

NOTES

Edited by **Jimmie D. Lawson and William Adkins**

A Simple Slide Rule for Finite Fields

Holger Schellwat

We describe how an index table for a finite field can be constructed easily by hand, provided that a primitive polynomial for that field is given.

Let q be a prime number and let n be a positive integer. Addition in the finite field \mathbf{F}_{q^n} of q^n elements is very easy if one views it as an n -dimensional vector space over \mathbf{F}_q (the integers modulo q). Likewise, multiplication in \mathbf{F}_{q^n} is very easy as its multiplicative group $\mathbf{F}_{q^n}^*$ is cyclic. In order to illustrate arithmetic in \mathbf{F}_{q^n} , involving both operations, most undergraduate algebra texts use the representation of \mathbf{F}_{q^n} as the factor ring of $\mathbf{F}_q[x]$ modulo the principal ideal generated by the minimal polynomial of \mathbf{F}_{q^n} over \mathbf{F}_q . Certainly, this illuminates the concept of factor rings, but actual computations can become tedious, as reduction modulo the ideal requires long division.

A very useful tool for finite field arithmetic is an *index table*. Before we explain this, let us briefly recall some theory of finite fields. As $\mathbf{F}_{q^n}^*$ is cyclic, every nonzero $b \in \mathbf{F}_{q^n}$ can be written as a power $b = \alpha^i$ of a generator α of that group, with a unique integer exponent $0 \leq i < q^n - 1$. This exponent is called the *index* of the element b , denoted by $i = \text{ind}_\alpha(b)$. Such a generator α is called a *primitive element* of \mathbf{F}_{q^n} ; it is a root (in \mathbf{F}_{q^n}) of a *primitive polynomial* $f(x) \in \mathbf{F}_q[x]$. Conversely, every root of a primitive polynomial is a primitive element. Suppose that we are given a primitive polynomial $f(x)$ for \mathbf{F}_{q^n} over \mathbf{F}_q . Then we can tie together the multiplicative structure of \mathbf{F}_{q^n} with its additive structure. We fix a root α of f , and the former is just the cyclic group generated by α . The latter is a vector space, having a basis $\mathcal{B} = \{1, \alpha, \dots, \alpha^{n-1}\}$. So every nonzero field element can be viewed as a power of α and as a linear combination of powers of α with coefficients in \mathbf{F}_q . The index table establishes the correspondence, listing for every exponent $0 \leq i < q^n - 1$ (as a column) the coordinates of the vector α^i with respect to \mathcal{B} . It works like a logarithm table, as the exponentiation laws for rings imply that $\text{ind}_\alpha(b \cdot c) = \text{ind}_\alpha(b) + \text{ind}_\alpha(c)$. Hence, all arithmetic in \mathbf{F}_{q^n} becomes easy: addition is vector addition modulo q , and multiplication is carried out using the table.

But where do we get the index table from? For example, the standard reference for finite fields conveniently contains nearly four pages of index tables [3, pp. 546–549]. However, we can construct our own tables very easily by hand (if n and q are not too large), provided that we know a primitive polynomial f of \mathbf{F}_{q^n} over \mathbf{F}_q . This construction is the aim of this Note. The reference [3] contains many primitive polynomials, too. Before we illustrate the method, let us make the notion of an index table precise:

Definition 1. An index table of \mathbf{F}_{q^n} over \mathbf{F}_q is the $n \times (q^n - 1)$ matrix $M = [m_{ij}]$, where $0 \leq i < n$, $0 \leq j < q^n - 1$, and $\alpha^j = \sum_{i=0}^{n-1} m_{ij} \alpha^i$.

Note that we start the numbering at 0. Note also that the index table given in [3] is the transpose of our matrix M .

The key observation is that the columns of an index table satisfy the linear recurrence relation defined by the coefficients of the minimal polynomial of α . Thus, if α is

a zero of the monic primitive polynomial $f = \sum_{k=0}^n f_k x^k$, it follows that the powers of α satisfy the recurrence $\alpha^{n+j} = \sum_{k=0}^{n-1} (-f_k) \alpha^{k+j}$ whenever $0 \leq j < q^n - n - 1$. Since the j th column \bar{m}_j of M is the coordinate vector of α^j with respect to the basis $\mathcal{B} = \{1, \alpha, \dots, \alpha^{n-1}\}$ of \mathbf{F}_{q^n} over \mathbf{F}_q , it follows from the isomorphism $\alpha^j \mapsto \bar{m}_j$ that the columns of M satisfy the same recurrence relation $\bar{m}_{n+j} = \sum_{k=0}^{n-1} (-f_k) \bar{m}_{k+j}$ whenever $0 \leq j < q^n - n - 1$. And hence we have the recurrence relation

$$m_{i \ n+j} = \sum_{k=0}^{n-1} (-f_k) m_{i \ k+j}$$

among the entries of the i th row of M whenever $0 \leq i < n$ and $0 \leq j < q^n - n - 1$.

The first n columns of the table M form an $n \times n$ identity matrix, so we begin by writing down the $n \times n$ identity matrix. Working row after row we construct the remaining entries in every row using the recurrence relation $m_{i \ n+j} = \sum_{k=0}^{n-1} (-f_k) m_{i \ k+j}$. We can simplify this process by assembling a paper slider

$-f_0$	$-f_1$	$-f_2$	\cdots	$-f_{n-1}$	\uparrow
--------	--------	--------	----------	------------	------------

by writing on it the negatives of the first n coefficients of the monic primitive polynomial f , followed by an upward pointing arrow, using the same spacing as in the matrix M . While working in a row, this arrow points to the table entry we want to compute. We multiply the coefficients $-f_k$ on the slider by the entries above them and sum from left to right, as if computing a dot product, and write the result above the arrow. Then we move the slider one step to the right in order to compute the next entry, and so on.

Example 2. $K := \mathbf{F}_2, F := \mathbf{F}_8, f = 1 + x + x^3$, slider

1	1	0	\uparrow
-----	-----	-----	------------

	α^0	α^1	α^2	α^3	α^4	α^5	α^6
1	1	0	0	1	0	1	1
α	0	<u>1</u>	<u>0</u>	<u>1</u>	1	1	0
α^2	0	0	1	0	1	1	1
<i>slider</i>		1	1	0	\uparrow		

Using the underlined entries we compute the entry in the box as $m_{14} = (-f_0) \cdot \underline{1} + (-f_1) \cdot \underline{0} + (-f_2) \cdot \underline{1} = 1 \cdot \underline{1} + 1 \cdot \underline{0} + 0 \cdot \underline{1} = 1$.

Example 3. $K := \mathbf{F}_3, F := \mathbf{F}_9, f = 2 + x + x^2$, slider

1	2	\uparrow
-----	-----	------------

	α^0	α^1	α^2	α^3	α^4	α^5	α^6	α^7
1	1	0	1	2	2	0	2	1
α	0	<u>1</u>	<u>2</u>	2	0	2	1	1
<i>slider</i>		1	2	\uparrow				

We compute $m_{13} = 1 \cdot \underline{1} + 2 \cdot \underline{2} = 2$.

All these concepts carry over to arbitrary finite extensions of finite fields, that is, q can be any prime power. The material necessary to see this can be found in [3]. A different approach to finite field arithmetic can be found in [4]. The latter approach takes less space, but the table approach is faster, once the table is constructed. And it is very easy to implement.

We have not addressed the question of existence and constructability of primitive polynomials. Existence can be shown rather easily using Möbius inversion in number theory [1, Theorem 16.9]. They can be constructed using Conway polynomials [2].

ACKNOWLEDGMENT. I thank Peter Schroth for inspiring conversations.

REFERENCES

1. N. L. Biggs, *Discrete Mathematics*, Oxford University Press, Oxford, 1989.
2. J. H. Conway, A tabulation of some information concerning finite fields, In: *Computers in Mathematical Research*, North-Holland, Amsterdam, 1968, pp. 37–50.
3. R. Lidl and H. Niederreiter, *Finite Fields, Second edition*, vol. 20 of *Encyclopedia of Mathematics and its Applications*, Cambridge University Press, Cambridge, 1997.
4. W. P. Wardlaw, Matrix Representation of Finite Fields, *Math. Mag.* 67 (1994) 289–293.

Örebro University, SE-701 82 Örebro, Sweden
holger.schellwat@nat.oru.se

A General Method for Establishing Geometric Inequalities in a Triangle

Razvan Alin Satnoianu

1. INTRODUCTION The purpose of this note is to present a simple but powerful principle of proof for a large class of geometric inequalities for triangles. The method consists of reducing the case for general triangles to that of isosceles triangles.

For a given euclidean triangle denote by a, b, c the measures of its angles in radians chosen so that

$$0 < a \leq b \leq c < \pi \quad \text{and} \quad a + b + c = \pi. \quad (1.1)$$

(Alternatively, it is occasionally convenient to assume that $c \leq b \leq a$). Then to establish that some inequality $f(a, b, c) \geq 0$ holds, it suffices to show that

$$f(a, b, c) \geq f\left(a, \frac{b+c}{2}, \frac{b+c}{2}\right) \geq 0, \quad (1.2)$$

where the second inequality represents the case of an isosceles triangle. We show that it often proves easier to establish the two inequalities of (1.2) than to establish the original one directly. We illustrate this approach with a variety of examples (taken from the proposed problems published in the MONTHLY through the years) in the next section.

To establish the first inequality, we typically consider the difference

$$e = e(a, b, c) = f(a, b, c) - f\left(a, \frac{b+c}{2}, \frac{b+c}{2}\right) \tag{1.3}$$

and use appropriate trigonometric inequalities to show that $e \geq 0$. One could also set $d = (b+c)/2$ and consider the function $h(t) = f(a, d-t, d+t) - f(a, d, d)$, where $0 \leq t \leq d-a < \pi/2$, note that $h(0) = 0$, and use the methods of calculus to show that h is non-decreasing.

In practice we may have to deal with more complicated forms for f (perhaps depending on other elements such as altitudes, bisectors, radii, etc.). For any such case it is clear that, by using standard results, we can always express these in terms involving only the trigonometric functions of the triangle's angles, which reduces the problem to the case shown above.

2. ILLUSTRATIONS

2.1. In every triangle we have the inequality

$$\sin(a/2) + \sin(b/2) + \sin(c/2) \leq 3/2. \tag{2.1}$$

The classical proof uses the concavity of the function $\sin(x/2)$ on a suitable interval. Using our method we consider the function

$$f(a, b, c) = 1.5 - \sin(a/2) - \sin(b/2) - \sin(c/2).$$

An application of the formula $\sin x + \sin y = 2 \sin((x+y)/2) \cos((x-y)/2)$ shows that

$$\begin{aligned} f(a, b, c) - f\left(a, \frac{b+c}{2}, \frac{b+c}{2}\right) &= 2 \sin\left(\frac{b+c}{4}\right) - \sin\left(\frac{b}{2}\right) - \sin\left(\frac{c}{2}\right) = \\ &= 2 \sin\left(\frac{b+c}{4}\right) \left(1 - \cos\left(\frac{c-b}{4}\right)\right) \geq 0. \end{aligned}$$

Equality occurs only when $b = c$. Further let us prove (2.1) for an arbitrary isosceles triangle. Because of symmetry we need only consider the case $b = c = t, a = \pi - 2t$, say with $t > 0$. Then $f_1 = f(\pi - 2t, t, t) = 3/2 - \cos(t) - 2 \sin(t/2)$, which is non-negative (compute the minimum!) for all $0 \leq t \leq \pi$. Thus (2.1) is proved. Furthermore, equality can hold only when $f_1 = 0$, which happens only for $a = b = c = \pi/3$.

In a similar way one can show that

$$\cos(a) + \cos(b) + \cos(c) \leq 3/2 \tag{2.1.1}$$

$$\sin(a) + \sin(b) + \sin(c) \leq 3\sqrt{3}/2 \tag{2.1.2}$$

$$\sin(a) \sin(b) \sin(c) \leq 3\sqrt{3}/8 \tag{2.1.3}$$

$$\cos(a) \cos(b) \cos(c) \leq 1/8 \tag{2.1.4}$$

$$\sin\left(\frac{a}{2}\right) \sin\left(\frac{b}{2}\right) \sin\left(\frac{c}{2}\right) \leq \frac{1}{8} \tag{2.1.5}$$

and so on. In fact (2.1.2–2.1.3 have appeared as problem E 3038 in the MONTHLY [6, p. 140], proposed by T. Sekiguchi.

Another example where the method of Section 2.1 is applicable is the following

$$3(\cos(a) + \cos(b) + \cos(c)) \geq 2(\sin(a) \sin(b) + \sin(b) \sin(c) + \sin(c) \sin(a)) \tag{2.1.6}$$

This is problem E 2029 [3, p. 1133], proposed by J. Garfunkel.

2.2. Prove that for every triangle ABC ,

$$p \leq 2R + (3\sqrt{3} - 4)r \tag{2.2.1}$$

where p, R, r are the semiperimeter, circumradius, and inradius, respectively. Equality holds only for the equilateral triangle.

This is problem E 1935 [1, p. 404], proposed by W. J. Blundon (it also appeared in [2], where it is stated that this is the strongest possible linear inequality in R, r, p).

First we reduce the problem to the appropriate form. On using the standard relations $r = 4R \sin(a/2) \sin(b/2) \sin(c/2)$ and $p = R(\sin(a) + \sin(b) + \sin(c))$ the problem is readily reduced to showing that in every triangle one has the inequality

$$f(a, b, c) = 2 + 4(3\sqrt{3} - 4) \sin\left(\frac{a}{2}\right) \sin\left(\frac{b}{2}\right) \sin\left(\frac{c}{2}\right) - \sin(a) - \sin(b) - \sin(c) \geq 0 \tag{2.2.2}$$

Again it is easy to see that the inequality

$$\begin{aligned} f_1 &= f(\pi - 2t, t, t) \\ &= 2 + 4(3\sqrt{3} - 4) \cos\left(\frac{t}{2}\right) \sin^2\left(\frac{t}{2}\right) - \sin(2t) - 2 \sin(t) \geq 0 \end{aligned}$$

is satisfied (compute the minimum of f_1 !), with equality either for the equilateral triangle or for the degenerate one with $a = 0, b = c = \pi/2$. For the other inequality we compute the difference $e = f(a, b, c) - f(a, (b+c)/2, (b+c)/2)$. We have

$$e = 2 \sin\left(\frac{b+c}{2}\right) - \sin b - \sin c + \alpha \sin\left(\frac{a}{2}\right) \left(\sin\left(\frac{b}{2}\right) \sin\left(\frac{c}{2}\right) - \sin^2\left(\frac{b+c}{2}\right) \right),$$

where $\alpha = 4(3\sqrt{3} - 4) > 0$. This time it is a bit trickier but after some simple trigonometric manipulations and use of the identities

$$\begin{aligned} 2 \sin \frac{b}{2} \sin \frac{c}{2} &= \cos \frac{b-c}{2} - \cos \frac{b+c}{2}, \\ 1 &= \sin \frac{a}{2} + 2 \sin^2 \frac{\pi-a}{4}, \\ \sin b + \sin c &= 2 \sin \frac{b+c}{2} \sin \frac{b-c}{2} \end{aligned}$$

we obtain

$$2e = \cos\left(\frac{b-c}{2}\right) \left(\alpha \sin\left(\frac{a}{2}\right) - 4 \cos\left(\frac{a}{2}\right)\right) - \alpha \sin^2\left(\frac{a}{2}\right) - 2\alpha \sin\left(\frac{a}{2}\right) \sin^2\left(\frac{\pi-a}{4}\right) + 4 \cos\left(\frac{a}{2}\right).$$

For $0 \leq a \leq \pi/3$ it is easy to see that the parenthesis multiplying $\cos((b-c)/2)$ is negative so that

$$2e \geq \left(\alpha \sin\left(\frac{a}{2}\right) - 4 \cos\left(\frac{a}{2}\right)\right) - \alpha \sin^2\left(\frac{a}{2}\right) - 2\alpha \sin\left(\frac{a}{2}\right) \sin^2\left(\frac{\pi-a}{4}\right) + 4 \cos\left(\frac{a}{2}\right) = 0!$$

Similarly one can show that the dual inequality

$$p \geq 3\sqrt{3}r \tag{2.2.3}$$

is valid in every triangle.

2.3. Given an acute triangle, let h_a, h_b, h_c denote, respectively, its altitudes, and let p denote its semiperimeter. Show that

$$\sqrt{3} \max\{h_a, h_b, h_c\} \geq p. \tag{2.3.1}$$

This is problem 10418 [4, p. 1013] proposed by the author.

This time we assume that the angles satisfy $a \geq b \geq c$. Then $\max\{h_a, h_b, h_c\} = h_c$. On using known relations ($S = pr$ and the law of sines, where S is the triangle's area and r is the radius of its inscribed circle) (2.3.1) can be transformed to the equivalent form

$$f(a, b, c) = 2\sqrt{3} \sin\left(\frac{a}{2}\right) \sin\left(\frac{b}{2}\right) - \cos\left(\frac{c}{2}\right) \geq 0 \quad \text{for } 0 \leq c \leq b \leq a \leq \frac{\pi}{2}. \tag{2.3.2}$$

Now consider the difference $e = f(a, b, c) - f(a, (b+c)/2, (b+c)/2)$. On using the relations

$$\sin x - \sin y = 2 \sin \frac{x-y}{2} \cos \frac{x+y}{2} \quad \text{and} \quad \cos x - \cos y = 2 \sin \frac{y-x}{2} \sin \frac{x+y}{2}$$

this readily simplifies to

$$e = 2 \sin\left(\frac{b-c}{8}\right) \left(2\sqrt{3} \sin\left(\frac{a}{2}\right) \cos\left(\frac{3b+c}{8}\right) - \sin\left(\frac{b+3c}{8}\right)\right).$$

Both factors here are positive because of the ordering taken in (2.3.2). Equality can hold only when $b = c$ (i.e., for an isosceles triangle). For the other inequality one can readily verify, on using that $b+c = \pi - a$, that

$$f\left(a, \frac{b+c}{2}, \frac{b+c}{2}\right) = 2\sqrt{3} \sin\left(\frac{a}{2}\right) \sin\left(\frac{\pi-a}{4}\right) - \cos\left(\frac{\pi-a}{4}\right) \geq 0 \tag{2.3.3}$$

for $\pi/3 \leq a \leq \pi/2$ with equality in (2.3.3) holding only for $a = \pi/3$. In fact by studying the function in (2.3.3) one can see that f vanishes also for $a \approx \pi/2 + 0.06208$. Therefore the inequality is valid for obtuse triangles to this small extent, as was shown already in one of the published proofs of MONTHLY Problem 10418 [5, p. 272].

There are many other inequalities along these lines that easily fit within the framework we have presented. We have given only some of the more interesting to illustrate our method.

ACKNOWLEDGEMENTS The author is indebted to Philip Maini for reading the manuscript and to the BBSRC/EPSRC Grant No 43-MMI 09782 for support.

REFERENCES

1. W. J. Blundon, Proposed problem E 1935, this MONTHLY 73 (1966) 1122.
2. W. J. Blundon, *Canad. Math. Bull.* 8 (1965) 615–626.
3. J. Garfunkel, Proposed problem E 2029, this MONTHLY 74 (1967) 1133.
4. R. A. Satnoianu, Proposed problem 10418, this MONTHLY 101 (1994) 1013.
5. Published solutions to problem 10418, this MONTHLY 105 (1998) 272.
6. T. Sekiguchi, Proposed problem E 3038, this MONTHLY 89 (1984) 140.

Mathematical Institute, Oxford University, 24-29 St Giles', Oxford OX1 3LB, UK
razvansa@maths.ox.ac.uk

A Theorem of D. J. Newman on Euler's ϕ Function and Arithmetic Progressions

J. M. Aldaz, A. Bravo, S. Gutiérrez, and A. Ubis

Euler's totient function $\phi(n)$ counts the number of elements in $\{1, \dots, n\}$ that are coprime with n . In a naive fashion, one might suspect, for example, that $\phi(210n) < \phi(6469693230n + 31)$ whenever $n \geq 1$, since the second argument is always distinctly larger than the first, the difference increases as n grows, and the inequality does hold for small values of n , say, for every $n \leq 10^{10\,000\,000}$ and far beyond. However, using Dirichlet's great theorem on arithmetic progressions, D. J. Newman has shown [1] that for infinitely many values of n the inequality is reversed: Whenever a, b, c, d , are nonnegative integers with $a, c > 0$ and $ad - bc \neq 0$, there exists an n (and hence infinitely many) such that $\phi(an + b) < \phi(cn + d)$.

In this note we modify Newman's argument to give a completely elementary proof that does not use the deep and difficult theorem of Dirichlet. As a bonus, when applied to concrete arithmetic sequences, this modification yields upper bounds that guarantee the reversal of the inequality, and also leads to a sharper statement: There exists a sequence $\{n_k\}$ of positive integers such that $\lim_k \phi(an_k + b)/\phi(cn_k + d) = 0$ if and only if $ad - bc \neq 0$. Note that $ad - bc \neq 0$ is equivalent to saying that the vectors (a, b) and (c, d) are linearly independent over \mathbb{Q} , or, since a and c are taken to be strictly positive, that there do not exist positive integers r and s such that $r(a, b) = s(c, d)$.

Theorem. Let a, b, c, d , be nonnegative integers with $a, c > 0$. If $ad - bc \neq 0$, then

$$\liminf_n \frac{\phi(an + b)}{\phi(cn + d)} = 0 \quad \text{and} \quad \limsup_n \frac{\phi(an + b)}{\phi(cn + d)} = \infty,$$

while if $ad - bc = 0$, then for every $n \geq 1$,

$$\frac{\phi(s)}{r} \leq \frac{\phi(an + b)}{\phi(cn + d)} \leq \frac{s}{\phi(r)},$$

where r and s are positive integers such that $r(a, b) = s(c, d)$.

In order to make this note as self-contained as possible, we prove everything that is not readily available in textbooks (and even some things that are). Our notation is standard: p always denotes a prime number; p_1, p_2, \dots is the list of primes in increasing order; and $\mathbb{Z}_a = \{[0], \dots, [a - 1]\}$ denotes the ring of integers modulo a . The ingredients we use in place of Dirichlet's theorem are elementary: (1) the formula $\phi(n) = n \prod_{p|n} (1 - p^{-1})$; and (2) $\prod_p (1 - p^{-1}) = 0$. This fact usually appears in the form $\prod_p (1 - p^{-1})^{-1} = \infty$ as a step in the proof of another theorem of Euler: $\sum_p p^{-1} = \infty$. To see why (2) holds, recall that for $|y| < 1$, $(1 - y)^{-1} = \sum_{k=0}^{\infty} y^k$. If $n \leq x$ then every prime appearing in the decomposition of n also satisfies $p \leq x$, so substituting p^{-1} for y gives

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leq x} \left(\sum_{k=0}^{\infty} \frac{1}{p^k}\right) \geq \sum_{n=1}^x \frac{1}{n} > \log x.$$

Also, from (1) and $\phi(n) \leq n$ we obtain $m\phi(n) \geq \phi(mn) \geq \phi(m)\phi(n)$ as follows:

$$\begin{aligned} m\phi(n) &= mn \prod_{p|n} \left(1 - \frac{1}{p}\right) \geq mn \prod_{p|mn} \left(1 - \frac{1}{p}\right) \\ &= \phi(mn) \geq m \prod_{p|m} \left(1 - \frac{1}{p}\right) n \prod_{p|n} \left(1 - \frac{1}{p}\right) = \phi(m)\phi(n), \end{aligned}$$

where the last inequality is actually an equality if $(m, n) = 1$, (i.e., ϕ is multiplicative).

Proof of the theorem. We prove the easier implication first. Let r and s be positive integers such that $r(a, b) = s(c, d)$. Then $r\phi(an + b) \geq \phi(r(an + b)) \geq \phi(r)\phi(an + b)$ and $s\phi(cn + d) \geq \phi(s(cn + d)) \geq \phi(s)(cn + d)$, so $s\phi(cn + d) \geq \phi(r)\phi(an + b)$ and $r\phi(an + b) \geq \phi(s)\phi(cn + d)$, whence

$$\frac{s}{\phi(r)} \geq \frac{\phi(an + b)}{\phi(cn + d)} \geq \frac{\phi(s)}{r}.$$

For the other implication, set $D := \prod_{\{p: p|a \text{ or } p|ad-bc\}} (a - p^{-1}) > 0$. This is a finite product by the assumption $ad - bc \neq 0$. We will produce a sequence $\{n_k\}$ of positive integers with $\lim_k n_k = \infty$, such that

$$\lim_k \frac{\phi(an_k + b)}{an_k + b} = 0 \quad \text{and} \quad \liminf_k \frac{\phi(cn_k + d)}{cn_k + d} \geq D.$$

Since

$$\lim_k \frac{an_k + b}{cn_k + d} = \frac{a}{c},$$

it follows that

$$\liminf_n \frac{\phi(an + b)}{\phi(cn + d)} = 0.$$

The result about the limit superior is obtained by interchanging the roles of (a, b) and (c, d) . Now $m_k := \prod_{\{p: p \leq p_k \text{ and } p \nmid a\}} p$ is coprime with a (that is, $[m_k]$ has a multiplicative inverse in \mathbb{Z}_a) so we can select A_k such that $A_k m_k = an_k + b$, where k_0 is chosen so that for every $k \geq k_0$, $n_k \geq 1$. This is always possible since $m_k \uparrow \infty$. Then

$$\lim_k \frac{\phi(an_k + b)}{an_k + b} = \lim_k \prod_{p|A_k m_k} \left(1 - \frac{1}{p}\right) \leq \lim_k \prod_{\{p: p \leq p_k \text{ and } p \nmid a\}} \left(1 - \frac{1}{p}\right) = 0.$$

Next, write $cn_k + d = \prod_{i=1}^{t_k} q_i^{\alpha_i}$, where $\alpha_i \geq 1$ and the q_i are primes in increasing order. Select F so that for $k \geq k_0$, $cn_k + d \leq F(an_k + b) = F A_k m_k \leq F a m_k$, and choose k large enough to satisfy $p_k > F a$. Then $\text{card}\{q_i : q_i > p_k\} \leq k + 1$, for else $cn_k + d \geq \prod_{q_i > p_k} q_i > p_k^{k+1} > F a m_k \geq cn_k + d$. Note also that if $p|m_k$ and $p|cn_k + d = (cA_k m_k + ad - bc)/a$, then $p|ad - bc$, so $\{q_i : q_i \leq p_k\} \subset \{p : p|a \text{ or } p|ad - bc\}$. Thus

$$\begin{aligned} \liminf_k \frac{\phi(cn_k + d)}{cn_k + d} &= \liminf_k \prod_{q_i \leq p_k} \left(1 - \frac{1}{q_i}\right) \prod_{q_i > p_k} \left(1 - \frac{1}{q_i}\right) \\ &\geq \lim_k D \left(\left(1 - \frac{1}{p_k}\right)^{p_k} \right)^{\frac{k+1}{p_k}} = D, \end{aligned}$$

since

$$\lim_k \frac{(k + 1)}{p_k} = 0. \quad \blacksquare$$

The fact that the set of primes has zero density (that is, $\lim_k (k + 1)/p_k = 0$) follows immediately from Chebyshev's easy estimate $\sum_{p \leq n} \log p \leq 4n$. In order to prove the theorem less is needed: It suffices to note that $k + 1 \leq p_k$, so replacing $k + 1$ with p_k in the exponent of $(1 - 1/p_k)^{k+1}$ yields the weaker lower bound D/e . But knowing that the limit inferior cannot be less than D tells more accurately where to look for reversals when studying concrete pairs of arithmetic sequences.

Let m be the greatest common divisor of c and d . Then

$$\frac{\phi(cn + d)}{cn + d} \leq \frac{\left(\frac{c}{m}n + \frac{d}{m}\right) \phi(m)}{\left(\frac{c}{m}n + \frac{d}{m}\right) m} = \frac{\phi(m)}{m},$$

so in order for $\phi(an + b) < \phi(cn + d)$ to hold it is necessary that

$$\frac{\phi(an + b)}{an + b} \frac{an + b}{cn + d} < \frac{\phi(m)}{m}.$$

Using this necessary condition it is easy to generate examples, such as the one given at the beginning of this note, where the first reversal of the inequality takes a really long time. On the other hand, one can search for the first time this condition is satisfied and look around using a computer, if one is interested in the smallest reversals. This method is followed in [2] to determine the least n such that $\phi(30n) > \phi(30n + 1)$. Applying the argument of the proof to $(a, b) = (30, 1)$ and $(c, d) = (30, 0)$ we generate an infinite number of examples without any need for computer work (though a calculator comes in handy).

We present some rather rough estimates, so the following examples are far away from being minimal. Clearly $(k + 1)/p_k \leq 2/3$ for $k \geq 5$, since about half the integers up to any $n \geq 11$ are even and there is only one even prime. Since $(1 - x^{-1})^x \uparrow 1/e$, for $x \geq 30$ we have $((1 - x^{-1})^x)^{2/3} \geq (29/30)^{20}$, so whenever $p_k \geq 30$, $\phi(A_k m_k - 1)/(A_k m_k - 1) > D(29/30)^{20}$, and hence $\phi(A_k m_k - 1)/A_k m_k > D/2 = 2/15$. On the other hand, for $x \in [p_k, p_{k+1})$, $D\phi(A_k m_k)/A_k m_k = \prod_{i=1}^k (1 - p_i^{-1}) < 1/\log x$, so choosing $x = \exp(225/8)$ and letting k_1 be the largest integer that satisfies $p_{k_1} \leq \exp(225/8)$, we have $\phi(30n_k) > \phi(30n_k + 1)$ for every $k \geq k_1$.

REFERENCES

1. D. J. Newman, Euler's ϕ function on arithmetic progressions, *Amer. Math. Monthly* **104** (1997) 256–257.
2. G. Martin, The smallest solution of $\phi(30n + 1) < \phi(30n)$ is . . . , *Amer. Math. Monthly* **106** (1999) 449–451.

Universidad de La Rioja, 26004 Logroño, La Rioja, Spain
 aldaz@dmc.unirioja.es
 ana.bravo@dmc.unirioja.es

A Counterexample for the Two-Dimensional Density Function

Liu Wen

In [1, p. 276] it was asserted that if a two-dimensional distribution function $F(x, y)$ has a continuous density $f(x, y)$, then

$$f(x, y) = \frac{\delta^2 F(x, y)}{\delta x \delta y}; \tag{1}$$

see also [2, p. 221]. Some intermediate text books in probability and statistics even assert that at a point of continuity for $f(x, y)$, $F(x, y)$ is twice differentiable, and 1 holds at that point; see [3, p. 206].

The purpose of this note is to point out that even continuity of the density cannot assure the existence of finite first-order partial derivatives of the distribution function. A counterexample is as follows.

Let $\varphi(y)$ be a positive, even, and continuous function on $(-\infty, \infty)$ such that $\varphi(y)$ is strictly decreasing on $(0, \infty)$ and

$$\int_{-\infty}^{\infty} \varphi(y) dy = 1. \tag{2}$$

Define

$$f(x, y) = \begin{cases} x/\varphi(y) + 1, & -\varphi(y) \leq x \leq 0; \\ -x/\varphi(y) + 1, & 0 \leq x \leq \varphi(y); \\ 0, & x < -\varphi(y) \text{ or } x > \varphi(y). \end{cases}$$

Then $f(x, y)$ is a continuous two-dimensional density function. Let $F(x, y)$ be the corresponding distribution function. We have for $0 < \Delta x < \varphi(0)$,

$$f(\Delta x, 0) - F(0, 0) \geq \int_0^{\varphi^{-1}(\Delta x)} \int_0^{\Delta x} f(x, y) dx dy \geq (\Delta x/2)\varphi^{-1}(\Delta x), \quad (3)$$

where φ^{-1} is the inverse function of $\varphi(y)$, and $0 \leq y < \infty$. It follows from (3) that

$$\lim_{\Delta x \rightarrow 0^+} \frac{F(\Delta x, 0) - F(0, 0)}{\Delta x} \geq \lim_{\Delta x \rightarrow 0^+} (1/2)\varphi^{-1}(\Delta x) = +\infty.$$

Hence $F(x, y)$ does not have a finite first-order partial derivative with respect to x at $(0, 0)$.

A similar argument shows that $\delta F(x, y)/\delta x$ does not exist at any point on the y -axis. However, it does exist for every point in the region of probability that is not on the y -axis. The y -axis is, of course, a set with zero probability.

REFERENCES

1. P. Billingsley, *Probability and Measure*, 2nd ed., Wiley, New York, 1986.
2. P. E. Pfeiffer and D. A. Schum, *Introduction to Applied Probability*, Academic Press, New York, 1973.
3. P. E. Pfeiffer, *Probability for Applications*, Springer, New York, 1990.

Hebei University of Technology, Tianjin 300130, China

The Remarkable Tetron

N. S. Astapov and N. C. Noland

Let D be the vertex of a trihedral angle having edges AD , BD , and CD (see Figure 1). Let the face angles at D be δ_1 in face ADB , δ_2 in face BDC , and δ in face ADC . From any point P on DB , let perpendiculars to BD be erected to meet AD at Q and DC at R . Then the dihedral angle at edge BD is $\angle QPR$, which we denote by \hat{BD} .

Let us begin with an easy proof of the following analog of the Law of cosines for the sides of the trihedral angle at the vertex D :

$$\cos \delta - \cos \delta_1 \cos \delta_2 = \sin \delta_1 \sin \delta_2 \cos \hat{BD}. \quad (1)$$

Let the lengths of the segments DQ , DP , DR , QR , PR , PQ , respectively, be x , y , z , p , q , r , as shown. From the right triangles PQD and PRD we have four of the values

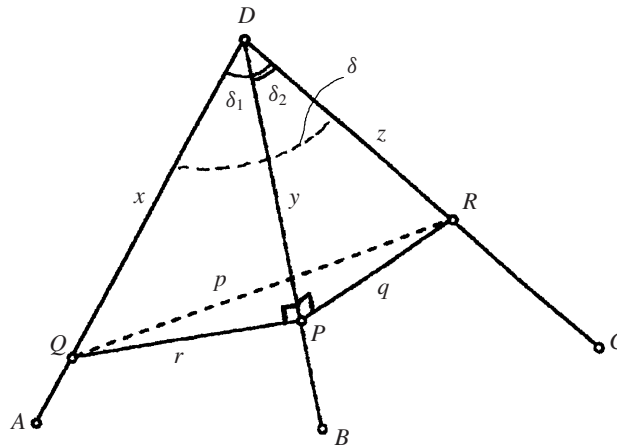


Figure 1.

involved, and applying the law of cosines to triangles QDR and PQR provides the remaining two values. Thus the claim is that

$$\frac{x^2 + z^2 - p^2}{2xz} - \frac{y}{x} \cdot \frac{y}{z} = \frac{r}{x} \cdot \frac{q}{z} \cdot \frac{q^2 + r^2 - p^2}{2qr},$$

which is immediately verified with the Pythagorean theorem and a brief simplification.

A *tetron* consists of four spatial points sequentially connected by segments. Segments that connect adjacent vertices of a tetron are called *sides*, and those connecting vertices that are not adjacent are *diagonals*.

We consider a tetron $ABCD$ to be defined by the listed order of its vertices A, B, C, D , where $a = AB, b = BC, c = CD, d = AD, m = AC, n = BD, \angle A = \angle BAD, \angle C = \angle BCD, \delta_1 = \angle ADB, \delta_2 = \angle BDC, \delta = \angle ADC$, and \hat{n} is the value of the dihedral angle by the edge n .

The tetron theorem. For any tetron,

$$m^2 n^2 = a^2 c^2 + b^2 d^2 - 2abcd(\cos \angle A \cos \angle C + \sin \angle A \sin \angle C \cos \hat{n}). \quad (2)$$

Proof. We have the following alternatives:

- 1) Some vertices coincide. This case is trivial.
- 2) All the vertices are distinct. Then (1) permits us to write

$$\cos \delta - \cos \delta_1 \cos \delta_2 = \sin \delta_1 \sin \delta_2 \cos \hat{n}. \quad (3)$$

Using the cosine rule for the left-hand side and the sine rule for the right-hand side of (3), we obtain

$$\frac{c^2 + d^2 - m^2}{2cd} - \frac{n^2 + d^2 - a^2}{2nd} \cdot \frac{n^2 + c^2 - b^2}{2nc} = \frac{ab}{n^2} \sin \angle A \sin \angle C \cos \hat{n}$$

or

$$\begin{aligned} a^2 c^2 + b^2 d^2 - 2m^2 n^2 + n^2(a^2 + b^2 + c^2 + d^2 - n^2) - a^2 b^2 - c^2 d^2 \\ = 4abcd \sin \angle A \sin \angle C \cos \hat{n}. \end{aligned} \quad (4)$$

Since $n^2 = a^2 + d^2 - 2ad \cos \angle A = b^2 + c^2 - 2bc \cos \angle C$, $n^2(a^2 + b^2 + c^2 + d^2 - n^2) = a^2b^2 + c^2d^2 + a^2c^2 + b^2d^2 - 4abcd \cos \angle A \cos \angle C$. Substituting this expression into (4), we obtain (2). ■

Corollary 1. *(The inverse Ptolemy theorem). If the lengths of the sides and diagonals of a tetron satisfy $mn = ac + bd$, then either all vertices lie on a straight line or the tetron is a convex quadrilateral inscribed in a circle.*

Proof. The assertion is trivial if one of the sides has zero length. Subtracting (2) from the identity $(mn)^2 = (ac + bd)^2$ gives

$$2abcd(1 + \cos \angle A \cos \angle C + \sin \angle A \sin \angle C \cos \hat{n}) = 0,$$

or

$$1 + \cos(\angle A + \angle C) = -\sin \angle A \sin \angle C(1 + \cos \hat{n}). \tag{5}$$

The left-hand side of (5) is nonnegative and the right-hand side is nonpositive, because $\sin \angle A \geq 0$ and $\sin \angle C \geq 0$. Hence, $\angle A + \angle C = \pi$. If $\sin \angle A = 0$ or $\sin \angle C = 0$, then all the vertices lie on a straight line. If $\cos \hat{n} = -1$, then all the vertices lie in one plane, and the vertices A and C lie on different sides of the straight line BD . Considering the equality $\angle A + \angle C = \pi$, we conclude that $ABCD$ is a convex cyclic quadrilateral. ■

Corollary 2. *For any tetron,*

$$\begin{aligned} a^2c^2 + b^2d^2 - 2abcd \cos(\angle A - \angle C) &\leq m^2n^2 \\ &\leq a^2c^2 + b^2d^2 - 2abcd \cos(\angle A + \angle C). \end{aligned}$$

Corollary 3. *A tetron is planar if and only if either of the following two equalities holds:*

- (a) $m^2n^2 = a^2c^2 + b^2d^2 - 2abcd \cos(\angle A + \angle C)$, or
- (b) $m^2n^2 = a^2c^2 + b^2d^2 - 2abcd \cos(\angle A - \angle C)$.

In case (a) the points A and C lie on different sides of the line BD ($\hat{n} = \pi$) or both points lie on BD , and in case (b) the points A and C lie on one side of the straight line BD ($\hat{n} = 0$) or both points lie on BD .

Corollary 4. *(The Ptolemy inequality). For any tetron, $|ac - bd| \leq mn \leq ac + bd$, equality being attained if and only if all vertices lie on a straight line or on a circle.*

Therefore, out of segments ac , bd , and mn , one can construct a triangle where the angle φ lying opposite the mn side is calculated, owing to (1), by the formula $\cos \varphi = \cos \angle A \cos \angle C + \sin \angle A \sin \angle C \cos \hat{n}$.

The tetron theorem makes possible a uniform approach to some questions concerning triangles, quadrilaterals, and 3-sided pyramids. Due to this theorem seemingly dissimilar facts (the Ptolemy theorem, the formula for the area of an arbitrary nonreflexive quadrilateral, etc.) can be proved uniformly.

*Novosibirsk State University, Novosibirsk, Russia
nika@hydro.nsc.ru*