Published by Oxford University Press on behalf of The British Computer Society. All rights reserved.
For Permissions, please email: journals.permissions@oxfordjournals.org
Advance Access published on August 11, 2005 doi:10.1093/comjnl/bxh124

Kolmogorov Lecture

This annual University of London lecture celebrates the life and work of Andrei Nikolaevich Kolmogorov, one of the greatest mathematical and scientific minds of the last century. The lecture addresses current issues arising from the impact of Kolmogorov's work in the fields of mathematical and computer sciences.

Each Kolmogorov Lecture is given by one of the leading figures in their field, who is presented with a medal in recognition of their own contribution to science. The speaker at the Second Annual Kolmogorov Lecture, held on February 24, 2004, was Professor Leonid Levin of Boston University. He presented a lecture entitled 'Randomness and Non-determinism':

> In the decades since fundamental questions like P = ?NP have been raised, we have not come much closer to answering them. Yet, we did learn one obscure but essential hint: a strange pattern of relationships between non-determinism and randomness—another major deviation from deterministic computations.
>
> I will give illustrations of these ideas: some simple, some powerful and ingenious to which many authors contributed. One example, foreshadowed by Andrei Kolmogorov, is the fundamental relationship between computer-generated randomness and hard non-deterministic problems (one-way functions). A converse example is a Monte Carlo method for instant verification of proofs of any theorems or computations—a quite general nondeterministic task.

Professor Levin, one of the world's foremost researchers in the field of Kolmogorov Complexity, works in the field of mathematical probability and the theory of computation, particularly with respect to randomness and complexity in computing. First introduced to Kolmogorov at the age of 15 during a school visit, he was later taught by Kolmogorov at Moscow University and was advised by him for his doctoral thesis. Professor Levin went on to become one of the originators of the theory of NP completeness (alongside S. A. Cook and R. Karp). In 2004 he was awarded an Outstanding Paper award by the Society of Industrial and Applied Mathematics for his work on Pseudorandom generators from one-way functions.

Randomness was a major topic of the Kolmogorov Lecture as well as a great passion of Kolmogorov himself. One of the remarkable effects of randomness is breaking the symmetries inherent in many natural and artificial phenomena. The following article supplements the Lecture with a look at some other (non-deterministic) mechanisms of symmetry breaking.

Professor Levin awarded the Kolmogorov Medal (From left) Professor Norman Gowar, Professor Leonid Levin and Professor Alex Gammerman.

Aperiodic Tilings: Breaking Translational Symmetry

LEONID A. LEVIN

Boston University, Department of Computer Science, 111 Cummington Street, Boston, MA 02215, USA

Classical results on aperiodic tilings are rather complicated and not widely understood. In the present article, an alternative approach to these results is discussed in the hope of providing additional intuition, not apparent in classical works.

Received 29 September 2004; revised 10 June 2005

1. PALETTES AND TILINGS

Physical computing media are asymmetric. Their symmetry is broken by irregularities, physical boundaries, external connections and so on. Such peculiarities, however, are highly variable and extraneous to the fundamental nature of the media. Thus, they are pruned from theoretical models, such as cellular automata, and reliance on them is frowned upon in programming practice.

However, computation, like many other highly organized activities, is incompatible with perfect symmetry. Some standard mechanisms must assure breaking the symmetry inherent in idealized computing models. A famous example of such mechanisms is aperiodic tiling: hierarchical self-similar constructions, first used for computational purposes in a classical—although rather complicated—work [1]. They were further developed in [2, 3, 4]; [5] gives a helpful exposition.

DEFINITION 1. *Let G be the grid of unit length edges between integer points on an infinite plane. A* **tiling** *T is its mapping into a finite set of* **colors***. Its* **crosses** *and* **tiles** *are ordered color combinations of four edges sharing a corner or forming a square, respectively. A* **palette** *P of T is a set including all its tiles (+***palette** *for crosses). We say P with a mapping f of its colors into a smaller color alphabet* **enforces** *a set S of tilings if replacing colors according to f turns each P-tiling into a tiling in S.*

Turning each edge orthogonally around its center turns G into its dual graph and palettes into +palettes and vice versa. Thus, one can use either type as convenient.

2. 2-ADIC COORDINATES

The set of all tilings with a given palette P has translational symmetry, i.e. any shift produces another P-tiling. We want a palette that forces a complete spontaneous breaking of this symmetry, i.e. prevents individual tilings from being *periodic*. Accordingly, each location in a given tiling will be uniquely characterized by a sort of *coordinates*. Their infinitely many values cannot be reflected in the finite variety of the tile's colors. They will be represented *distributively*, i.e. in the colors of the surrounding tiles, and computable from them to any given number of digits.

Let us first so distribute the horizontal Cartesian integer coordinates $x = (2i + 1)2^k$ of vertical edges by reflecting one bit (i mod 2) in their color. We view this bit as the direction of a ***bracket***. In this tiling C_1, the brackets of the same ***rank*** k are equidistant (Figure 1).

It is convenient to visualize the bits of even rank, picturing them }, { or red, or dotted, separately from odd, depicted] , [. The bits of either shape at each side of the origin form a progression of balanced parenthetical expressions, called ***domains***. Each domain has four ***grandchildren*** of the second lower rank: two within its outermost brackets and one to each side. The two ***children*** have the other shape and are centered at each border of the ***parent***, thus connecting it with its grandchildren.

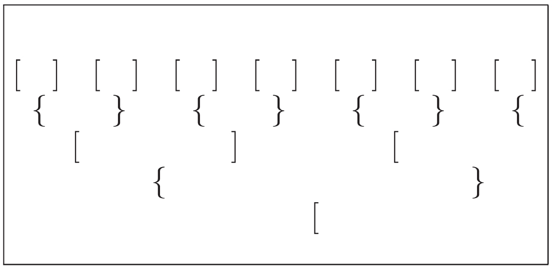

FIGURE 1. Brackets of C_1 split by rank.

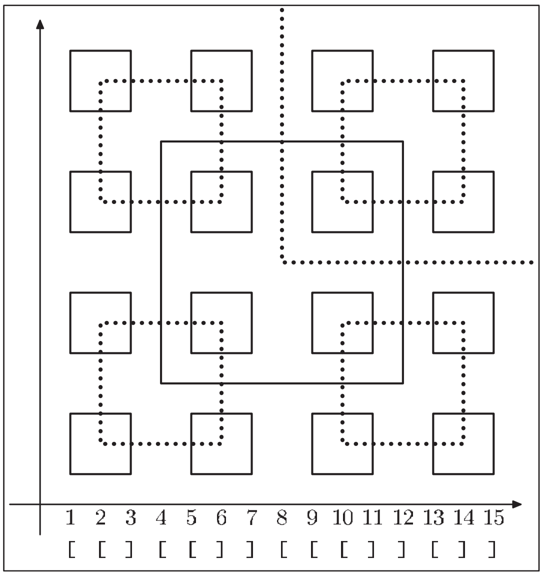

FIGURE 2. Boldness bit lines in C. A colour version of this figure is available as Supplementary Data on the journal's website at www.comjnl.oxfordjournals.org.

Handling the vertical coordinate similarly yields a neat 2D tiling C called ***central***. Figure 2[1] marks the borders of intersections of its vertical and horizontal domains of equal ranks with a ***boldness*** bit.

C_1 has a special, i.e. unmatched, bracket in the origin, directed arbitrarily and unranked. No palette can enforce a set of tilings with unique special points (designated by a Borel function commuting with shifts) since the set of all tilings is compact,[2] whereas the set of locations of their special point and the group $\mathbb{Z}$ of their shifts is not. We will extend $\mathbb{Z}$ to a compact group and also ***define ranks*** in other tilings, e.g. shifted C_1, using the following property.

REMARK 1. *A shift by $(2i+1)2^k$ in C_1 reverses all brackets of rank $k-1$, none of lower ranks and every second bracket of any rank $> k$.*

Therefore, the shifts by $(2i + 1)2^k$ change our bits only at a $2/2^k$ fraction of locations. This fraction can be used as a

[1] Courtesy of A. Shen and B. Durand.

[2] and so has finite shift-invariant measures, e.g. defined by condensation points of frequencies of finite configurations in some quasiperiodic tiling.

metric on the group of shifts which can then be completed for it. The result is a remarkable compact group g of 2-adic integers, or ***2-adics***, acting on a similarly completed set of 2-adic coordinates. A 2-adic a is a formal infinite sum $\sum_{i\geq 0} 2^i a_i = \cdots + 4a_2 + 2a_1 + a_0$, where $a_i \in \{0,1\}$, viewed as an infinite to the left sequence of bits. The usual algorithms for addition and multiplication make g a ring with $\mathbb{Z}$ as a subring (e.g. $-1 = \cdots + 8 + 4 + 2 + 1$).[3]

The natural action of $\mathbb{Z}$ (by shifts) can be extended to the action of the whole g on C_1 and its images.

Indeed, the brackets of rank k are unaffected by terms a_i with $i > k+1$. Thus, a 2-adic shift a of C_1 can be defined as the pointwise limit of the sequence of shifts by integers approximating a. With inverse shifts, this sequence diverges for the unranked bracket in the origin of C_1 and of its integer shifts. The direction of this bracket is determined not by its location, but by an arbitrary ***default*** included as an additional (external, unmoved by shifts) point in the tilings. The ***reflection*** reverses the default, all brackets, and the signs of their locations. With added reflection, the action of g is free and transitive: each of these tilings can be obtained from any other, e.g. from C_1.

In two dimensions we can also add the diagonal reflection exchanging the vertical and horizontal coordinates.[4]

3. ENFORCING THE COORDINATE SYSTEM WITH A PALETTE

THEOREM 1. *The set of 2-adic shifts and reflections of tiling C can be enforced by a palette.*

To prove it, we use multicomponent colors in T which are projected by f onto their first component—bracket bit. The second component includes two ***enforcement*** bits that extend C to the enhanced tiling CE, with a +palette ce of seven crosses modulo eight reflections.[5] One of its bits is the already described boldness bit (Figure 2). The other is a ***pointer*** in the direction of the nearest orthogonal line of the same rank. On the (unranked) axes these bits are set by a default central cross.

DEFINITION 2. *A* **box** *is an* **open** *ce-tiled rectangle, i.e. one with the border edges removed. Its k-***block** *is a square with monochromatic sides that is*[6] *a tile (for $k = 0$) or a combination of four $(k-1)$-blocks sharing a corner. The four segments connecting the block's center to its sides are called $(k-1)$-***medians***. The rest of the open block is called a* **frame**. *We call a box k-***tiled** *if removing an outer layer which is thinner than a k-block turns it into a box composed of (open at the box border) k-blocks.*[7]

LEMMA 1. *(i) Borders between open blocks in a box are monochromatic. (ii) All k-frame patterns in a box are enclosed in its open k-blocks. (iii) All open k-blocks are congruent and have equal frames.*

Proof. (i) comes from all ce-crosses having one or four inward pointers. (ii,iii) for $k > 2$ follow from $k-1$ by viewing 1-blocks as tiles. Let 1-blocks a and b be adjacent in a 2-block c; (L, l) and (R, r) be pairs of medians of a and b with l, r directed to the side s of c, $L-R$ crossing a median m of c at a cross x. x forces L, R to be both pale or both bold. This forces opposite brackets on l, r which, too, must be both pale or both bold depending on the bracket of $L-R$. l, r cannot be both bold which would require the pointer of s to agree with their opposite brackets.

Thus, all external medians of 2-frames are pale, internal medians bold, their brackets face the frame's center forcing inward pointers on the 1-medians, like m. □

LEMMA 2. *Any 1-tiled box is k-tiled. (Follows from $k = 2$ case by viewing $(k-2)$-blocks as tiles.)*

Proof. The eight colors of edges fix their location in 2-frames, forcing open 1-blocks to alternate in the pattern of 2-frames which, by Lemma 1, extend to 2-blocks. □

COROLLARY 1. *Any $2^k \times 2^k$ box, extendible to a three times wider cocentric 1-tiled box, extends to a $(k+4)$-block.*

Induction basis. For the simplest enforcement of tiling decomposition into 1-blocks we can use a 2-periodic ***parity*** bit to mark ***odd*** lines carrying 0-medians. All pointers on odd lines point to odd crossing lines, thus forcing a period 2 on them. One needs only to assure an odd line exists. This can be easily done with a ***parity pointer*** on even lines, pointing to a crossing odd line.

Proof of Corollary. The box is k-tiled covering the inner box with four blocks sharing a cross. The extension comes by viewing them as tiles with parity bit reflecting the blocks' orientation and noting that each cross of C with parity appears in its open 4-blocks. □

Proof of Theorem 1. Let T be a ce-tiling decomposed, for each k, into k-blocks with equal frames. Then a shift of CE matches T on all lines of rank $< k$. The shifted CE converge pointwise to T, except possibly on their (unranked) axes. By Remark 1, the shift increments grow in rank, and so sum to one 2-adic shift. Finally, reflections match the brackets on axes. □

3.1. Parsimonious enforcement of the grid of 1-blocks

First, we reduce the needed parity colors. A parity pointer on a single edge suffices, so it needs to accompany only one color if we show that ce-tilings cannot skip colors. Indeed, all ce-crosses are either ***bends***, i.e. have four inward pointers, or ***passes***, i.e. have one. Thus, a third of crosses are bends, up to $O(n)$ accuracy for $n \times n$ boxes. Moreover, all orientations of bends are equally frequent, alternating on each line. □

[3] Odd 2-adics have inverses. This allows extending g to a famous locally compact field with fractions $a/2^i$.

[4] We allow fewer tilings than [5] which permits different shifts at each side of the origin.

[5] [2] uses only six tiles (with reflections) but colors their corners, in addition to sides.

[6] The rest of the requirement is redundant but useful in the proof.

[7] ce prevents crossing of monochromatic segments, making decompositions of boxes into blocks unique.

Tedious case investigation of [6] shows *ce* bits themselves forcing 1-blocks, rendering parity bits redundant. A *k-**bar*** is a maximal bold or pale segment, k being its length. $k > 1$ and no bold 3-bar exists since it is easy to see that its middle link would be connected by a tile to a 1-bar. Levitsky first proves that each *ce*-tiling has bold 2-bars. Here is a simpler argument for this.

The average bar length is 3 since a third of crosses are bends. Absent bold 2-bars, this average would allow positive density only of bold 4-bars and pale 2-bars. Tilings with such bars have period 6 and map onto a 6×6 torus with three bold 4×4 squares. But $\mathbb{Z}_6$ cannot have three disjoint pairs of points of equal parity! □

The rest of [6] analysis assures bold 2-bars two tiles away at each side of any bold 2-bar. This involves a case-by-case demonstration that no violation can be centered in a 10×10 box. The analysis is laborious but may be verifiable by a computer check.

ACKNOWLEDGEMENTS

These remarks were developed in my attempts to understand the classical constructions of aperiodic tilings while working on [7]. My main source of information was [5] and its explanations by B. Durand and A. Shen to whom I owe all my knowledge on this topic. This research was supported by NSF grant CCR-0311411.

REFERENCES

[1] Berger, R. (1966) The undecidability of the domino problem. *Mem. Amer. Math. Soc.*, **66**, 1–72.

[2] Robinson, R. M. (1971) Undecidability and nonperiodicity of tilings of the plane. *Inventiones Mathematicae*, **12**, 177–209.

[3] Myers, D. (1974) Nonrecursive tilings of the plane. ii. *J. Symbolic Logic*, **39**(2), 286–294.

[4] Gurevich, Yu. and Koriakov, I. (1972) A remark on Berger's paper on the domino problem. *Siberian Math. J.*, **13**, 459–463.

[5] Allauzen, C. and Durand, B. (1996) Appendix A: tiling problems. pp. 407–420. In Boerger, E., Graedel, E. and Gurevich, Y. (eds), *The Classical Decision Problem*. Springer-Verlag.

[6] Alexander Levitsky (2004) Aperiodicheskie zamoshcheniya s malym alfavitom (Aperiodic Tilings with small alphabet). In Russian. Master Thesis. Moscow State University.

[7] Durand, B., Levin, L. A. and Shen, A. (2001) Complex tilings. In *Proc. 33rd Annual ACM Symp. on Theory of Computing*, Heraklion, Crete, Greece. July 6–8, pp. 732–739. ACM.

[8] Gacs, P. (2001) Reliable cellular automata with self-organization. *J. Stat. Phys.*, **103**(1,2), 45–267. Available at http://www.arxiv.org/abs/math.PR/0003117 .