Nonexistence of 2-reptile simplices

Jiří Matoušek

Department of Applied Mathematics and
Institute of Theoretical Computer Science (ITI)
Charles University
Malostranské nám. 25, 118 00 Praha 1 Czech Republic

Abstract. A simplex S is called an *m-reptile* if it can be tiled without overlaps by simplices $S_1, S_2, \ldots, S_m$ that are all congruent and similar to S. The only m-reptile d-simplices that seem to be known for $d \geq 3$ have $m = k^d$, $k \geq 2$. We prove, using eigenvalues, that there are no 2-reptile simplices of dimensions $d \geq 3$. This investigation has been motivated by a probabilistic packet marking problem in theoretical computer science, introduced by Adler in 2002.

1 Introduction

A closed set $A \subset \mathbf{R}^d$ with nonempty interior is called an *m-reptile* (sometimes written "m rep tile" or "m rep-tile") if there are sets $A_1, A_2, \ldots, A_m$ with disjoint interiors and with $A = A_1 \cup A_2 \cup \cdots \cup A_m$ that are all congruent and similar to A. Such sets have been studied in connection with fractals and also with crystallography and tilings of $\mathbf{R}^d$; see, for example, [4], [14], [9], [8], [12]. The connection with tilings stems mainly from the simple observation that any m-reptile, $m \geq 2$, tiles $\mathbf{R}^d$.

Here we consider the following question: For what m and d there exist d-dimensional *simplices* that are m-reptiles? This investigation was motivated by a paper of Adler [1] on probabilistic marking of Internet packets. We will briefly discuss this connection and the quite interesting questions arising there in Section 3 (see [2] for more details). From this point of view, it would be interesting to find d-dimensional m-reptile simplices with m as small as possible.

In the plane, there are several types of m-reptile triangles. The following list exhausts all possible cases [14] (see Fig. 1):

(a) Any triangle is a k^2-reptile for all $k = 2, 3, \ldots$.
(b) A right triangle with acute angles $\frac{\pi}{6}$ and $\frac{\pi}{3}$ is a $3k^2$-reptile for all $k = 1, 2, \ldots$.
(c) A right triangle whose two shorter sides have ratio $k : \ell$ is a $(k^2 + \ell^2)$-reptile, $k, \ell = 1, 2, \ldots$.

Higher-dimensional simplex reptiles seem to be much more rare. At a first encounter with the problem it is tempting to think that the dissection of an equilateral triangle, say, into four equilateral triangles (a special case of (a) above) can be generalized to a dissection of a regular tetrahedron, but once one cuts off the corners of the tetrahedron, one obtains a regular octahedron, which cannot be tiled by regular simplices. The only known construction, at least as far as I could find, of higher-dimensional simplex m-reptiles has $m = k^d$ and is known as the *Hill simplex* (or *Hadwiger-Hill simplex*). A d-dimensional Hill simplex is the convex hull of vectors 0, b_1, $b_1 + b_2$,…,$b_1 + \cdots + b_d$, where $b_1, b_2, \ldots, b_d$ are vectors of equal length such that the angle between any two of them is the same and lies in the interval $(0, \frac{2\pi}{3})$. Fig. 2 shows the decomposition of a 3-dimensional Hill simplex, with $(b_1, b_2, b_3) = (e_1, e_2, e_3)$ the standard orthonormal basis, into 8 congruent pieces similar to it.

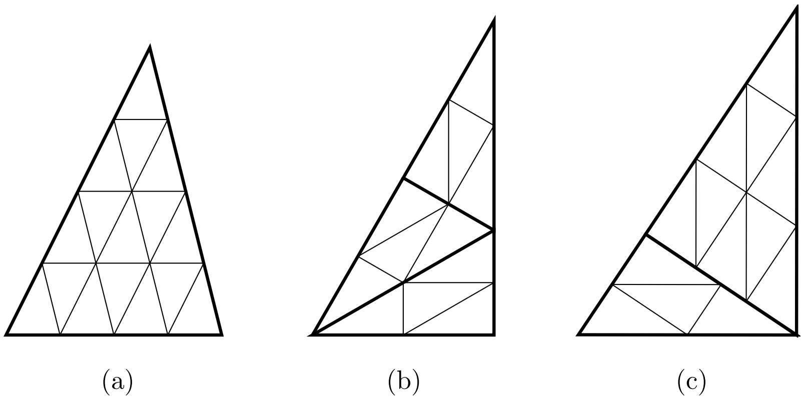

Fig. 1. Planar reptile triangles

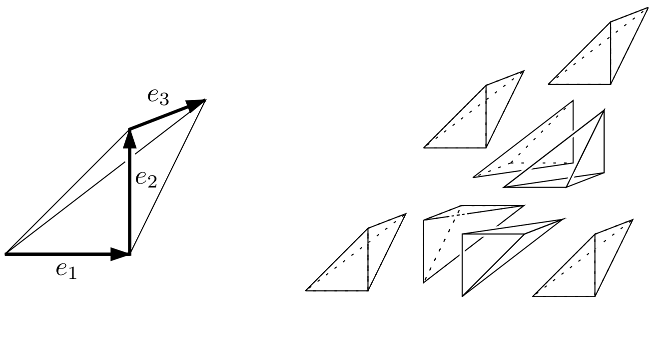

Fig. 2. A 3-dimensional Hill simplex as an 8-reptile

In the absence of constructions of m-reptile simplices with $m < 2^d$ one can try to prove nonexistence results, but the general problem seems quite challenging. The only known result on this question I could find is by Hertel [10], who proves that a 3-dimensional simplex is a k^3-reptile using a "standard" way of dissection if and only if it is a Hill simplex. He conjectures that Hill simplices are the only 3-dimensional reptile simplices. Simplex dissection was considered in several other papers (e.g., [6], [15], [3]) but from different points of view.

In this note we establish the following partial result:

Theorem 1. *For $d \geq 3$ no d-dimensional simplex is a 2-reptile.*

It is easy to see that there is just one way of dissecting a a simplex into two simplices. So supposing that a 2-reptile simplex exists, one can quickly derive a lot of information about the volume of its facets, the edge lengths, and the dihedral angles (Coxeter diagram). It is possible that a simple proof of Theorem 1 can be obtained using this information, but at least it didn't look obvious.

The proof presented here is based on eigenvalues of the linear transformations associated with the similarity maps that send the simplex onto the two tiles. This approach arose naturally while considering a problem associated with the probabilistic packet marking; that problem is more general than the existence of m-reptile simplices and geometric quantities such as facet volume or edge length cannot be directly used in it. Perhaps this approach could be of some interest in tiling problems.

2 Proof of Theorem 1

We proceed by contradiction, assuming that S is a d-dimensional 2-reptile simplex. Let $v_1, v_2, \ldots, v_{d+1} \in \mathbf{R}^d$ be the vertices of S. Let S_1 and S_2 be the two tiles; that is, $S = S_1 \cup S_2$, where S_1 and S_2 are congruent, similar to S, and have disjoint interiors. Here is the observation mentioned in the introduction:

Lemma 1. *The numbering of the vertices of S can be chosen in such a way that S_1 has the vertex set $v_1, v_2, \ldots, v_d, w$, where $w = \frac{1}{2}(v_d + v_{d+1})$, and S_2 has the vertex set $v_1, v_2, \ldots, v_{d-1}, v_{d+1}, w$; see Fig. 3.*

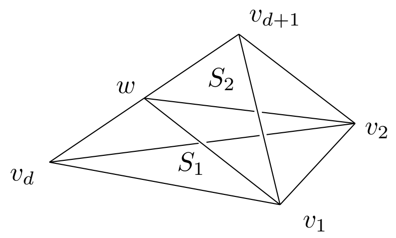

Fig. 3. The dissection of S into S_1 and S_2.

Proof. The interiors of S_1 and of S_2 are disjoint convex sets, and so they can be separated by a hyperplane h. Let V^0, V^+, V^- be the subsets of vertices of S lying on h, on one side of h, and on the other side of h, respectively. Each edge of S connecting a vertex from V^+ to a vertex from V^- gives rise to a vertex of both S_1 and S_2. Hence $|V^+|+|V^0|+|V^+|\cdot|V^-| = d+1$ and $|V^-|+|V^0|+|V^+|\cdot|V^-| = d+1$, and we get $|V^+| = |V^-| = 1$, $|V^0| = d-1$. Hence h contains $d-1$ vertices of S and it has to bisect the edge connecting the two remaining vertices so that S_1 and S_2 have the same volume. $\square$

From now on, we assume that the vertex sets of S_1 and of S_2 are as in the lemma. Let f_k be the similarity map sending S to S_k, $k = 1, 2$. That is, f_k is an isometry followed by scaling in the ratio $\alpha = 2^{-1/d}$ (since the volume of S_k is half of the volume of S).

Let us write $v'_i = v_i$ for $i = 1, 2, \ldots, d$ and $v'_{d+1} = w$, and let π_1 be the permutation of $\{1, 2, \ldots, d+1\}$ defined by $f_1(v_i) = v'_{\pi_1(i)}$, $i = 1, 2, \ldots, d+1$.

Lemma 2. *The permutation π_1 either has a single cycle (of length $d+1$), or it has d as a single fixed point and $1, 2, \ldots, d-1$, and $d+1$ form a single cycle of length d.*

Proof. Let us suppose that π_1 has at least two cycles, and let U be the union of all cycles that do not contain $d+1$. Then the face F of S spanned by the vertices v_i, $i \in U$, is fixed (setwise) by f_1. Since the diameter of the image of S under the iterated mapping $f_1 \circ f_1 \circ \cdots \circ f_1$ (t-fold composition) tends to 0 as $t \to \infty$, F has to be 0-dimensional, and hence $|U| = 1$. So either π_1 is unicyclic or it has one fixed point, different from $d+1$, and one cycle of length d.

Let j be the fixed point of π_1 and let F_j be the facet of S not containing v_j. If $j \neq d$, then $f_1(F) \subset F$, and again the diameter of the image of S under iterations of f_1 would not shrink to 0. Hence $j = d$ as claimed. $\square$

We define the permutation π_2 analogously using f_2. That is, we set $v''_i = v_i$ for $i \in \{1, 2, \ldots, d-1, d+1\}$ and $v''_d = w$, and we define π_2 by $f_2(v_i) = v''_{\pi_2(i)}$. The analogy of Lemma 2 holds for π_2; i.e., π_2 either is unicyclic or has a fixed point $d+1$ and a cycle of length d.

Let us write $f_k(x) = A_k x + b_k$, $k = 1, 2$, for $d \times d$ matrices A_1 and A_2. Since f_k is an isometry followed by scaling by α, A_k is an orthogonal matrix multiplied by α, and hence all of its eigenvalues have absolute value α. More generally, for any sequence $(k_1, k_2, \ldots, k_{2t})$ of integers, the product matrix $A_1^{k_1} A_2^{k_2} \cdots A_2^{k_{2t}}$ must have all eigenvalues with absolute value $\alpha^{k_1+k_2+\cdots+k_{2t}}$, since the corresponding composed map is a similarity map with the appropriate ratio. We will show that these conditions cannot hold.

The eigenvalues of matrices are preserved under similarity (of matrices, i.e. TAT^{-1} is similar to A; this should not be confused with similarity maps considered elsewhere in this paper). Hence we can choose a basis of $\mathbf{R}^d$ as convenient: we will assume that $v_{d+1} = 0$ (which can be achieved by translation of S) and we will use the basis $(v_1, v_2, \ldots, v_d)$. Expressing f_1 and f_2 with respect to this basis, we obtain explicit and simple matrices $\bar{A}_1$ and $\bar{A}_2$, depending only on the permutations π_1 and π_2, which have to satisfy the eigenvalue condition formulated above for A_1 and A_2. We will now compute the characteristic polynomials. The possibility of unicyclic π_1 can be excluded based on the eigenvalues of $\bar{A}_1$ alone, while for π_1 with a single fixed point we will use the product $\bar{A}_2^{-1}\bar{A}_1$ as well.

The unicyclic case. Here we assume that π_1 has a single cycle. We note that while the vertices v_d and v_{d+1} are distinguished (by the split edge), the roles of the others are completely symmetric, and so the only thing that matters is number k of elements between d and $d+1$ in the single cycle of π_1, $0 \le k \le d-1$. Let us fix the numbering of v_1 through v_{d-1} so that π_1 looks as in Fig. 4. The ith column of $\bar{A}_1$ is $f_1(v_i) - f_1(v_{d+1}) = v'_{\pi_1(i)} - v'_{\pi_1(d+1)}$ expressed in the basis $(v_1, \ldots, v_d)$. Here the coordinate vector of v'_i with respect to this basis is e_i (the standard basis vector) for $1 \le i \le d$ and it is $\frac{1}{2}e_d$ for $i = d$ (we have $v'_{d+1} = w = \frac{1}{2}(v_d + v_{d+1}) = \frac{1}{2}v_d$).

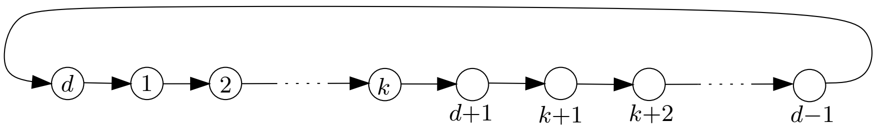

Fig. 4. The permutation π_1 in the unicyclic case

The matrices $\bar{A}_1$ look as follows (they are shown for $d = 5$ and $k = 0, 1, 2$ and 4):

$$\begin{pmatrix} -1 & -1 & -1 & -1 & -1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & \frac{1}{2} \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 & -1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & \frac{1}{2} & 0 & 1 & 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ -1 & -1 & -1 & \frac{1}{2} & -1 \end{pmatrix}.$$

The characteristic polynomial, easily calculated, is

$$\begin{aligned} p_k(x) &= -\left(x^d + x^{d-1} + \cdots + x^{d-k+1} + \frac{x^{d-k}}{2} + \frac{x^{d-k-1}}{2} + \cdots + \frac{1}{2}\right) \\ &= \frac{2x^{d+1} - x^{d-k} - 1}{2(1-x)}. \end{aligned}$$

Lemma 3. *For $d \geq 3$ and for every $k = 0, 1, \ldots, d-1$, there is at least one root of $p_k(x)$ with absolute value different from $\alpha = 2^{-1/d}$.*

We postpone the proof to the end of this section. This verifies that the case of a unicyclic permutation yields no 2-reptile simplices.

The case of a single fixed point. Here $\pi_1(d) = d$ and the remaining points form a single cycle. Since $v_1, v_2, \ldots, v_{d-1}$ are completely symmetric, we can choose the notation so that $\pi_1(1) = 2$, $\pi_1(2) = 3, \ldots$, $\pi_1(d-2) = d-1$, $\pi_1(d-1) = d+1$, and $\pi_1(d+1) = 1$. The characteristic polynomial of the matrix $\bar{A}_1$ turns out to be $x^d - \frac{1}{2}$, and it does have all roots with absolute value α. This means, as is easy to check, that one can indeed choose the vertices $v_1, \ldots, v_{d+1}$ so that the mapping f_1 determined by π_1 as above is a similarity with ratio α. We thus have to consider both f_1 and f_2 simultaneously.

Since we have excluded the unicyclic case, π_2 also has to consist of one cycle of length d and a single fixed point, which in this case is $d+1$ (v_{d+1} plays the same role in S_2 as v_d does in S_1). However, if we consider π_1 and π_2 simultaneously, we can no longer choose the numbering of the vertices along the cycle of π_2, as we did for π_1.

In order to determine the possibilities for π_2, we will consider the volumes of the facets of S, S_1, S_2. Let F_i be the facet of S that does not contain v_i, let V_i be its $(d-1)$-dimensional volume, let F_i' be the facet of S_1 not containing v_i', of volume V_i', and let F_i'' and V_i'' be defined analogously for S_2.

Lemma 4. *If π_1 is as above and π_2 has fixed point $d+1$, then we have $V_i = 2^{i/d} \cdot V_d$, $i = 1, 2, \ldots, d-1$ and $V_{d+1} = V_d$.*

Proof. By the geometry of the slicing of S into S_1 and S_2 (see Fig. 3) we have $V'_d = V''_{d+1}$ (this facet is shared by S_1 and S_2), $V'_{d+1} = V_{d+1}$ (the facet shared by S_1 and S), $V''_d = V_d$ (the facet shared by S_2 and S), and $V'_i = V''_i = \frac{1}{2}V_i$ for $i = 1, 2, \ldots, d-1$ (these facets of S are halved by the slicing).

Since f_1 and f_2 change $(d-1)$-dimensional volumes by the factor α^{d-1}, we have $V'_{\pi_1(i)} = V''_{\pi_2(i)} = \alpha^{d-1}V_i$. Since $\pi_1(d) = d$, $\pi_2(d+1) = d+1$, and $V'_d = V''_{d+1}$, we obtain $V_d = V_{d+1}$.

Next, from $V'_2 = \frac{1}{2}V_2$ and $V'_2 = V'_{\pi_1(1)} = \alpha^{d-1}V_1$ we get $V_2 = 2\alpha^{-(d-1)}V_1 = 2 \cdot 2^{-(d-1)/d}V_1 = 2^{1/d}V_1$. Similarly we calculate $V_3, \ldots, V_{d-1}$ and V_{d+1} and obtain the values in the lemma. □

The lemma shows that the facet volumes are uniquely determined by π_1. Since $V_1, \ldots, V_{d-1}$ are all distinct, π_1 can be reconstructed from the facet volumes (in other words, if the numbering of $v_1, \ldots, v_{d-1}$ is hidden, we can reconstruct it from the facet volumes). By symmetry, π_2 is also uniquely determined by the facet volumes, and we have $\pi_2(1) = 2$, $\pi_2(2) = 3$,..., $\pi_2(d-1) = d$, $\pi(d) = 1$ (and $\pi_2(d+1) = d+1$).

We can now write down both the matrices $\bar{A}_1$ and $\bar{A}_2$ (we show them again for $d = 5$):

$$\bar{A}_1 = \begin{pmatrix} -1 & -1 & -1 & -1 & -1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 1 \end{pmatrix}, \quad \bar{A}_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & \frac{1}{2} & 0 \end{pmatrix}.$$

The matrix $\bar{A}_2^{-1}\bar{A}_1$ has the following particularly simple form:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 2 \\ -1 & -1 & -1 & -1 & -1 \end{pmatrix}.$$

The characteristic polynomial is $(1-x)^{d-2}(x^2 - 2x + 3)$. By the necessary condition on $\bar{A}_1$ and $\bar{A}_2$, all roots should have absolute value 1, but the roots of $x^2 - 2x + 3$ are $1 \pm i\sqrt{2}$. This concludes the proof of Theorem 1. □

Proof of Lemma 3. We use (the first part of) the following criterion due to Lehmer [11]:

For a polynomial g of the form $g(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_0$ we define the polynomial $T(g)$ by $T(g)(z) = \overline{a}_0 g(z) - a_n z^n \overline{g(z^{-1})}$, where the bar above a symbol denotes complex conjugation. Let g be a polynomial that has no (complex) root on the unit circle $\Gamma = \{z \in \mathbf{C} : |z| = 1\}$ and such that $g(0) \neq 0$. If, for some integer $h > 0$, $T^h(g)(0) < 0$, then g has at least one root inside Γ (T^h denotes an h-fold composition of the operator T). If $T^i(g)(0) > 0$ for $i = 1, 2, \ldots, h$ and $T^h(g)$ is a constant polynomial, then g has no root inside Γ.

We note that $T(g)(0) = |a_0|^2 - |a_n|^2$, which will be useful later.

We apply the criterion to show that $q_k(x) = 2x^{d+1} - x^{d-k} - 1$, the numerator in the second expression for $p_k(x)$, has a root strictly inside the circle $\Gamma' = \{z \in \mathbf{C} : |z| = 2^{-1/d}\}$. To this end, we check by Lehmer's criterion that for some $\beta < 2^{-1/d}$ the polynomial $g_k(z) = q_k(\beta z)$ has a root in the unit circle. We calculate $g_k(z) = 2\beta^{d+1}z^{d+1} - \beta^{d-k}z^{d-k} - 1$, and $T(g_k)(z) = \beta^{d-k}z^{d-k} + 2\beta^{2d+1-k}z^{k+1} - (2\beta^{d+1})^2 + 1$.

For β sufficiently close to $2^{-1/d}$, the absolute term of $T(g_k)(z)$ satisfies $1 - (2\beta^{d+1})^2 \le 1 - 2^{-2/d} + \varepsilon \le 1 - 2^{-2/3} + \varepsilon < \frac{1}{2}$. The leading term of $T(g_k)(z)$ is

$$\begin{array}{ll} \beta^{d-k} & \text{for } d > 2k+1, \\ 2\beta^{2d+1-k} & \text{for } d < 2k+1, \\ \beta^{(d+1)/2} + 2\beta^{3d/2+1} & \text{for } d = 2k+1. \end{array}$$

In all three cases the leading term is at least $\frac{1}{2}$, and hence $T^2(g_k)(0) < 0$. Lehmer's criterion shows that $p_k(x)$ has a root with absolute value below $2^{-1/d}$ and the lemma is proved. □

3 Probabilistic packet marking

In this section we outline some ideas from [1] and [2] directly related to the present paper.

The *denial-of-service attacks* on the Internet operate by sending an enormous number of packets to the attacked computer through the network. For defense against such attacks it would be very helpful to trace such packets back to their source. Internet packets contain the address of origin, but that can easily be forged. Along its path through the network, each packet passes through several routers, so the source could be traced if each router added its address to each packet passing through it. However, the packets have a standard format which doesn't leave much room for information added by the routers, and even if the packet format could be changed, sending along the addresses of all routers would burden the network significantly. The idea of *probabilistic packet marking* (suggested in [5], with the first actual schemes given in [13] and [7]) is to take advantage of the large number of packets used in attacks and encode information about the route into the *probability distribution* of the values of a small number of bits in the packets.

We explain a simple and ingenious packet marking scheme from [1] (ignoring some technical issues). For simplicity we assume that just one bit B is available for the marking in each packet, with possible values $B = 0$ and $B = 1$. We assume that in some considered period, all packets reaching some destination pass through routers $R_1, R_2, \ldots, R_n$ in this order. Each R_i wants to "record" a one-bit message r_i, with value 0 or 1, into B (actual addresses of routers have more than 1 bit, of course, but we want to explain the principle). It proceeds according to the following protocol.

- For $r_i = 0$: A received packet with $B = 0$ is sent further with $B = 0$. A received packet with $B = 1$ is sent further with B set at random, to $B = 0$ with probability $\frac{1}{2}$ and to $B = 1$ with probability $\frac{1}{2}$ (the random choice is independent of the choices for other packets and in the other routers).
- For $r_i = 1$: A received packet with $B = 1$ is sent further with $B = 1$. A received packet with $B = 0$ is sent further with B set at random, again to 0 or 1 with probability $\frac{1}{2}$ each.

According to this protocol, if the packets incoming to R_i have probability x of having $B = 1$, then the outgoing packets have probability of $B = 1$ equal to $\frac{1}{2}x$ if $r_i = 0$, and equal to $\frac{1}{2} + \frac{1}{2}x$ if $r_i = 1$. Thus, if we interpret the probability distribution of B as a point $x \in [0,1]$, then for $r_i = 0$, the router R_i performs the affine map $g_0 : x \mapsto \frac{1}{2}x$, while for $r_i = 1$ it performs the affine map $g_1 : x \mapsto \frac{1}{2} + \frac{1}{2}x$. If the initial probability distribution of B entering R_1 is given by $y \in [0,1]$, then distribution "seen" at the destination after R_n is given by $x = 2^{-1}r_n + 2^{-2}r_{n-1} + \cdots + 2^{-n}r_1 + 2^{-n-1}y$, and hence the messages of the routers can be read off as the n most significant bits of x. (The technical issues ignored here include how precisely

x can be determined, what are effects of "noisy" packets coming along alternative routes, etc.)

Geometrically, the above packet marking scheme is based on the tiling of $[0,1]$ by the two intervals $[0,\frac{1}{2}]$ and $[\frac{1}{2},1]$. Now one may want to generalize the scheme: First, more than one bit may be available in each packet for the marking; generally one can assume that the marking part of the packet may attain $d+1$ distinct values. Then the probability distribution is specified by a point in the standard d-dimensional simplex $\Delta_d = \{x \in \mathbf{R}^{d+1} : x_1,\ldots,x_{d+1} \geq 0, x_1+x_2+\cdots+x_{d+1} = 1\} \subset \mathbf{R}^{d+1}$, where x_j represents the probability of the jth value among the $d+1$ possible values. And second, the messages of the routers may attain some number m of distinct values, say $1,2,\ldots,m$. In such a situation, we would need m affine maps $g_1, g_2, \ldots, g_m \colon \Delta_d \to \Delta_d$, where a router with message i converts an incoming probability distribution $x \in \Delta_d$ into the probability distribution $g_i(x)$ (it is easy to check that any affine map $\Delta_d \to \Delta_d$ can be realized by a suitable protocol, which works with one packet at a time and for which one need not know the incoming probability distribution). We would like to choose the g_i so that the messages of all routers along the path can be reconstructed from the probability distribution at the destination, allowing for as large error margin in reading off that distribution as possible.

The exact requirements on the g_i can be discussed at great length and are a subject for further research. Here we mention a condition which, if it can be satisfied, yields "asymptotically optimal" marking schemes.

The simplices $g_1(\Delta_d)$, $g_2(\Delta_d)$,..., $g_m(\Delta_d)$ tile Δ_d without overlap, and there exists a constant $c>0$ such that for any finite sequence $i_1, i_2, \ldots, i_n$, $1 \leq i_j \leq m$, the composed map $g = g_{i_1} \circ g_{i_2} \circ \cdots \circ g_{i_n}$ doesn't contract distances too much: it satisfies $\|g(x)-g(y)\| \geq c \cdot m^{-n/d} \cdot \|x-y\|$ for every $x,y \in \Delta_d$.

It is easy to check that if S is a d-dimensional simplex that is an m-reptile, $f_1,\ldots,f_n$ are the similarity maps sending S to the tiles $S_1,\ldots,S_m$, and T is an affine isomorphism $S \to \Delta_d$, then the maps $g_1,\ldots,g_m$ given by $g_i = T \circ f_i \circ T^{-1}$ satisfy the above requirement and thus lead to an asymptotically optimal protocol. Unfortunately, so far it seems that simplex m-reptiles with small m, which would be useful in this context, exist very seldom.

Finally, let us remark that the above condition for the g_i implies the eigenvalue condition formulated in the proof of Theorem 1 (in the special case $m=2$). Thus, the part of that proof using only the eigenvalue condition also applies to the existence of the maps g_i for an asymptotically optimal protocol. However, the part considering the facet volumes does not seem to apply directly in this greater generality.

Acknowledgment

I thank Micah Adler and Uri Zwick for discussions about probabilistic packet marking, which were a starting point of the research reported in this paper. For kind answers to my queries about reptiles, matrices, and similar things I would like to thank Christoph Bandt, Maurice Cochand, David Eppstein, Eike Hertel, Krystyna Kuperberg, Włodek Kuperberg, and Petr Plecháč, and finally, I thank Petr Škovroň for pointing out a gap in an earlier version of the proof.

References

1. M. Adler. Tradeoffs in probabilistic packet marking for IP traceback. In *Proc. 34th Annu. ACM Symposium on Theory of Computing*, pages 407–418, 2002.

2. M. Adler, J. Edmonds, and J. Matoušek. Towards asymptotic optimality in probabilistic packet marking. In *Proc. 37th Annu. ACM Symposium on Theory of Computing*, 2005. To appear.
3. G. L. Alexanderson and J. E. Wetzel. Dissections of a simplex. *Bull. Amer. Math. Soc.*, 79:170–171, 1973.
4. C. Bandt. Self-similar sets. V. Integer matrices and fractal tilings of $\mathbf{R}^n$. *Proc. Amer. Math. Soc.*, 112(2):549–562, 1991.
5. H. Burch and B. Cheswick. Tracing anonymous packets to their approximate source. Contribution at the conference Usenix LISA (New Orleans), 2000.
6. H. E. Debrunner. Tiling Euclidean d-space with congruent simplexes. In *Discrete geometry and convexity (New York, 1982)*, volume 440 of *Ann. New York Acad. Sci.*, pages 230–261. New York Acad. Sci., New York, 1985.
7. T. W. Doeppner, P. N. Klein, and A. Koyfman. Using router stamping to identify the source of IP packets. In *Proc. 7th ACM conference on Computer and communications security*, pages 184–189, 2000.
8. G. Gelbrich. Crystallographic reptiles. *Geom. Dedicata*, 51(3):235–256, 1994.
9. G. Gelbrich. Self-affine lattice reptiles with two pieces in $\mathbf{R}^n$. *Math. Nachr.*, 178:129–134, 1996.
10. E. Hertel. Self-similar simplices. *Beiträge Algebra Geom.*, 41(2):589–595, 2000.
11. D. H. Lehmer. A machine method for solving polynomial equations. *J. Assoc. Comput. Mach.*, 8:151–162, 1961.
12. S.-M. Ngai, V. F. Sirvent, J. J. P. Veerman, and Y. Wang. On 2-reptiles in the plane. *Geom. Dedicata*, 82(1-3):325–344, 2000.
13. S. Savage, D. Wetherall, A. Karlin, , and T. Anderson. Practical network support for IP traceback. In *Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (ACM SIGCOMM)*, pages 295–306, 2000.
14. S. L. Snover, C. Waiveris, and J. K. Williams. Rep-tiling for triangles. *Discrete Math.*, 91(2):193–200, 1991.
15. T. Zaslavsky. Maximal dissections of a simplex. *J. Combinatorial Theory Ser. A*, 20(2):244–257, 1976.