability, we have

$$\mathrm{P}\left(\bigcap_{n=1}^{\infty} \{\sup_k Y_k > \varepsilon_n\}\right) = \lim_{n\to\infty} \mathrm{P}\Big(\sup_k Y_k > \varepsilon_n\Big) = 0,$$

which is equivalent to $\mathrm{P}\Big(\bigcup_{n=1}^{\infty}\{\sup_k Y_k \leqslant \varepsilon_n\}\Big) = 1$. This implies that there exists $n_\omega \in \mathbb{N}$ for almost every $\omega \in \Omega$, such that $\sup_k Y_k(\omega) \leqslant \varepsilon_{n_\omega} < \infty$. □

3. The general method

In this section let $\{X_k,\ k \in \mathbb{N}\}$ be a sequence of random variables defined on a fixed probability space $(\Omega, \mathcal{F}, \mathrm{P})$ and $S_n = \sum_{k=1}^{n} X_k$ for all $n \in \mathbb{N}$. Let $\{\alpha_k,\ k \in \mathbb{N}\}$ be a sequence of nonnegative real numbers, $r > 0$ and $\{b_k,\ k \in \mathbb{N}\}$ a nondecreasing unbounded sequence of positive real numbers. Assume that

$$\sum_{k=1}^{\infty} \alpha_k b_k^{-r} < \infty$$

and there exists $c>0$ such that for any $n\in\mathbb{N}$ and any $\varepsilon>0$

$$\mathrm{P}\Big(\max_{k\leqslant n}|S_k|\geqslant\varepsilon\Big)\leqslant c\varepsilon^{-r}\sum_{k=1}^{n}\alpha_k. \tag{3.1}$$

Let $f\in\Psi$, $g(x)=f^{-1/r}(x)$ if $x>0$, $g(0)=0$ and

$$\beta_n=\max_{k\leqslant n}b_k g\left(\sum_{i=k}^{\infty}\alpha_i b_i^{-r}\right).$$

Remark 3.1. It is proved that these conditions imply $\lim_{n\to\infty}S_nb_n^{-1}=0$ a.s. (See Theorem 2.4 in [6].)

Theorem 3.2. *If there exists $t\in\mathbb{N}$ such that $\alpha_t\neq 0$, then*

$$\frac{S_n}{\beta_n}=\begin{cases}O(1)\ \text{a.s.}, & \text{if } \beta_n=O(1),\\ o(1)\ \text{a.s.}, & \text{if } \beta_n\neq O(1).\end{cases}$$

Proof. It is easy to see that $0<\beta_1\leqslant\beta_2\leqslant\cdots$. First we shall prove that

$$\sum_{k=1}^{\infty}\alpha_k\beta_k^{-r}<\infty. \tag{3.2}$$

If $\alpha_k>0$ for finitely many k, then (3.2) is obvious. If $\alpha_k>0$ for infinitely many k, then

$$\begin{aligned}\beta_n^{-r}&=\left(\max_{k\leqslant n}b_kf^{-1/r}\Big(\sum_{i=k}^{\infty}\alpha_ib_i^{-r}\Big)\right)^{-r}\\&\leqslant\left(b_nf^{-1/r}\Big(\sum_{i=n}^{\infty}\alpha_ib_i^{-r}\Big)\right)^{-r}=b_n^{-r}f\left(\sum_{i=n}^{\infty}\alpha_ib_i^{-r}\right).\end{aligned}$$

This inequality and Lemma 2.2 imply

$$\sum_{k=1}^{\infty}\alpha_k\beta_k^{-r}\leqslant\sum_{k=1}^{\infty}\alpha_kb_k^{-r}f\left(\sum_{i=k}^{\infty}\alpha_ib_i^{-r}\right)<\infty.$$

Thus (3.2) is proved. Now, if $\beta_n\neq O(1)$, then Remark 3.1 and (3.2) imply the statement. If $\beta_n=O(1)$, then we get by (3.2)

$$\sum_{k=1}^{\infty}\alpha_k\leqslant\sum_{k=1}^{\infty}\alpha_k\big(\beta_k^{-1}\sup_n\beta_n\big)^r=\big(\sup_n\beta_n\big)^r\sum_{k=1}^{\infty}\alpha_k\beta_k^{-r}<\infty. \tag{3.3}$$

By Lemma 2.3 and (3.1) we have

$$\mathrm{P}\Big(\sup_k|S_k|>\varepsilon\Big)\leqslant\lim_{n\to\infty}\mathrm{P}\Big(\max_{k\leqslant n}|S_k|\geqslant\varepsilon\Big)\leqslant c\varepsilon^{-r}\sum_{k=1}^{\infty}\alpha_k\quad\text{for all }\ \varepsilon>0.$$

This inequality and (3.3) imply

$$\lim_{n\to\infty} \mathrm{P}\Big(\sup_k |S_k| > \varepsilon_n\Big) = 0,$$

where $0 < \varepsilon_n \uparrow \infty$. Hence by Lemma 2.4 we get $\sup_k |S_k| < \infty$ a.s. On the other hand $S_n\beta_n^{-1} \leqslant \sup_k |S_k|\beta_1^{-1}$. Thus the theorem is proved. □

Remark 3.3. Sung, Hu and Volodin proved in [5] (Lemma 4) that if $\alpha_n \equiv 1$ then $\beta_n \neq O(1)$. Hence Theorem 3.2 implies that if $\alpha_n \equiv 1$ then $\lim_{n\to\infty} S_n\beta_n^{-1} = 0$ a.s.

Theorem 3.4. *The following statements are true:*
(1) $S_nb_n^{-1} = O(\beta_nb_n^{-1})$ *a.s.*
(2) $\lim_{n\to\infty} S_nb_n^{-1} = 0$ *a.s.*
(3) *If* $\alpha_k > 0$ *for finitely many* k*, then* $\lim_{n\to\infty} \beta_nb_n^{-1} = 0$.
(4) *If* $\lim_{x\to 0} f(x) = \infty$*, then* $\lim_{n\to\infty} \beta_nb_n^{-1} = 0$.

Proof. Let $w_k = \sum_{i=k}^{\infty} \alpha_i b_i^{-r}$. Then $w_1 \geqslant w_2 \geqslant \ldots$ and $\lim_{n\to\infty} w_n = 0$, hence we get

$$\beta_n \leqslant \max_{k<m} b_kg(w_k) + \max_{m\leqslant k\leqslant n} b_kg(w_k) \leqslant \max_{k<m} b_kg(w_k) + b_ng(w_m), \quad \text{if} \quad n > m. \tag{3.4}$$

On the other hand

$$\lim_{n\to\infty} \big(b_n^{-1} \max_{k<m} b_kg(w_k) + g(w_m)\big) = g(w_m), \quad \forall m \in \mathbb{N}. \tag{3.5}$$

Now, we shall prove that

$$\lim_{m\to\infty} g(w_m) = 0. \tag{3.6}$$

If $\alpha_k > 0$ for finitely many k, then (3.6) is obvious. If $\alpha_k > 0$ for infinitely many k, then the condition is $\lim_{x\to 0} f(x) = \infty$, which implies $\lim_{m\to\infty} f(w_m) = \infty$. Hence, (3.6) is true in this case too. Then (3.4), (3.5) and (3.6) imply $\lim_{n\to\infty} \beta_nb_n^{-1} = 0$.

Now, we turn to statement $S_nb_n^{-1} = O(\beta_nb_n^{-1})$ a.s. If there exists $t \in \mathbb{N}$ such that $\alpha_t \neq 0$, then by Theorem 3.2 we have

$$\frac{S_n}{b_n} = \frac{S_n}{\beta_n}\frac{\beta_n}{b_n} = O(1)\frac{\beta_n}{b_n} = O\left(\frac{\beta_n}{b_n}\right) \quad \text{a.s.}$$

If $\alpha_k \equiv 0$, then by (3.1) we get

$$\mathrm{P}\Big(\max_{k\leqslant n} |S_k| \geqslant \varepsilon_m\Big) = 0 \quad \forall m, n \in \mathbb{N},$$

where $0 < \varepsilon_m \downarrow 0$. It follows that $S_n = 0$ a.s. for all $n \in \mathbb{N}$ in this case.

Finally $\lim_{n\to\infty} S_nb_n^{-1} = 0$ a.s. is proved by Tómács and Líbor in [6] (Theorem 2.4). □

References

[1] Fazekas, I. and Klesov, O., A general approach to the strong laws of large numbers, *Theory of Probab. Appl.*, 45/3 (2000) 568–583.

[2] Fikhtengolts, G.M., A course of differential and integral calculus, *People's Education Press* (1954).

[3] Hájek, J. and Rényi, A., Generalization of an inequality of Kolmogorov, *Acta Math. Acad. Sci. Hungar.* 6 no. 3–4 (1955) 281–283.

[4] Hu, S. and Hu, M., A general approach rate to the strong law of large numbers, *Stat. & Prob. Letters* 76 (2006) 843–851.

[5] Sung, S.H., Hu, T.-C. and Volodin, A., A note on the growth rate in the Fazekas-Klesov general law of large numbers and some applications to the weak law of large numbers for tail series, *Submitted to Publicationes Mathematicae Debrecen* (July 8, 2006).

[6] Tómács, T. and Líbor, Zs., A Hájek–Rényi type inequality and its applications, *Annales Mathematicae et Informaticae*, 33 (2006) 141–149.

Tibor Tómács
Department of Applied Mathematics
Károly Eszterházy College
P.O. Box 43
H-3301 Eger
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 103–109
http://www.ektf.hu/tanszek/matematika/ami

Complex Fiber Visualization

Henrietta Tomán[a], Róbert Tornai[b], Marianna Zichar[c]

[a] Department of Computer Graphics
University of Debrecen
e-mail: toman@inf.unideb.hu

[b] Department of Computer Graphics
University of Debrecen
e-mail: rtornai@inf.unideb.hu

[c] Department of Computer Graphics
University of Debrecen
e-mail: zicharm@inf.unideb.hu

Submitted 6 October 2007; Accepted 18 December 2007

Abstract

In this paper we give a short overview about how the known, different methods (DTI, WMT) can be integrated as new components into a multi functional system. Our exact aim was to develop a well applicable implementation for the DTI method and Fiber Tracking. The final goal is to integrate the fibers or ellipsoids into the surface model clipped by examination planes. Furthermore, the stream of the molecules (the fibers) can be modelled by a particle system. These techniques are available by the new graphic cards and the standards they support.

Keywords: Diffusion Tensor Imaging, fiber tracking, diffusion ellipsoid, shader languages, parallelized algorithms

MSC: 68U05, 92C55

1. Introduction

The white matter of human brain has a complex structure and plays an essential role in brain function.

In spite of the fact, that a fair amount of information is available today about white matter, not all the aspects of its structure are completely known and understood. We know even less about how the white matter structure is affected by neurological diseases, tumors or traumas.

Diffusion Tensor Imaging (DTI) is an emerging Magnetic Resonance Imaging (MRI) technique based on water diffusion. Fiber tracking, also called White Matter Tractography (WMT), uses the directional information of diffusion tensor maps to estimate connection pathways in white matter.

The method is presented in the PhD dissertation of Mariana Lazar (see [2]).

Our aim is to reconstruct the fiber tracts of the human brain from measurements of fiber orientation and visualize them on the image of the brain. Generally the programs show the surface model clipped by orthogonal sections (coronal, axial and sagital). The current version of our software is capable to visualize the surface model clipped by (even more than the usual three) planes having arbitrary directions. The software component is able to promote the recognition of the brain diseases and after the diagnosis it helps to select the appropriate way of cure. When surgical intervention is needed, the point and the direction of the permeation can be determined more exactly. The software component can be parallelized by using the shading languages (see [6]).

The visualization procedure belongs to a complex software system developed by a team led by Miklós Emri. This project is part of a new partnership between the Department of Computer Graphics and the PET Center of the Medical School and Health Science Center.

2. Theoretical background

During an MRI scanning process radio waves are sent through the brain which are 10 000 to 30 000 times stronger than Earth's magnetic field. This forces the nuclei into a different position and when they move back into their place they send out radio waves of their own. The scanner picks up these signals and records their strength as numeric values into a file.

Diffusion MRI measures the diffusion of water molecules in biological tissues. In an isotropic medium (e.g.: inside a glass of water) water molecules naturally move randomly according to Brownian motion. In biological tissues however, the diffusion may be anisotropic that is to say the diffusion properties vary with orientation. The recent development of Diffusion Tensor Imaging (DTI) (see [7]) enables diffusion to be measured in multiple directions and the fractional anisotropy in each direction to be calculated for each voxel. The most important base concepts are reviewed, while a complex overview of anisotropic water diffusion is presented by Beaulieu (see [1]).

2.1. Diffusion tensor

It is well known that the diffusion in white matter is the largest along fiber directions. When diffusion is anisotropic, a scalar diffusion measure is insufficient for describing diffusion properties. It has been shown that the diffusion in this case can be described by a second-order diagonally symmetric tensor, called the diffusion tensor. This tensor model of diffusion can be used well to describe the directional diffusion information.

$$D = \begin{pmatrix} D_{xx} & D_{xy} & D_{xz} \\ D_{yx} & D_{yy} & D_{yz} \\ D_{zx} & D_{zy} & D_{zz} \end{pmatrix}$$

The six independent elements of the diffusion tensor can be estimated from a series of diffusion-weighted images. When diffusion weighted measurements are performed along N directions, the following matrix equation can be constructed (see [5]):

$$B\vec{d}^{\,T} = \vec{A}^{\,T}$$

where

$$\vec{A} = \begin{pmatrix} \ln\frac{S_1}{S_0} & \ln\frac{S_2}{S_0} & \dots & \ln\frac{S_N}{S_0} \end{pmatrix}$$

is the vector of the corresponding logarithmic signal ratios and

$$B = \begin{pmatrix} \vec{b_1} \\ \vec{b_2} \\ \vdots \\ \vec{b_N} \end{pmatrix}$$

includes the influences of all the encoding gradients.

3. The process of calculation

In practice 25 files are provided usually containing the results of diffusion weighted measurements, and we need also a sepatare file describing the baseline data. All of them serve as input data of the algorithm and they are referred as volume of voxels further on. The input files have an extention ’mnc’ because they have a special inner structure. A plug-in is responsible for writing and reading of this file type.

3.1. Diffusion tensor

During the calculation special volume iterators are used, that makes more convenient to reach all the data belonging to the same voxel at same time in a very effective way. This makes also possible that the algorithm remains independent from the size of volumes. The names of input files are used as command line parameters, that is why the program are able to handle dinamically the number of input volumes. A function was constructed to determine the six tensor elements of a voxel, which works in the following way.

1. If the input data make possible the gradients themselves are yielded or default values are used instead.

2. The components of vector A are calculated based upon the signal values. (S_0 denotes the value derived from the baseline data.)

3. The equation itself is solved by using the appropriate function of GSL. The GNU Scientific Library (GSL) is a numerical library for C and C++ programmers, which is a free software under the GNU General Public License and provides a wide range of mathematical routines. The selected GSL function is able to find the least squares solution to our overdetermined system.

4. Finally the resulted 6 values, that is to say the 6 independent elements of diffusion tensor are to be stored in appropriate position of new volumes.

3.2. Parameters of diffusion ellipsoid

A principal frame of directions (x', y' and z') can be defined by the eigenvectors of the diffusion tensor for each voxel. The diffusion displacement profile may be represented as an ellipsoid with the length of principal axes described by the tensor eigenvalues λ_1, λ_2 and λ_3 (principal diffusivities) and the directions given by the tensor eigenvectors ($\vec{e_1}$, $\vec{e_2}$ and $\vec{e_3}$). Figure 1 shows the geometric meanings of the computed values.

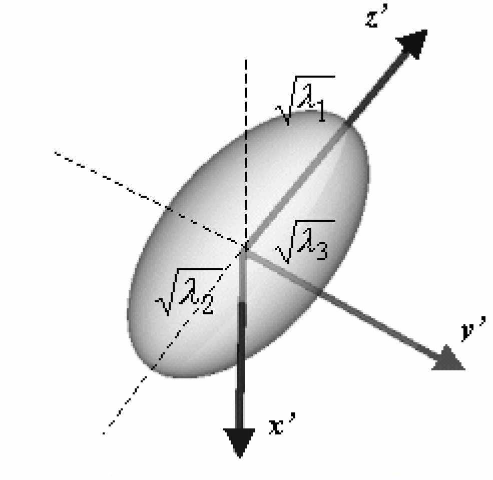


Figure 1: The diffusion ellipsoid.

The diffusion eigenvectors are generally not aligned with the laboratory frame. In the principal component frame, the displacements along x', y', and z' appear uncorrelated and the diagonal elements of the tensor are equal to tensor eigenvalues. The major axes are given by the diffusion tensor eigenvectors. The length of the ellipsoid along the axes is proportional with the square root of the tensor eigenvalues.

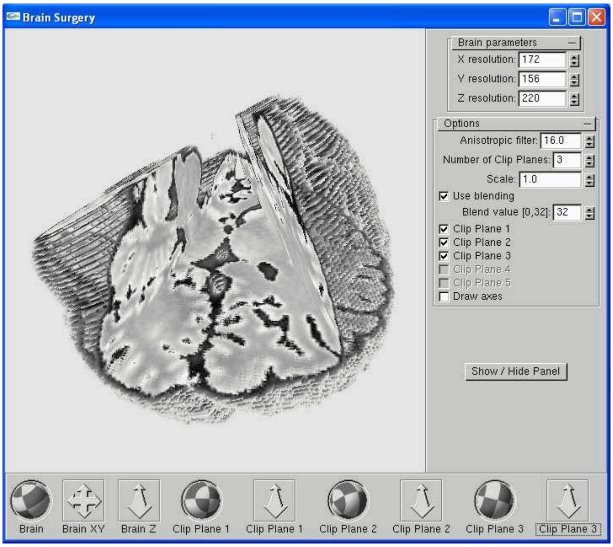
Depending on the relation between the eigenvalues volume, three types of diffusion and corresponding ellipsoidal shapes can be differentiated:

a) Isotropic diffusion: $\lambda_1 \approx \lambda_2 \approx \lambda_3$
Diffusion in gray matter and fluids generally appears isotropic. The corresponding diffusion ellipsoid has a spherical shape.

b) Planar diffusion: $\lambda_1 \approx \lambda_2 \gg \lambda_3$
Planar diffusion is generally associated with diffusion in sheets or it may describe regions of crossing fibers. The corresponding diffusion ellipsoid has a special disk shape.

c) Prolate diffusion: $\lambda_1 \gg \lambda_2 > \lambda_3$
Prolate or uniaxial diffusion is observed in highly organized white matter regions. The corresponding diffusion ellipsoid has a prolate shape.

White matter structures (corpus callosum and corticospinal tract) are generally characterized by uniaxial diffusion. Planar diffusion is dominant in regions of crossing or fanning fibers. For the visualization of the stream directions at each voxel ellipsoids are used. These ellipsoids can be incorporated with the brain model. Figure 2 shows how the brain can be clipped by three arbitrary planes that is not common in usual softwares.



Brain parameters
X resolution: 172
Y resolution: 156
Z resolution: 220

Options
Anisotropic filter: 16.0
Number of Clip Planes: 3
Scale: 1.0
☑ Use blending
Blend value [0,32]: 32
☑ Clip Plane 1
☑ Clip Plane 2
☑ Clip Plane 3
☐ Clip Plane 4
☐ Clip Plane 5
☐ Draw axes

Figure 2: Brain clipped by three arbitrary positioned planes.

From the computed diffusion ellipsods fibers can be built up (see [4]). Current algorithms do not handle the fiber crossings. In this case they follow the stronger track only. For the dynamic modelling of the fibers, we apply a particle system (see [3]). The molecule groups inspected by the measurements can be modelled by points moving along the actual fiber. These fibers make up a complex brain structure. For example the tumors distort the fibers, so a change in the fiber structure prognosticate the illness.

Moreover, our software is capable to handle more pictures (e.g.: one individual and one picture that is common for a population) and blend them together in any ratio. Besides, we can enhance a strip of the brain around any given intensity value.

The above work uses the OpenGL system, particularly its multitexturing, 3D texturing and alpha blending subsystems.

4. Conclusion and further research

The standard algorithms are improved and new methods are developed by our team considering the branching and merging problems also. We plan to massively parallelize the algorithms by using heavily the shader languages (vertex, geometry and pixel shaders).

Beyond the completed new methods, we want to combine them as the final step. We will integrate the ellipsoids and the particle system with the brain model having arbitrary clipping planes.

References

[1] Beaulieu, C., The basis of anisotropic water diffusion in the nervous system, *NMR Biomed.*, Vol. 15 (2002), 435–455.

[2] Lazar, M., White matter tractography: an error analysis and human brain fiber tract reconstruction study (PhD dissertation, University of Utah) (2003).

[3] McReynolds, T., Blythe, D., Advanced Graphics Programming Using OpenGL *Morgan Kaufmann* (2005)

[4] Mori, S., van Zijl, P.C.M., Fiber tracking: principles and strategies - a technical review, *NMR Biomed.*, Vol. 15 (2002), 468–480.

[5] Papadakis, N.G., Xing, D., Huang, C.L., Hall, L.D., Carpenter, T.A., A comparative study of acquisition schemes for diffusion tensor imaging using MRI, *J. Magn. Reson.*, Vol. 137 (1999), 67–82.

[6] Rost, R.J., OpenGL ® Shading Language, Second Edition *Addison Wesley Professional* (2006).

[7] Taylor, A.J., Diffusion tensor imaging: evaluation of tractography algorithm performance using ground truth phantoms (Thesis, Virginia Polytechnic Institute and State University) (2004).

Henrietta Tomán
Department of Computer Graphics
University of Debrecen
Egyetem tér 1.
H-4010 Debrecen, Hungary

Róbert Tornai
Department of Computer Graphics
University of Debrecen
Egyetem tér 1.
H-4010 Debrecen, Hungary

Marianna Zichar
Department of Computer Graphics
University of Debrecen
Egyetem tér 1.
H-4010 Debrecen, Hungary

Methodological papers

Annales Mathematicae et Informaticae
34 (2007) pp. 113–122
http://www.ektf.hu/tanszek/matematika/ami

Spatial ability of engineering students

Rita Nagy-Kondor

Faculty of Technical Engineering
University of Debrecen
e-mail: rita@mfk.unideb.hu

Submitted 20 November 2007; Accepted 11 December 2007

Abstract

We made the survey in September 2004 and 2006 in the University of Debrecen, Faculty of Technical Engineering among first year engineering students. In the beginning of the semester on the first week we examined with a test whether the students have sufficient differences between their spatial ability, their fundamental knowledge on descriptive geometry, since it is essential for the students to look at projections and to make operations with them and also to see the bodies with their mind's eye. We prepared the test in a way that it contained the important components of the spatial ability.

Keywords: spatial ability

1. Introduction

This article reports about a survey about the topic of spatial ability. In the University of Debrecen, Faculty of Technical Engineering we surveyed the knowledge of 80 first year mechanical engineering students. We get most of our knowledge in a visual way so it is very important for us how much we are aware of the language of vision. The definition of spatial ability according to Séra and his colleagues – relying on the ideas of Haanstra [5, p. 88] and others – is the following: "the ability of solving spatial problems by using the perception of two and three dimensional shapes and the understanding of the perceived information and relations" [12, p. 19].

Gardner [4] distinguishes between seven different types of intelligence: linguistic, logical-mathematical, spatial, musical, physical-kinaesthetic, interpersonal and intrapersonal. According to Gardner [4, p. 9] the "spatial intelligence is the ability of forming a mental model of the spatial world and manoeuvring and working with this model". The multiple intelligence theory was improved by Maier [8], distinguishing between five branches of spatial intelligence:

- spatial perception: the perpendicular and horizontal fixation of direction regardless of troublesome information;
- visualisation: it is the ability of depicting of situations when the components are moving compared to each other;
- mental rotation: rotation of three dimensional solids mentally;
- spatial relations: the ability of recognizing the relations between the parts of a solid;
- spatial orientation: the ability of entering into a given spatial situation.

Vásárhelyi's definition of geometrical spatial ability [16]: the mathematically controlled complex unity of abilities and skills that allows:

- the exact conception of the shape, the size and the position of the spatial configurations;
- the unequivocal illustration of seen or imaginary configurations based on the rules of geometry;
- the appropriate reconstruction of unequivocally illustrated configurations;
- the constructive solution of different spatial (mathematical, technological, etc.) problems, and the imagery and linguistic composition of this solution.

Séra and his colleagues [12] are approaching the spatial problems from the side of the activity. The types of exercises:

- projection illustration and projection reading: establishing and drawing two dimensional projection pictures of three dimensional configurations;
- reconstruction: creating the axonometric image of an object based on projection images;
- the transparency of the structure: developing the inner expressive image through visualizing relations and proportions;
- two-dimensional visual spatial conception: the imaginary cutting up and piecing together of two-dimensional figures;
- the recognition and visualization of a spatial figure: the identification and visualization of the object and its position based on incomplete visual information;

- recognition and combination of the cohesive parts of three-dimensional figures: the recognition and combination of the cohesive parts of simple spatial figures that were cut into two or more pieces with the help of their axonometric drawings;

- imaginary rotation of a three-dimensional figure: the identification of the figure with the help of its images depicted from two different viewpoints by the manipulation of mental representations;

- imaginary manipulation of an object: the imaginary following of the phases of the objective activity;

- spatial constructional ability: the interpretation of the position of three-dimensional configurations correlated to each other based on the manipulation of the spatial representations;

- dynamic vision: the imaginary following of the motion of the sections of spatial configuration.

The conventions of the spatial representation can be taught effectively at the age of 9–12. The demand for the visualisation and drawn expression of the three-dimensional space appears at the age of 12–14. According to the experience of art teachers, the space representation has to be taught for some children because they would never reach that level by themselves. [12] Therefore our image and definitions of space are not congenital; they are the result of a long developmental and experimental learning process.

Mental Cutting Test (MCT) is one of the most widely used evaluation method for spatial abilities. Németh and Hoffmann [9, 10] presented an analysis of MCT results of first-year engineering students, with emphasis on gender differences. They used the classical MCT test for first-year engineering students of Szent István University. Németh, Sörös and Hoffmann [11] attempted to find possible reasons of gender difference, concluding, that typical mistakes play central role in it. They show typical mistakes can be one of the possible reasons, since female students made typical mistakes in some cases more frequently than males.

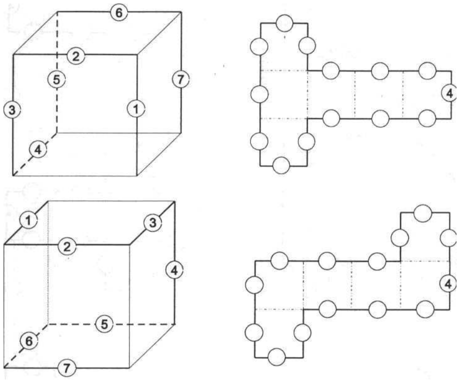
2. The survey and its results

We made the survey in September 2004 and 2006 in the University of Debrecen, Faculty of Technical Engineering among first year mechanical engineering students. In the beginning of the semester on the first week we examined the students' spatial ability and fundamental knowledge on descriptive geometry, since it is essential for the students to look at projections and to make operations with them and also to see the bodies with their mind's eye. 80 students took the test. The students had 50 minutes to complete the task sheet. We prepared the test in a way that it contained the important components of the spatial ability.

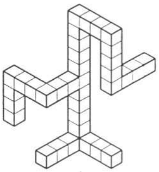
Shea and his colleagues [13] state that the intellectually talented adolescents who has better spatial than verbal abilities are more likely to be found in the field of engineering, computer sciences and mathematics. We according to the researches of Shea and his colleagues [13], expect a good result from engineer students.

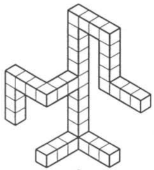
The tasks of the test:

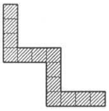
1. The network of a cube was cut by the bordering lines and after making the flexion the cutting lines that became next to each other we stuck together. The axonometric representations of the cube, the stuck edges are marked with a wide line and we numbered them. Mark those cutting lines with the same number on the network that was moved next to each other by sticking! [14]

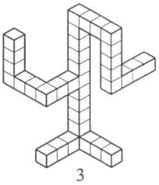


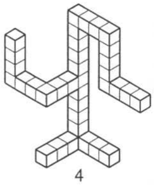
2. Which of the bodies that are numbered on the sheet can enter the lined gap? [14]


1

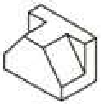

2

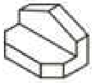


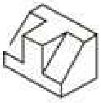

3

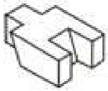

4

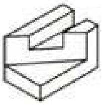
3. Make pairs of these bodies and projection pictures! [3]

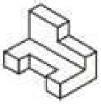
1


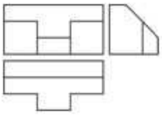
2


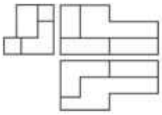
3


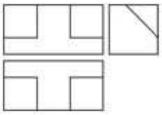
4


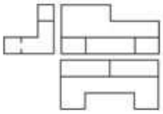
5


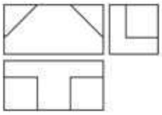
6


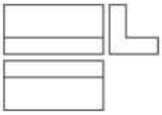
a


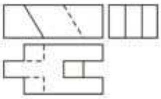
b


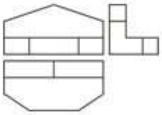
c


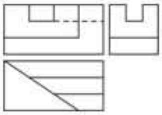
d


e


f


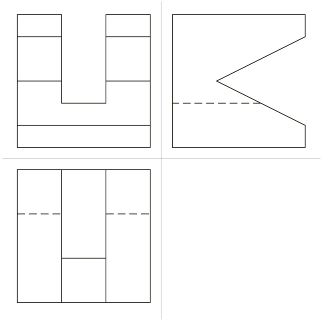
g


h


i


1	
2	
3	
4	
5	
6	

4. Make an axonometric picture according to the projections!



5. Make the projections of the given body!

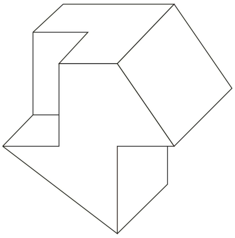


Figure 1 shows the performance of the students on the test.

Following the theory of Séra and his colleagues [12] we made the task sheet from the more important types of tasks. The first task focuses on the imaginary manipulation of the solid. The task is to follow such phases of the objective activity that consist of the complex spatial transformation of the solid. The second task focuses on the imaginary rotation of a three-dimensional figure. The third and fifth tasks belong to the types of tasks that deals with representation and reading of the projection. By mobilizing the experience of the motion, changing the inner viewpoint, imaginary rotation, manipulation of mental representations, and the task is to produce and draw the two-dimensional projection picture of a three-dimensional solid. This type of task is characterized by analytical operations from concrete to abstract. The fourth task is a reconstructural task. We have to create the axonometric picture of the solid based on the projection pictures. During the reconstruction the student synthesizes the visual information by studying the projection pictures. The map will be constructed by the series of changing the inner viewpoint by harmonizing three channels.

The first three tasks were solved with an 80 percent success or more. The imaginary manipulation of the object, the imaginary rotation of a solid and reading of projection went well. Some of the students wrote the numbers to a wrong place in part two of task 1. The 14 percent of the students gave only one solution in

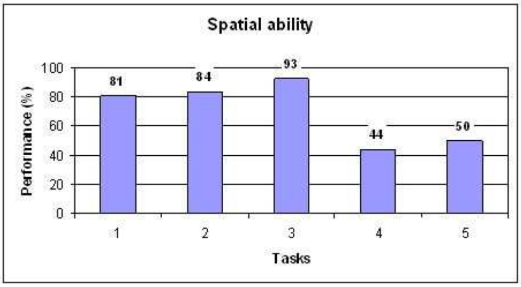


Figure 1: The results of the test

task 2.

The task 3 was the biggest success, where the bodies had to be compared with the projection pictures. To make the task more difficult, there were more projections as bodies. Some of the students wrote wrong letter to body 1 or body 3 or body 6.

Task 4 and 5 were like task 3, but here the projection or the body was missing. As opposed to this, these tasks were the least successful. The 36 percent of the students reconstructed the solid incorrectly or incompletely based on its projection picture in task 4 (Figure 2). Some of the students did not even start the task at all.

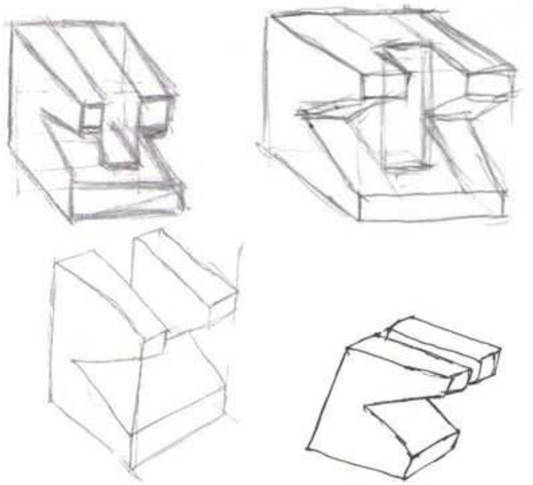


Figure 2: Some solutions of the students (Task 4)

55 percent of the students reversed the order of projections or represented in-

completely (Figure 3).

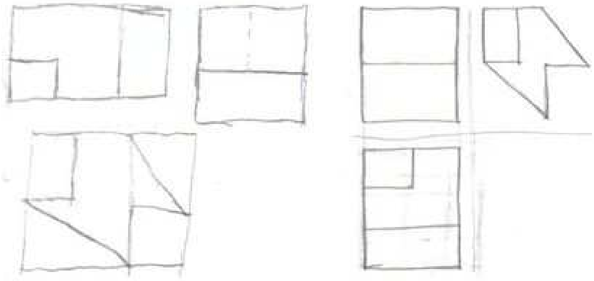


Figure 3: Some solutions of the students (Task 5)

Further study of spatial ability and other tests with more tasks from the more important types of tasks are among our future aims.

3. Summary

The results of the survey prove that it causes a problem for many students to imagine a spatial figure, the reconstruction and representation of the projection. In contrast to Shea and his colleagues [13] we found that the students of our survey, they do not have really good spatial ability. How could we develop the spatial ability?

Lord applied a 30 minutes practise on a 14 weeks course with first/second year students where they had tasks in which they had to cut three-dimensional solids in their mind and then they had to draw the surface of the two-dimensional planes they got. [7] In the post-test the spatial awareness and efficiency became better.

Field [2] describes work conducted at Monash University aimed at measuring spatial skills, improving the sensitivity of visualisation tests, and developing the skill for some engineering undergraduates. The testing of undergraduate students at Monash University has indicated the following factors:

- First level engineering students are to possess specially higher spatial skills than the general population.
- Spatial skills are not measurably developed by a conventional mechanical engineering undergraduate course.
- A special course with about 50 contact hours appears to have been successful in developing visualisation skill in first level engineers. (There is some evidence that freehand drawing of three dimensional objects, in orthogonal, isometric and perspective views makes a major contribution to the development of spatial skill.)

According to Horváth and his colleagues [6] in the teaching and learning of geometry the three-dimensional models can be a great help. It is much easier to imagine and represent the different views of a solid when we can see the formal characteristics. The proper use and frequent study of spatial visual aids can result in such an inner spatial vision that makes the individual imagination of the spatial relations possible. [16] The effectiveness of teaching spatial geometry can be influenced to a great extent by using several different models that we can even prepare ourselves. Vásárhelyi [15] calls the attention to the use of computers besides the traditional models, because they provide help for the motivation of the students. According to Vásárhelyi [16] it is practical to make four periods in the usage of models:

- with models,
- with models and their pictures,
- with pictures and their prepared models or animated pictures,
- problemsolving only with the help of pictures.

Bakó [1] was studying the conditions of the beneficial usage of computer in the teaching of spatial geometry. On the grounds of her researches she concluded that in acquiring the basic definitions of spatial geometry and the cognition of solids, the usage of models are still needed. After the development of basic abilities, the computer can get a role in developing the spatial intelligence from the 7th year of the primary school. She found that the help of the computer could develop all of the skills given by Maier [8]. At the same time, she experienced that we should not overdo the use of computers, because the explanation of the teacher, the usage of models and individual work are needed as well.

Development of the spatial ability is a very important task because we have to understand and develop the geometry knowledge of the students in the unity of the theoretical knowledge and the spatial abilities. Every skill, like the spatial ability as well can be developed at the right age with the suitable teaching strategy.

References

[1] Bakó, M., Utilisation de l'ordinateur pour le développement de la vision spatiale, *These En Co-Tutelle, L'école doctorale CLESCO, Université Paul Sabatier, Toulouse et de L'école doctorale de Mathématiques et Informatiques, Université de Debrecen*, (2006).

[2] Field, B. W., A Course in Spatial Visualisation, *Journal for Geometry and Graphics*, Vol. 3 (1999), No. 2, 201–209.

[3] French, T.E., Vierck, C.J., The Fundamentals of Engineering Drawing and Graphic Technology, *McGraw-Hill Book Company*, New York (1978).

[4] Gardner, H., Frames of mind: the theory of multiple intelligences, *Basic Books*, New York (1983).

[5] Haanstra, F.H., Effects of art education on visual-spatial and aesthetic perception: two meta-analysis, *Rijksuniversiteit Groningen*, Groningen (1994).

[6] Horváth, J., Kiss, A., Horváth, L., Néhány gondolat a térszemlélet fejlesztéséről, *Szombathelyi Berzsenyi Dániel Tanárképző Főiskola Tudományos Közleményei, VIII. Módszertani dolgozatok*, Szombathely (1991).

[7] Lord, T.R., Enhancing the visuo-spatial aptitude of students, *Journal of Research in Science Teaching*, Vol. 22 (1985), No. 5, 395–405.

[8] Maier, P.H., Spatial geometry and spatial ability – How to make solid geometry solid? *In Elmar Cohors-Fresenborg, K. Reiss, G. Toener, and H.-G. Weigand, editors, Selected Papers from the Annual Conference of Didactics of Mathematics 1996*, Osnabrueck (1998), 63–75.

[9] Németh, B., Measurement of the development of spatial ability by Mental Cutting Test, *Annales Mathematicae et Informaticae*, Vol. 34 (2007), 123–128.

[10] Németh, B., Hoffmann, M., Gender differences in spatial visualization among engineering students, *Annales Mathematicae et Informaticae*, Vol. 33 (2006), 169–174.

[11] Németh, B., Sörös, Cs., Hoffmann, M., Typical mistakes in Mental Cutting Test and their consequences in gender differences, *Teaching Mathematics and Computer Science*, (to appear).

[12] Séra, L., Kárpáti, A., Gulyás, J., A térszemlélet, *Comenius Kiadó*, Pécs (2002).

[13] Shea, D.L., Lubinski, D., Benbow, C.P., Importance of assessing spatial ability in intellectually talented young adolescents: A 20-year longitudinal study, *Journal of Educational Psychology*, Vol. 93 (2001), 604–614.

[14] Varga, L., Térszemlélet-fejlesztés, *JGYF Kiadó*, Szeged (1999).

[15] Vásárhelyi, É., A geometriai térszemlélet fejlesztése dinamikus geometriai programmal, `http://ikon.inf.elte.hu/~kid/ELEMIMAT/BLOKK2003/terszemlelet/TERSZEML.HTML`

[16] Vásárhelyi, É., A vizuális reprezentáció fontossága a matematikaoktatásban, `http://ikon.inf.elte.hu/~kid/ELEMIMAT/BLOKK2003/vizualis/VIZUALIS.HTML`

Rita Nagy-Kondor
H-4028 Debrecen
Ótemető u. 2-4.
Hungary

Annales Mathematicae et Informaticae
34 (2007) pp. 123–128
http://www.ektf.hu/tanszek/matematika/ami

Measurement of the development of spatial ability by Mental Cutting Test

Brigitta Németh

Department of Descriptive Geometry and Computer Science
Szent István University
e-mail: nemeth.brigitta@ymmfk.szie.hu

Submitted 28 September 2007; Accepted 3 December 2007

Abstract

Spatial visualization of first-year engineering students has been evaluated at the beginning and at the end of the two semesters, which contain the essential Descriptive Geometry courses. The evaluation has been processed by Mental Cutting Test (MCT) which is one of the most widely used evaluation method for spatial abilities. In this paper we present an analysis of MCT results of the students, with special emphasis on gender differences. The development is found to be considerable while gender differences have became even more significant during this period.

Keywords: spatial visualization, spatial skills, MCT, gender differences

MSC: 51N05

1. Introduction

Spatial abilities are obviously essential in engineering studies. These abilities are not determined genetically, but rather a result of a long learning process. This fact is proved by Piaget's experiences and examinations by twins [1]. Due to Wallon a certain minimum of spatial imagination is a common basement and requirement for all kind of intelligence [2]. Since there are various theories about intelligence itself, there are also different approaches to spatial imagination: while Lohman considers three factors of spatial abilities as visualization, spatial orientation and fast rotation [3], McGee defines it as "the ability to mentally manipulate, rotate, twist or invert pictorally presented stimuli" [16] and classifies five components of spatial skills as spatial perception, spatial visualization, mental rotations, mental relations and spatial orientation.

The measurement of spatial abilities is standardized by international tests, among which Mental Rotation Test (MRT) and Mental Cutting Test (MCT) are of greatest importance. Mental Rotation Test is introduced by Vanderberg and Kuse [17], while Mental Cutting Test, originally developed for entrance examination in the United States [18], has a long history and widely used for testing the spatial ability of students at any level. Other tests can also be mentioned like Objective Test on Orthographic Projection (OTO) evaluating the effects of the education in orthographic view [6], or Space Imagination Test (TPP) developed by international cooperation in VEGA project [10], or a test by Guay entitled Purdue Spatial Visualization Test [4]. This latter test consists of three parts: Developments, Rotations and Views. Developments consists of 12 questions designed to see how well students can visualize the folding of developments into three-dimensional objects. Rotations consists of 12 questions to evaluate the visualization of the rotation of three-dimensional objects. Finally Views consists 12 questions to visualize how three-dimensional objects look like from various viewing positions. Similar test has been applied in [13].

The aim of this paper is to evaluate classical MCT test results of first-year engineering students in Hungary, with special emphasis on gender differences.

2. The Mental Cutting Test

In our project we used the standard Mental Cutting Test, which consists of 25 problems. In each problem a perspective drawing of a solid body is given, which has been cut by a plane. Students are asked for choosing the cross section among the 5 given alternatives, always one being correct.

Basically there are two different types of problems can be found in MCT: pattern recognition problems and quantity problems [7]. In the first category one can find strongly different alternatives of possible cross sections, thus the right solution can be found simply by recognizing the pattern of the section from the spatial figure. In the quantity problems, however, some of the cross sections are similar (more precisely affine) to the correct one, thus the right answer can be determined only by guessing the relative quantities, like ratios of lengths or angles between the edges.

Most of the solids in MCT have relatively complicated, unusual forms, some of them are truncated cubes, others are curved objects, like cylinders. As Tsutsumi et al. reported in [8], failures are mostly based on the fact that students are not able to recognize the spatial form of the object.

3. Results - Improvement of spatial ability

Here we used the classical MCT test for first-year engineering students of Szent István University. At the beginning of the first semester 250 students filled the MCT test, third of them being females. Based on these tests gender differences have been studied in [14], while typical mistakes have been observed and examined in [15].

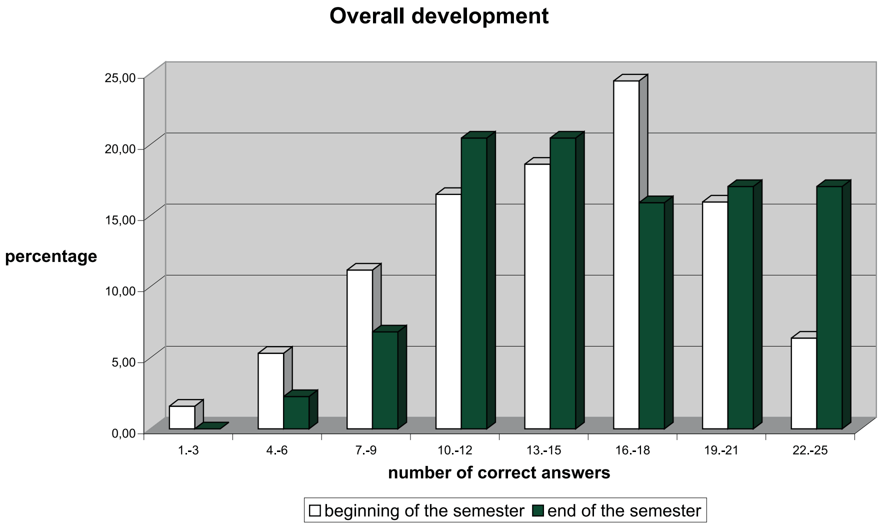


Figure 1: Correct answers at the beginning of the first semester (white) and at the end of the second semester (dark).

At the end of the second semester, which included various descriptive geometry studies, like Axonometry, Monge-projection and partly Perspective Drawing, more than 100 tests have been filled by these students. Main purpose of our study was to evaluate the improvement of spatial abilities after these Descriptive Geometry courses. Diagram in Fig. 1 shows the overall development of the students, where the improvement is obvious, especially in the lowest and highest rankings. Means of the results before and after the semesters show statistically significant difference at the level of 98% by one-sample t-test [5].

There are few problems where the results were lower at the end of the year. These are all quantitative problems, that is sections are closely related in structure, differing only in lengths and angles. These problems seem to be the hardest ones for the students.

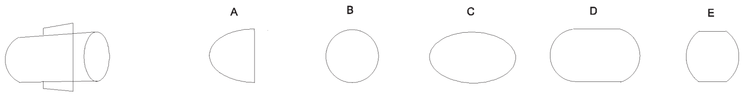


Figure 2: Problem 118: section of a cylinder.

In problem 118 (Fig. 2), however the improvement was more than 20%. This is the section of a cylinder, which is studied at the end of the second semester, thus students may remember well for this problem .

Gender differences were also evaluated before and after the semesters. At the beginning of the semester, similarly to the results of Tsutsumi [7], we observed significant difference between male and female students [14, 15].

At the end of the semester this difference were also significant, measured by two-sample t-test [5]. As one can observe in diagrams of Fig. 3 and Fig. 4, the improvement of spatial ability is even higher for male students, which yields that gender differences were getting stronger.

Male students achieved especially high degree improvement in the highest range (between points 22–25), from 8.82% to 29.79%, but development is also remarkable in the second highest range (between point 19–21) (Fig. 3).

For female students the improvement of spatial ability is not as remarkable and obvious, as for males. There is good improvement in the lowest range (between points 0–9), and some development (although far from that one by males) in the highest range (between points 19–25). The most obvious improvement can be observed in the middle range (between points 10–15) (Fig. 4).

These results support our strong belief that teaching descriptive geometry can highly improve the spatial ability of students. However this improvement is more reliable in the case of male students, female engineering students can also gain some extra ability during these courses, especially those who had only limited spatial imagination previously.

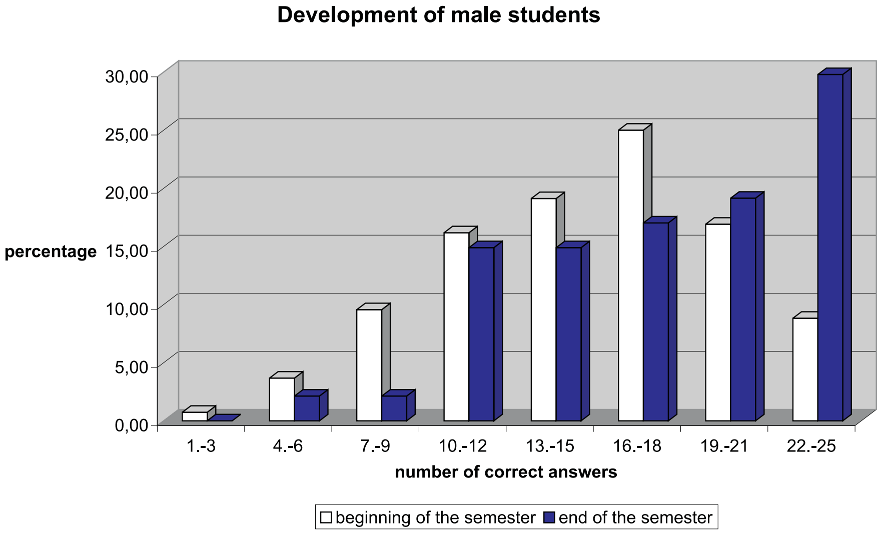


Figure 3: Improvement of spatial ability of male students.

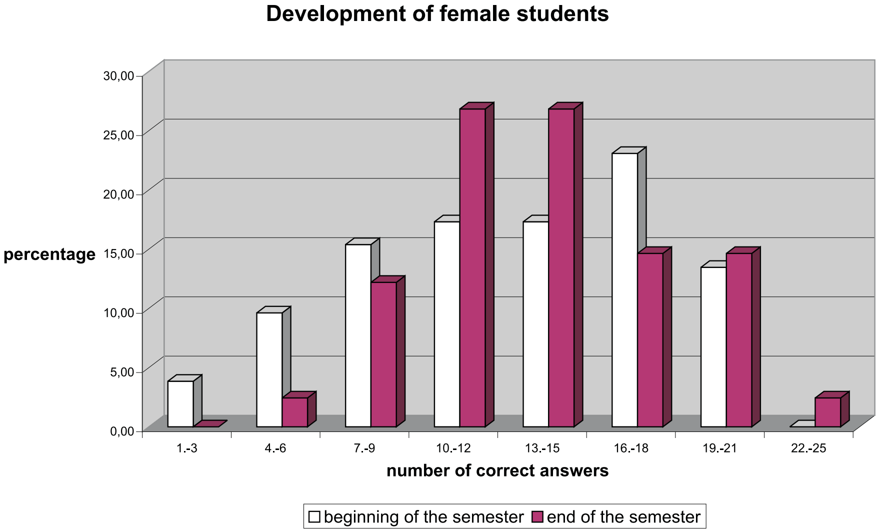


Figure 4: Improvement of spatial ability of female students.

4. Conclusion and further research

Spatial imagination of engineering students has been studied in this paper. Their abilities were tested by the standard MCT tool which is widely used for this purpose. In accordance with the international experiences we observed relevant improvement after two semesters of descriptive geometry courses. Differences in male and female students' abilities, however, remained the same, development of male students was more significant. Future work will be focused on longitudinal research with regular testing periods along their university studies.

References

[1] Inhelder, B., Piaget, J., A gyermek logikájától az ifjú logikájáig. A formális műveleti struktúrák kialakulása, *Akadémiai Kiadó*, Budapest, 1967.

[2] Wallon, H., Délire de persécution. Le délire chronique a base d'interprétation, Bailliere, Paris, 1909.

[3] Lohman, D.F., Nichols, P.D.,Training spatial abilities: Effects of practice on rotation and synthesis tasks, *Learning and Individual Differences*, **2** (1990), 67–93.

[4] Guay, R.B., Purdue Spatial Visualization Test, *Purdue Research Foundation,* 1976.

[5] Guilford, J.P., Fundamental Statistic in Psychology and Education, McGraw Hill, New York, 1965.

[6] Takeyama, K., Maeguchi, R., Chibana, K., Yoshida, K., Evaluation of Objective Test using a pair of orthographic projections for descriptive geometry, *Journal for Geometry and Graphics*, **3** (1999), 99–109.

[7] Tsutsumi, E., A Mental Cutting Test using drawings of intersections, *Journal for Geometry and Graphics*, **8** (2004), 117–126.

[8] Tsutsumi, E., Shiina, K., Suzaki, A., Yamanouchi, K., Takaaki, S., Suzuki, K., A Mental Cutting Test on female students using a stereographic system, *Journal for Geometry and Graphics*, **3** (1999), 111–119.

[9] Gorska, R., Sorby, S., Leopold, C., Gender differences in visualization skills - an international perspective, *The Engineering Design Graphics Journal*, **62**, (1998), 9–18.

[10] Juscaková, Z., Gorska, R., A pilot study of a new testing method for spatial abilities evaluation, *Journal for Geometry and Graphics*, **7** (2003), 237–247.

[11] Gorska, R., Spatial imagination - an overview of the longitudinal research at Cracow University of Technology, *Journal for Geometry and Graphics*, **9** (2005), 201–208.

[12] Gorska, R., Sorby, S., Leopold, C., International comparisons of gender differences in spatial visualization and the effect of graphics instruction on the development of these skills, *Proc. of the 8th Intl. Conf. of Engineering Comp. Graph. and Descriptive Geom. (ICECGDG), Austin, USA*, 1998, 261–266.

[13] Nagy-Kondor, R., Spatial ability of engineering students, *Annales Mathematicae et Informaticae*, Vol. 34 (2007), 113–122.

[14] Németh, B., Hoffmann, M., Gender differences in spatial visualization among engineering students. *Annales Mathematicae et Informaticae*, **31** (2006), 169–174.

[15] Németh, B., Sörös, Cs., Hoffmann, M., Typical mistakes in Mental Cutting Test and their consequences in gender differences, *Teaching Mathematics and Computer Science* (to appear).

[16] McGee, M.G., Human Spatial Abilities: Psychometric studies and environmental, genetic, hormonal and neurological influences, *Psychological Bulletin*, **86**, 899–918.

[17] Vanderberg, S.G., Kuse, A.R., Mental Rotations, a group test of three dimensional spatial visualization, *Perceptual and Motor Skills*, **47** (1978), 599–604.

[18] CEEB Special aptitude test in spatial relations, College Entrance Examination Board, USA, 1939.

Brigitta Németh
Department of Descriptive Geometry and Compute Science
Szent István University
Thököly str. 74.
H-1146 Budapest, Hungary