

Exact Euclidean medial axis in higher resolution

André Vital Saúde^{1,2,*}, Michel Couprie², and Roberto Lotufo¹

¹ State University of Campinas, School of Electrical and Computer Engineering,
DCA-FEEC-UNICAMP, Caixa Postal 6101, 13081-970 Campinas/SP, Brazil
{andrevit, lotufo}@dca.fee.unicamp.br

² Institut Gaspard-Monge, Laboratoire A2SI, Groupe ESIEE
Cité Descartes, BP 99, 93162 Noisy-le-Grand Cedex, France
{vitalsaa, coupriem}@esiee.fr

Abstract. The notion of skeleton plays a major role in shape analysis. Some usually desirable characteristics of a skeleton are: sufficient for the reconstruction of the original object, centered, thin and homotopic. The Euclidean Medial Axis presents all these characteristics in a continuous framework. In the discrete case, the Exact Euclidean Medial Axis (MA) is also sufficient for reconstruction and centered. It no longer preserves homotopy but it can be combined with a homotopic thinning to generate homotopic skeletons. The thinness of the MA, however, may be discussed. In this paper we present the definition of the Exact Euclidean Medial Axis on Higher Resolution which has the same properties as the MA but with a better thinness characteristic, against the price of rising resolution. We provide and prove an efficient algorithm to compute it.

1 Introduction

In 1961, Blum [1] introduced the notion of medial axis or skeleton, which has since been the subject of numerous theoretical studies and has also proved its usefulness in practical applications. Consider a subset X (called object) of a metric space. The medial axis of X is the set composed by the centers of the maximal balls for X , that is, the balls which are included in X but which are not included in any other ball included in X .

Although originally defined in the continuous plane, the medial axis can be defined using the same terms in the n -dimensional discrete grid \mathbb{Z}^n . The discrete medial axis is a set of points which is, by nature, centered in the object with respect to the distance which is used to define the notion of ball. To achieve a certain degree of rotation invariance, the Euclidean distance between points of \mathbb{Z}^n may be used. Nevertheless even in this case, the medial axis has not, in general, the same nice properties as its continuous counterpart. In particular, the properties of thinness and homotopy are lost (see for example Figure 1(a) where the medial axis is “two-pixels thick” in some places, and has not the same number of connected components as the original object). Topological aspects are out of the scope of this paper. Nevertheless, let us mention that in order to obtain an homotopic skeleton which contains the medial axis, the use of guided and constrained discrete homotopic transformations has been proposed by several authors (see *e.g.* [2,3,4,5,6]).

On the other hand, the problem of thickness of the skeleton has been tackled in different ways. Some authors use an asymmetric thinning step in order to reduce two-pixel thick configurations. But in this case, the result cannot be considered anymore as centered with respect to the original object, and the property of reconstruction is lost. In order to get a thin medial axis while preserving centeredness (in the sense of the so-called 8-distance), G. Bertrand introduced the notion of derived grid [7]. Also, in the study of discrete topology-preserving transformations, several recent works promote the use of the Khalimsky grid or its variations [8,9,10,11,12]. From a geometrical point of view, the Khalimsky grid \mathbb{H}^n associated to \mathbb{Z}^n can be embedded in $[\frac{1}{2}\mathbb{Z}]^n$, that is, by doubling the resolution of the grid for each dimension. Starting from an initial object in \mathbb{Z}^n , a “model” of this object in \mathbb{H}^n can be computed and then thinned by a symmetrical algorithm [11], producing a result which is both centered and thin.

* A.V. Saúde is thankful to the financial support from Fapesp and Capes, Brazil.

The drawback of the above approaches lies in their sensitivity to rotations. Since they implicitly or explicitly rely on the 8-distance, the skeletons can be quite different for an object and its rotation by, say, $\pi/4$. Our aim in this paper is to provide a notion of medial axis in a doubled resolution grid, based on the Euclidean distance, and an efficient algorithm to compute it. In addition to the Euclidean balls centered on points of \mathbb{Z}^n , we will also consider the balls centered on points of $[\frac{1}{2}\mathbb{Z}]^n$ (see Figure 1(b)).

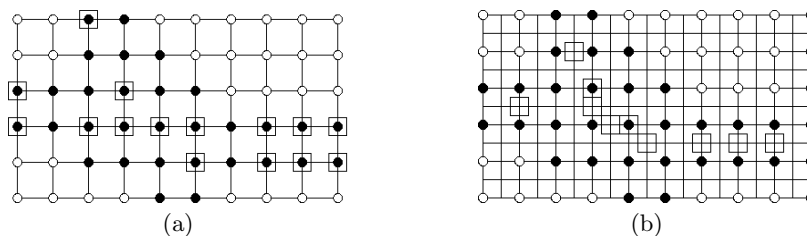


Fig. 1. (a) The object $X \subset \mathbb{Z}^2$ is depicted in black. The squares mark the points of the medial axis, based on the Euclidean distance; (b) The medial axis of X in the doubled resolution grid (squares).

Dealing with the Euclidean distance in \mathbb{Z}^n is far from easy. Many algorithms found in the literature only compute approximations of the Euclidean distance transform (*e.g.* [13]) or medial axis (*e.g.* [14]). A simple to implement, optimal algorithm for building exact Euclidean distance maps was proposed only in 1996 [15,16], and efficient algorithms to compute exact Euclidean medial axes were not known before 2003 [17,18,19]. In this paper, we deal with exact notions and provide proofs of the proposed algorithms.

Let us briefly and informally sketch the proposed method. First, rather than using the grid $[\frac{1}{2}\mathbb{Z}]^n$, we transform the original object X by doubling the coordinates of all its points and consider the grid \mathbb{Z}^n as the doubled resolution grid. This choice leads to simpler notations and proofs. Then, we consider the set X_h composed of all the points of \mathbb{Z}^n which are in the neighborhood of a point of X (scaled). We compute the exact squared Euclidean distance map of X_h using a linear-time algorithm [20,15]. Finally, we propose an efficient algorithm to extract the higher resolution medial axis of X from this distance map. This algorithm is based on the same idea as the one proposed by Rémy and Thiel [17,19] and is also based on pre-computed lookup tables. The biggest of these tables is indeed shared by Rémy and Thiel's method and ours. Obtaining a medial axis for an object X from a distance map relative to a different object X_h is not obvious, and we prove several intermediate properties to establish this fact.

2 Basic notions

We denote by \mathbb{Z} the set of integers, and by \mathbb{N} the set of nonnegative integers. Let $X \subset \mathbb{Z}^n$, we denote by \bar{X} the complementary of X . We denote by $(y-x)^2$ the squared Euclidean distance between two points $x \in \mathbb{Z}^n$ and $y \in \mathbb{Z}^n$.

Let $X \subset \mathbb{Z}^n$, the *squared Euclidean distance transform* of X , denoted by D_X^2 , associates to each point $x \in X$ its squared Euclidean distance to the nearest point in \bar{X} : $D_X^2(x) = \min\{(y-x)^2, y \in \bar{X}\}$.

Let x be a point in \mathbb{Z}^n and let R be a positive integer. The set of points y of \mathbb{Z}^n such that $(y-x)^2 = R$ will be of particular interest in what follows. Each such point y corresponds to a decomposition of R into a sum of n square integers. We introduce some notations to deal with square decompositions of integers.

Definition 1 (Square Decomposition). *Let $n \in \mathbb{N}$, $R \in \mathbb{N}$, the n -uple $(r_1, r_2, \dots, r_n) \in \mathbb{N}^n$ is a square n -decomposition of R if $r_1 \geq r_2 \geq \dots \geq r_n \geq 0$ and $(r_1^2 + r_2^2 + \dots + r_n^2) = R$. We denote by $SQD_n(R)$ the set of all square n -decompositions of R . There are other decompositions of R into*

the sum of n squares, satisfying only the second condition. They may be obtained from the above decompositions by permutations and sign changes.

Let $R \in \mathbb{N}$, we define:

$$\begin{aligned} \bar{R} &= \min\{\delta \in \mathbb{N} \mid \text{SQD}_n(\delta) \neq \emptyset, \delta \geq R\}; & R^+ &= \overline{R+1} \\ \underline{R} &= \max\{\delta \in \mathbb{N} \mid \text{SQD}_n(\delta) \neq \emptyset, \delta \leq R\}; & R^- &= \underline{R-1} \end{aligned}$$

Table 1 illustrates the square decompositions and the above notations.

$R \in \mathbb{N}$	2D				3D					
	$\text{SQD}_2(R)$	\bar{R}	R^+	\underline{R}	R^-	$\text{SQD}_3(R)$	\bar{R}	R^+	\underline{R}	R^-
...										
22	\emptyset	25	25	20	20	$\{(3, 3, 2)\}$	22	24	22	21
23	\emptyset	25	25	20	20	\emptyset	24	24	22	22
24	\emptyset	25	25	20	20	$\{(4, 2, 2)\}$	24	25	24	22
25	$\{(5, 0), (4, 3)\}$	25	26	25	20	$\{(5, 0, 0), (4, 3, 0)\}$	25	26	25	24

Table 1. Illustration of some square decompositions.

Let $R \in \mathbb{N}$. Observe that, if $\text{SQD}_n(R) \neq \emptyset$ then $\bar{R} = \underline{R} = R$ and $(R^-)^+ = (R^+)^- = R$. In addition, if $\text{SQD}_n(R) = \emptyset$ then $\bar{R} = R^+$ and $\underline{R} = R^-$.

We set $\mathbb{D}_n = \{R \in \mathbb{N} \mid \text{SQD}_n(R) \neq \emptyset\}$, the set of n -decomposable integers. It is known that for any $n \geq 4$, $\mathbb{D}_n = \mathbb{N}$ (Lagrange's theorem, see [21], Section 20.5).

Definition 2 (Euclidean Ball). Let $x \in \mathbb{Z}^n$, $R \in \mathbb{N}$, we denote by $B^{\leq}(x, R)$ the Euclidean ball centered in x with (squared) radius R and we denote by $B^{<}(x, R)$ the Euclidean ball centered in x with (squared) strict radius R , where $B^{\leq}(x, R) = \{y \in \mathbb{Z}^n, (x - y)^2 \leq R\}$ and $B^{<}(x, R) = \{y \in \mathbb{Z}^n, (x - y)^2 < R\}$.

Let $x \in \mathbb{Z}^n$, $R \in \mathbb{N}$, we have $B^{\leq}(x, R) = B^{<}(x, R^+)$ and $B^{<}(x, R) = B^{\leq}(x, R^-)$.

Definition 3 (Maximal Ball). Let $X \subset \mathbb{Z}^n$, $x \in X$, $R \in \mathbb{N}$,

- A ball $B^{<}(x, R) \subseteq X$ is a maximal ball for x in X if it is the largest ball centered in x and included in X , i.e., $\forall R' \in \mathbb{N}, B^{<}(x, R) \subseteq B^{<}(x, R') \subseteq X \Rightarrow B^{<}(x, R) = B^{<}(x, R')$;
- A ball $B^{<}(x, R) \subseteq X$ is a maximal ball for X if it is not strictly included in any other ball included in X , i.e., $\forall R' \in \mathbb{N}, \forall y \in X, B^{<}(x, R) \subseteq B^{<}(y, R') \subseteq X \Rightarrow B^{<}(x, R) = B^{<}(y, R')$.

Proposition 1. Let $X \subset \mathbb{Z}^n$, $x \in X$ and $R \in \mathbb{D}_n$. The ball $B^{<}(x, R)$ is maximal for x in X if and only if $R = D_X^2(x)$.

Proof. It is known that $R = D_X^2(x) \Rightarrow B^{<}(x, R)$ is maximal for x in X [19]. In the other direction, suppose $B^{<}(x, R)$ is maximal for x in X , i.e., (1): $B^{<}(x, R) \subseteq X$ and (2): $\forall R' \in \mathbb{N}, B^{<}(x, R) \subseteq B^{<}(x, R') \subseteq X \Rightarrow B^{<}(x, R) = B^{<}(x, R')$. Suppose that $R < D_X^2(x)$, and let $R' = D_X^2(x)$, we have $B^{<}(x, R) \subseteq B^{<}(x, R') \subseteq X$ and since $R \in \mathbb{D}_n$ and $R' \in \mathbb{D}_n$, $B^{<}(x, R) \neq B^{<}(x, R')$ in contradiction with (2). On the other hand, if $R > D_X^2(x)$ we see that (1) cannot hold. Thus $R = D_X^2(x)$.

Observe that, if $B^{<}(x, R)$, with $R \in \mathbb{N}$, is maximal for X , then it is maximal for x in X . Now let us recall the definition of the medial axis [22].

Definition 4 (Medial Axis). Let $X \subset \mathbb{Z}^n$, the medial axis of X , denoted by $MA(X)$, is the set of the centers of all the maximal balls for X .

3 Euclidean medial axis in higher resolution

The goal of changing resolution is to extract a medial axis of the object X by considering a new family of Euclidean balls which are not necessarily centered on points of X . More precisely, we also take into account Euclidean balls centered on the vertices of a doubled resolution grid. For simplicity, instead of considering half integers for the coordinates in the higher resolution grid, we begin by doubling coordinates of the original object. Thus \mathbb{Z}^n is used as the higher resolution grid, and the points with only even coordinates constitute the support of the scaled original image.

Definition 5. Let $i \in \{0 \dots n\}$. We define the set $E_i \subset \mathbb{Z}^n$ as the set of elements in \mathbb{Z}^n with exactly i even coordinates, more precisely $E_i = \{(z_1, z_2, \dots, z_n) \in \mathbb{Z}^n, \sum_{j=1}^n ((z_j + 1) \bmod 2) = i\}$.

Let $X \subset \mathbb{Z}^n$, we write $E_i(X) = E_i \cap X$. Observe that the family $\{E_i\}_{i=0 \dots n}$ forms a *partition* of \mathbb{Z}^n , i.e. $\mathbb{Z}^n = E_0 \cup E_1 \cup \dots \cup E_n$ and $\forall i, j \in \{0 \dots n\}, i \neq j \Rightarrow E_i \cap E_j = \emptyset$.

Definition 6 (Neighborhood). Let $x \in \mathbb{Z}^n$, we define the neighborhood of x as the set $N_n(x) = \{y \in \mathbb{Z}^n \mid \max_{i=1 \dots n} |y_i - x_i| \leq 1\}$. Let $X \subset \mathbb{Z}^n$, we define the set $N_n(X) = \bigcup_{z \in X} N_n(z)$.

Definition 7. Let $X \subset \mathbb{Z}^n$, we define $\phi(X)$ and $\phi^{-1}(X)$ by $\phi(X) = \{2z, z \in X\}$ and $\phi^{-1}(X) = \{z, 2z \in X\}$.

Note that for any subset X of \mathbb{Z}^n , $\phi(X) \subseteq E_n$.

Definition 8 (H-transform). Let $X \subset \mathbb{Z}^n$, the H -transform of X , denoted by $\mathcal{H}(X)$, is defined by $\mathcal{H}(X) = N_n(\phi(X))$.

Figure 2 illustrates the H -transform of a set in \mathbb{Z}^2 . Let $X \subset \mathbb{Z}^n$, observe that $\phi^{-1}(\phi(X)) = X$ and that $E_n(\mathcal{H}(X)) = \phi(X)$, hence $\phi^{-1}(E_n(\mathcal{H}(X))) = X$. The following proposition is elementary.

Proposition 2. The H -transform is increasing, i.e., for each $A, B \subset \mathbb{Z}^n, A \subset B \Rightarrow \mathcal{H}(A) \subset \mathcal{H}(B)$.

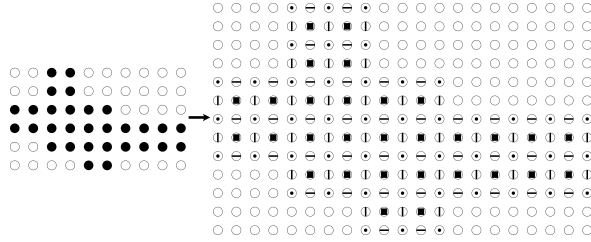


Fig. 2. H -transform of a set in \mathbb{Z}^2 . On the left, the set X (in black), and on the right, the set $\mathcal{H}(X)$. Elements of $\mathcal{H}(X)$ are marked based on the sets of the partition: E_0 (with a dot), E_1 (with a vertical or horizontal line) and E_2 (with a square).

Definition 9 (E_n -tight). Let $X \subset \mathbb{Z}^n, x \in X, R \in \mathbb{D}_n$. The ball $B^{\leq}(x, R)$ is said to be E_n -tight if there is no n -decomposable integer $R' < R$ such that $E_n(B^{\leq}(x, R')) = E_n(B^{\leq}(x, R))$.

It can easily be seen that $B^{\leq}(x, R)$ is E_n -tight if and only if there exists $y \in E_n(B^{\leq}(x, R))$ such that $(x - y)^2 = R$. The following proposition will play an important role to prove the algorithms that we are going to propose. Put briefly, it says that any E_n -tight ball B is included in $N_n(E_n(B))$.

Proposition 3. Let $n \in \mathbb{N}, n \leq 3$. Let $B = B^{\leq}(x, R)$, where $x \in \mathbb{Z}^n, R \in \mathbb{D}_n$, be an E_n -tight ball. For any $z \in B$, there exists a point $w \in N_n(z)$ such that $w \in E_n(B)$, i.e., $B \subseteq N_n(E_n(B))$.

Although this proposition may seem simple, it is in fact false in general but true in dimensions 2 and 3. Furthermore, the counter-example of Figure 3 shows that the condition “ E_n -tight” is indeed necessary for the proposition. With this condition, we will be able to justify our algorithms, and the practical applications are mostly in dimensions 2 and 3.

Proof. For simplicity, we present only the proof in 2 dimensions. The proof for 3 dimensions is more technical but uses essentially the same kind of arguments. It is given in the appendix.

If $R = 0$ or $R = 1$, the proposition can be verified easily. Suppose now that $R > 1$. Let $z = (z_1, z_2) \in B$. Without loss of generality, suppose that $z_1 - x_1 \geq z_2 - x_2 \geq 0$.

First, let us suppose that $z_2 - x_2 \geq 1$. Let $a = (z_1 - 1, z_2)$, $b = (z_1, z_2 - 1)$ and $c = (z_1 - 1, z_2 - 1)$. It can be easily seen (Figure 4) that a , b and c are in B , furthermore at least one of a , b , c or z belongs to E_n . Let w be this point, we have $w \in E_n(B) \cap N_n(z)$.

Now take the case $z_2 - x_2 = 0$. Let $l_1 = z_1 - x_1$, let $r = R - 1$ and let $a' = (z_1 - 1, z_2)$, $b' = (z_1, z_2 + 1)$, $c' = (z_1 - 1, z_2 + 1)$. If $l_1^2 \leq r$, then, by elementary geometry, it can be seen that $b' \in B$, and we have the same argument as in the previous case, with the points a' , b' , c' , z (see Figure 4). Otherwise, we have $r = R - 1 < l_1^2 \leq R$, thus $l_1^2 = R$ and $b' \notin B$. If $a' \in E_n$ or $c' \in E_n$ or $z \in E_n$ then we are done, suppose that it is not the case, thus b' must be in E_n . It implies that z_2 and x_2 are odd and z_1 is even. By hypothesis, $\exists y \in E_n(B)/(x - y)^2 = R = l_1^2$. Since x_2 is odd and $y \in E_n$, then $x_2 - y_2$ is odd. Let us examine the possible cases. Case 1: l_1 is even; since z_1 is even, x_1 must also be even, so $x_1 - y_1$ is even; thus we have a contradiction because $(x_1 - y_1)^2 + (x_2 - y_2)^2 = l_1^2$ and the sum of an even number and an odd number cannot be even. Case 2: l_1 is odd; in this case x_1 must be odd, so $x_1 - y_1$ is odd; thus we have a contradiction because the sum of two odd numbers cannot be odd. \square

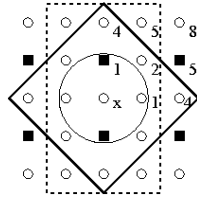


Fig. 3. (a) Consider the ball $B = B^{\leq}(x, 4)$, surrounded by a solid rectangle. The points of E_n are marked by black squares. We see that B is not E_n -tight, and that B is not included in $N_n(E_n(B))$ (surrounded by a dashed rectangle). On the other hand, the ball $B' = B^{\leq}(x, 1)$ (surrounded by a circle) is E_n -tight and included in $N_n(E_n(B'))$;

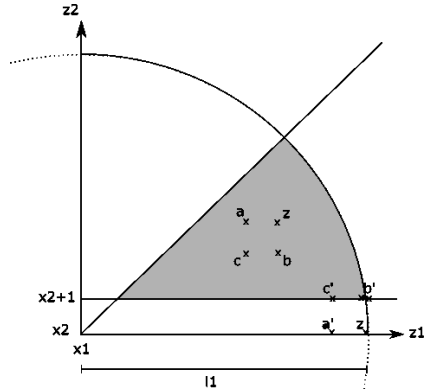


Fig. 4. (b) Illustration for the proof of Proposition 3 in 2D. All the considered points have integer coordinates.

No proof has been done for Proposition 3 in dimensions higher than 3. We do not know the dimension until which this proposition remains true. However, it is easy to find counter examples in dimensions higher or equal to 9: the simplest one is based on the square decomposition $3^2 = 1^2 + 1^2 + \dots + 1^2$. Using the same notations as above, take $x = (1, 1, 1, 1, 1, 1, 1, 1, 1)$, $z = (4, 1, 1, 1, 1, 1, 1, 1, 1)$, and $y = (2, 2, 2, 2, 2, 2, 2, 2, 2)$. It can be seen that any neighbor of z which is in $B^{\leq}(x, 9)$ has an odd first coordinate, and thus does not belong to E_n .

E_n -balls and higher resolution medial axis

For any $x \in \mathbb{Z}^n$, $R \in \mathbb{D}_n$, the set $E_n(B^<(x, R))$ is called an E_n -ball, it can be seen as an Euclidean ball in E_n which is centered in any point of \mathbb{Z}^n (not necessarily in E_n). E_n -balls may have different

symmetry characteristics depending on where they are centered. Some E_n -balls are illustrated in Figure 5 for \mathbb{Z}^2 .

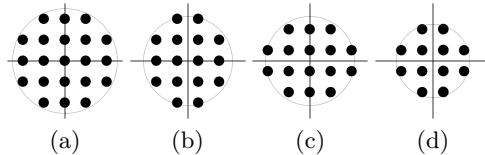


Fig. 5. E_n -balls in \mathbb{Z}^2 . Only points of E_n are represented. (a) E_n -ball centered in E_2 , (b) and (c) E_n -balls centered in E_1 , (d) E_n -ball centered in E_0 .

Definition 10 (E_n -maximal balls). Let $X \subset \mathbb{Z}^n$, $x \in X$, $R \in \mathbb{N}$,

a) An E_n -ball $E_n(B^<(x, R)) \subseteq X$ is an E_n -maximal ball for x in X if it is the largest E_n -ball centered in x and included in X , i.e., $\forall R' \in \mathbb{N}, E_n(B^<(x, R)) \subseteq E_n(B^<(x, R')) \subseteq X \Rightarrow E_n(B^<(x, R)) = E_n(B^<(x, R'))$;

b) An E_n -ball $E_n(B^<(x, R)) \subseteq X$ is an E_n -maximal ball for the set X if it is not strictly included in any other E_n -ball included in X , i.e., $\forall R' \in \mathbb{N}, \forall y \in \mathbb{Z}^n, E_n(B^<(x, R)) \subseteq E_n(B^<(y, R')) \subseteq X \Rightarrow E_n(B^<(x, R)) = E_n(B^<(y, R'))$.

Definition 11 (HMA). Let $X \subset \mathbb{Z}^n$. The higher resolution medial axis $HMA(X)$ is the set of centers of all E_n -maximal balls of $\mathcal{H}(X)$.

The problem of extracting the HMA is to find the set of E_n -maximal balls for the object. Knowing the radii of the E_n -maximal balls for each point is necessary to test maximality for the object. Let $X \subset \mathbb{Z}^n$, $X_h = \mathcal{H}(X)$, $x \in X_h$, in nD the radius of the E_n -maximal ball for x can be obtained from $D_{X_h}^2(x)$ by looking for the first integer $R \geq D_{X_h}^2(x)$ such that $x + v \in E_n(\overline{X_h})$, with v being any vector satisfying $v^2 = R$. However, in 2D and 3D, Proposition 3 can be used to prove the following proposition; which ensures that $D_{X_h}^2(x)$ is precisely the radius of the E_n -maximal ball for x in X_h .

Proposition 4. Let $X \subset \mathbb{Z}^n$, $X_h = \mathcal{H}(X)$, $x \in X_h$, $R \in \mathbb{D}_n$, $n \leq 3$. If $B^<(x, R)$ is maximal for x in X_h then $E_n(B^<(x, R))$ is E_n -maximal for x in X_h .

Proof. If $B^<(x, R)$ is maximal for x in X_h , then $R = D_{X_h}^2(x)$ (Proposition 1). Let B_M be an E_n -maximal ball for x in X_h . By definition of B_M , we have $E_n(B^<(x, R)) \subseteq B_M$, we are going to prove the converse. Let $B_h = N_n(B_M)$. Notice that B_h is not a ball in general. Notice also that $E_n(B_h) = B_M$, thus B_M is E_n -maximal for x in B_h . We know that $B_M \subseteq E_n(X_h)$, thus $B_h \subseteq X_h$ by Proposition 2. Let $R_M \in \mathbb{D}_n$ be the smallest decomposable integer such that $E_n(B^<(x, R_M)) = B_M$. Since R_M is minimal under this constraint, then $B^<(x, R_M)$ is E_n -tight and, from Proposition 3, $B^<(x, R_M) \subseteq N_n(E_n(B^<(x, R_M))) = B_h$. Thus, $\forall y \in \mathbb{Z}^n$, we have $(y - x)^2 \leq R_M \Rightarrow y \in B_h$ and, by negation, $z \in \overline{B_h} \Rightarrow (z - x)^2 > R_M$. Thus, $D_{B_h}^2(x) > R_M$ and $B^<(x, R_M) \subseteq B^<(x, D_{B_h}^2(x))$. But $B_h \subseteq X_h$ implies $D_{B_h}^2(x) \leq D_{X_h}^2(x)$, thus $B^<(x, D_{B_h}^2(x)) \subseteq B^<(x, D_{X_h}^2(x))$. Taking the intersection with E_n , we deduce that $B_M = E_n(B^<(x, R_M)) \subseteq E_n(B^<(x, D_{X_h}^2(x)))$. \square

4 Algorithm to compute the HMA

In this section we present an algorithm to compute the higher resolution medial axis (HMA). Testing if an E_n -ball is maximal for the object is not trivial. One way of doing this is to test if it is not included in another E_n -ball. This can be done by an adaptation of the algorithm presented by Rémy and Thiel [19] for the extraction of the exact Euclidean medial axis (MA).

Euclidean balls have a number of symmetries that simplify the problem. An Euclidean ball can be reconstructed from only one of its cones (octant in 2D) by retrieving symmetries of each point (or vector) of that cone. We chose the *generator* cone to be the set of vectors $v^g \in \mathbb{Z}^n$ such that $v^g = (v_1, v_2, \dots, v_n), v_1 \geq v_2 \geq \dots \geq v_n \geq 0$. We distinguish two types of symmetries of v^g :

- Type 1. A symmetry obtained by setting signs to the coordinates of v^g . It can be obtained by $S_1 v^g$, where S_1 is a matrix in which every element in the diagonal equals 1 or -1 , with 0s everywhere else. A vector in \mathbb{Z}^n has therefore 2^n Type 1 symmetries, which gives 4, 8 and 16 for $n = 2, 3$ and 4 respectively. We denote by S_1^n the set of all Type 1 matrices in nD .
- Type 2. A symmetry obtained by a permutation of the coordinates of v^g . It can be obtained by $S_2 v^g$, where S_2 is a matrix obtained by permuting the rows of an identity matrix according to some permutation of the numbers 1 to n . Every row and column therefore contains precisely a single 1 with 0s everywhere else. A vector in \mathbb{Z}^n has therefore $n!$ Type 2 symmetries, which gives 2, 6 and 24 for $n = 2, 3$ and 4 respectively. We denote by S_2^n the set of all Type 2 matrices in nD .

Below we give some examples in 3D of Type 1 and Type 2 symmetries of v^g obtained by a Type 1 matrix S_1 and a Type 2 matrix S_2 , respectively:

$$S_1 = \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix}, v^g = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}, S_1 v^g = \begin{bmatrix} -v_1 \\ v_2 \\ -v_3 \end{bmatrix}; \quad S_2 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, v^g = \begin{bmatrix} v_1 \\ v_2 \\ v_3 \end{bmatrix}, S_2 v^g = \begin{bmatrix} v_2 \\ v_3 \\ v_1 \end{bmatrix}$$

For the algorithm we are going to present in this section, we need all the combinations of symmetries of Types 1 and 2. Any symmetry of v^g in \mathbb{Z}^n can be obtained by $S_1 S_2 v^g, S_1 \in S_1^n, S_2 \in S_2^n$. There are therefore $2^n n!$ symmetries in \mathbb{Z}^n , which gives 8, 48 and 384 for $n = 2, 3$ and 4 respectively. We denote by S^n the set of all products $S_1 S_2$, with $S_1 \in S_1^n$, and $S_2 \in S_2^n$.

4.1 Algorithm for the medial axis (Rémy and Thiel)

Given a set $X \in \mathbb{Z}^n$ and its square Euclidean distance transform D_X^2 , the algorithm proposed by Rémy and Thiel [19] tests, for each point $x \in X$, if the maximal ball for x in X , $B^<(x, D_X^2(x))$, is a maximal ball for X . This is done by testing if $B^<(x, D_X^2(x))$ is not included in another ball in X . If the maximal radius of all maximal balls for X is not greater than a previously known radius $R_{max} \in \mathbb{N}$, the inclusion test can be performed efficiently with the help of previously computed lookup tables. These lookup tables are described below and the algorithms to compute them are shortly presented in Annex. See the reference [19] for details.

- Let $X \in \mathbb{Z}^n, x \in X$, if the maximal radius of all maximal balls for the set X is not greater than a previously known radius $R_{max} \in \mathbb{N}$, it is possible to precompute a limited set of generator vectors $\mathcal{M}_{R_{max}}^g$ which is sufficient to ensure that, if $\forall v^g \in \mathcal{M}_{R_{max}}^g, \forall S \in S^n, B^<(x, D_X^2(x)) \not\subseteq B^<(x + S v^g, D_X^2(x + S v^g))$, then $x \in \text{MA}(X)$. $\mathcal{M}_{R_{max}}^g$ is the set of sufficient vectors for the radius R_{max} .
- Let $x \in \mathbb{Z}^n, v^g \in \mathcal{M}_{R_{max}}^g$, for any value of R_{max} , let $R \in \mathbb{D}_n$. The table $\text{Lut}[v^g, R]$ gives the minimal radius $R' \in \mathbb{D}_n$ necessary for having $\forall S \in S^n, B^<(x, R) \subseteq B^<(x + S v^g, R')$. Note that $\text{Lut}[0, R] = R$.

To compute the MA of a set $X \in \mathbb{Z}^n$, it is sufficient to apply the **IsMA** function for every point $x \in X$. The correctness of Function **IsMA** lies on Proposition 5 and Proposition 6, proved in [19].

Function IsMA(x, R_{max}, D_X^2)

```

// tests if  $x \in \text{MA}(X)$ 
1 foreach  $v^g \in \mathcal{M}_{R_{max}}^g$  do
2   foreach  $S \in S^n$  do
3      $v \leftarrow S v^g$ ;
4      $R_v \leftarrow \text{Lut}[v^g, D_X^2(x)]$ ;
5     if  $D_X^2(x + v) \geq R_v$  then return false
6 return true

```

Proposition 5. Let $x \in \mathbb{Z}^n, v^g \in \mathcal{M}^g, S \in S^n, v = Sv^g, R \in \mathbb{D}_n, R' \in \mathbb{D}_n$, we have $B^<(x, R) \subseteq B^<(x + v, R') \Leftrightarrow R' \geq Lut[v^g, R]$.

Proposition 6. Let $X \subset \mathbb{Z}^n, x \in X, R_{max} = \max\{D_X^2(z) \mid z \in X\}$. The ball $B^<(x, D_X^2(x))$ is maximal for X if and only if $\forall v^g \in \mathcal{M}_{R_{max}}^g, \forall S \in S^n, B^<(x, D_X^2(x)) \not\subseteq B^<(x + v, D_X^2(x + v))$ where $v = Sv^g$.

4.2 Algorithm to extract the HMA

The MA algorithm presented above takes profit of the minimal radii given by the lookup table *Lut*. We need a notion of minimal radius for the E_n -balls.

Definition 12 (E_n -minimal radius). Let $x \in \mathbb{Z}^n, R \in \mathbb{D}_n, v \in \mathbb{Z}^n$, the E_n -minimal radius relative to x, R and v , denoted by $R^V(x, R, v)$, is the strict radius of the smallest ball centered in $x + v$ which includes $E_n(B^<(x, R))$, i.e., $R^V(x, R, v) = \min\{R' \in \mathbb{D}_n, E_n(B^<(x, R)) \subseteq E_n(B^<(x + v, R'))\}$.

The following proposition is elementary.

Proposition 7. Let $x \in \mathbb{Z}^n, R \in \mathbb{D}_n, R' \in \mathbb{D}_n, v \in \mathbb{Z}^n, R' < R^V(x, R, v) \Leftrightarrow E_n(B^<(x, R)) \not\subseteq E_n(B^<(x + v, R'))$.

Unlike Euclidean balls in \mathbb{Z}^n , E_n -balls may not be invariant by symmetries of Type 2. Thus the value of $R^V(x, R, v)$ depends on to which subset E_i of \mathbb{Z}^n belong the points x and $x + v$. The construction of a lookup table with E_n -minimal radii may be prohibitive. We propose to calculate $R^V(x, R, v)$ on runtime with the Function **EnRmin** below.

Function EnRmin(x, R, v)

```

// we consider  $S_1 \in S_1^n, S_2 \in S_2^n, v = S_1 S_2 v^g$ ,
// where  $v^g$  is the generator of  $v$ 
1  $R_v \leftarrow Lut[v^g, R]$ ;
2 while  $R_v > 0$  do
3   foreach  $r^g \in SQD_n(R_v^-)$  do
4     foreach  $S'_2 \in S_2^n$  do
5        $r \leftarrow S_1 S'_2 r^g$ ;
6       if  $((x + v - r) \in E_n)$  and  $((v - r)^2 < R)$ 
7         then return  $R_v$ 
8    $R_v \leftarrow R_v^-$ ;
9 return 0

```

We illustrate the Function **EnRmin** with the help of Figure 6, which is a crop of a set $X_h = \mathcal{H}(X), X \subset \mathbb{Z}^2$. The values on each pixel are the values of $D_{X_h}^2$. The pixels with a circle correspond to the E_2 points. We consider the point x , in the dark gray square, with $R = D_{X_h}^2(x) = 41$. The contour of the maximal ball for x in X_h , $B^<(x, R)$, is marked in dark gray. Considering for instance $v^g = (3, 1)$ and its symmetric $v = (-1, -3)$, the point $x + v$ is the medium gray square with value 85. The Type 1 symmetry of v is $S_1 = [-1, 0; 0, -1]$. We know that $R_v = Lut[v^g, 41] = 91$ satisfies $B^<(x, R) \subseteq B^<(x + v, R_v)$. The contour of the ball $B^<(x + v, R_v)$ is represented in light gray and we see that it is not included in X_h . This can also be deduced from the fact that $91 > 85 = D_{X_h}^2(x + v)$, but this is not important to us. Remark that we have $E_n(B^<(x, R)) \subseteq E_n(B^<(x + v, R_v))$. In line 3 of **EnRmin**, $R_v^- = 9^2 + 3^2 = 90$, and $SQD_2(R_v^-) = \{(9, 3)\}$, so the **foreach** loop executes only with $r^g = (9, 3)$. The **foreach** loop in line 4 executes twice, which is the number of Type 2 symmetries in 2D. In line 5, we will have first $r = (-9, -3)$ and then $r = (-3, -9)$. We see that the points in $B^<(x, R)$ which are the farthest from $x + v$ are in the shaded (very light gray) region, which is the quadrant with signs opposite to the signs of v , then $x + v - r$ gives one of the farthest points of $B^<(x + v, R_v)$ in that quadrant, $x + v - r - x = v - r$ are its coordinates relative to x , and $(v - r)^2$ is its distance to x . We understand that $(v - r)^2 < R$ tests if $(x + v - r) \in B^<(x, R)$. The points $x + v - (-9, -3) = x + (8, 0)$ and $x + v - (-3, -9) = x + (2, 6)$ are marked by the arrows. None is in E_2 , so R_v is reduced and the while loop continues. When R_v reaches 89, we have $R_v^- = 85$, $SQD_2(R_v^-) = \{(9, 2), (7, 6)\}$ and r is $(-9, -2), (-2, -9), (-7, -6)$ or $(-6, -7)$. The points $x + v + (-9, -2) = x + (8, -1)$ and $x + v + (-7, -6) = x + (6, 3)$ are in E_2 , but not in $B^<(x, R)$,

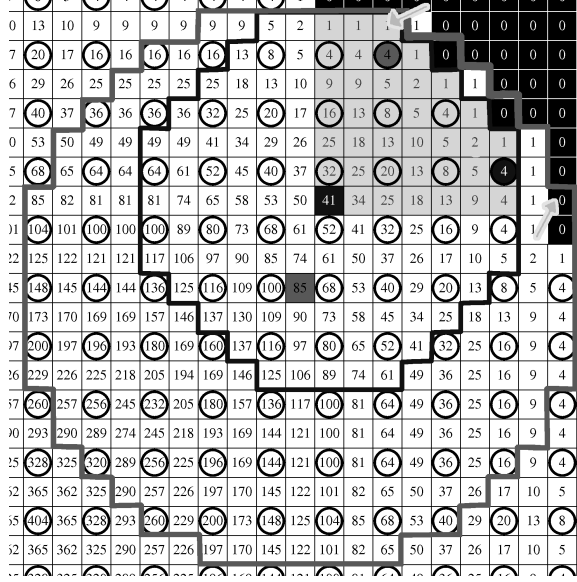


Fig. 6. Illustration of the EnRmin function. The first coordinate grows from left to right and the second coordinate grows from down to top. The coordinates of the dark gray square with value 41, relative to the medium gray square with value 85 is $v = (-1, -3)$.

so R_v continues to be reduced until $R_v = 74$. Then $R_v^- = 73$ and $\text{SQD}_2(73) = \{(8, 3)\}$. With $r = (-3, -8)$, we have $x + v + (-3, -8) = x + (2, 5)$. Here $x + (2, 5) \in E_2$ and $x + (2, 5) \in B^<(x, R)$ and the function returns $R_v = 74$. Note that the point $x + (2, 5)$, with a light gray circle, is the point of E_2 which is the farthest from $x + v$ in $B^<(x + v, 74)$ but it is not the farthest from x in $B^<(x, R)$. This last one is the point $x + (6, 1)$, marked with the dark gray circle.

Proposition 8. *The value R_v returned by the EnRmin function is equal to $R^V(x, R, v)$.*

Proof. We consider the invariant $I(R_v) = [E_n(B^<(x, R)) \subseteq E_n(B^<(x + v, R_v))]$. The initialization $R_v \leftarrow \text{Lut}[v^g, R]$ sets $I(R_v)$ to true, because, by Proposition 5 we have $B^<(x, R) \subseteq B^<(x + v, R_v)$. By negation of Proposition 7, we see that $R_v \geq R^V(x, R, v)$. The if clause guarantees that R_v is reduced only if $I(R_v)$ remains true. Thus the algorithm stops when $E_n(B^<(x, R)) \not\subseteq E_n(B^<(x + v, R_v^-))$ and from Proposition 7 we deduce that $R_v^- < R^V(x, R, v)$. As post-condition we have $R_v^- < R^V(x, R, v) \leq R_v$. But $R_v^- < R_v$, which means that $R^V(x, R, v) = R_v \square$

The number of iterations of the Function EnRmin is limited by the number of square decompositions of all integers greater than $R^V(x, R, v)$ and smaller than $\text{Lut}[v^g, R]$. This value increases as the size of the analyzed balls increases. It is of course limited by the maximal radius of the object.

Now we need to construct a table \mathcal{M}^h , which gives the set of vectors sufficient to compute the HMA. The construction of this table is done by the BuildMhLut procedure presented in Annex. This procedure, similar to the one of [19] to compute \mathcal{M}^g , is based on the observation that if $\mathcal{M}_{R_{max}}^h$ is sufficient to extract, from any ball with a radius less or equal to R_{max} , a medial axis which is reduced to a single point, then $\mathcal{M}_{R_{max}}^h$ enables to extract correctly the HMA from any squared distance map which values do not exceed R_{max} .

By construction of \mathcal{M}^h and as a direct consequence of Proposition 7 and Proposition 8, we have the two following properties.

Proposition 9. *Let $x \in \mathbb{Z}^n, v^g \in \mathcal{M}^h, S \in S^n, v = Sv^g, R \in \mathbb{N}, R' \in \mathbb{N}$, we have $E_n(B^<(x, R)) \subseteq E_n(B^<(x + v, R')) \Leftrightarrow R' \geq \text{EnRmin}(x, R, v)$.*

Proposition 10. Let $X \subset \mathbb{Z}^n$, $X_h = \mathcal{H}(X)$, $x \in X_h$, $R_{max} = \max\{D_{X_h}^2(x'), x' \in X_h\}$. The E_n -ball $E_n(B^<(x, D_{X_h}^2(x)))$ is E_n -maximal for X_h if and only if $\forall v^g \in \mathcal{M}_{R_{max}}^h, \forall S \in S^n, E_n(B^<(x, D_{X_h}^2(x))) \not\subset E_n(B^<(x+v, D_{X_h}^2(x+v)))$, where $v = Sv^g$.

We conclude from Proposition 9 and Proposition 10 that, given a set $X \subset \mathbb{Z}^n$, the computation of $\text{HMA}(X)$ may be done by the computation of the IsHMA function for every point $x \in \mathcal{H}(X)$.

Function $\text{IsHMA}(x, R_{max}, D_{X_h}^2)$

```

// tests if  $x \in \text{HMA}(X)$  in  $\mathbb{Z}^n$ ,  $X_h = \mathcal{H}(X)$ 
1 foreach  $v^g \in \mathcal{M}_{R_{max}}^h$  do
2   foreach  $S \in S^n$  do
3      $v \leftarrow Sv^g$ ;
4      $R_v \leftarrow \text{EnRmin}(x, D_{X_h}^2(x), v)$ ;
5     if  $D_{X_h}^2(x+v) \geq R_v$  then return false
6 return true

```

To efficiently calculate R^+ , R^- for any integer R , another precomputed lookup table is used: the square decompositions table SQD_n defined in Section 2. To precompute this table in 2D, we use the simple algorithm listed in Annex. Its generalization to nD is obvious. Let $R \in \mathbb{N}$, $x \in \mathbb{Z}^n$, calculations are expressed as follows:

$$\begin{aligned} \overline{R}: & \text{ (while } (\text{SQD}_n(R) = \emptyset) \text{ do } R \leftarrow R + 1); & R^+: & (R \leftarrow R + 1; R \leftarrow \overline{R}) \\ \underline{R}: & \text{ (while } (\text{SQD}_n(R) = \emptyset) \text{ do } R \leftarrow R - 1); & R^-: & (R \leftarrow R - 1; R \leftarrow \underline{R}) \end{aligned}$$

5 Results

Besides the didactic example given in Figure 1(a), in this section we present some examples of the HMA comparing it to the MA. In Figure 7 we show results in 2D and in 3D.

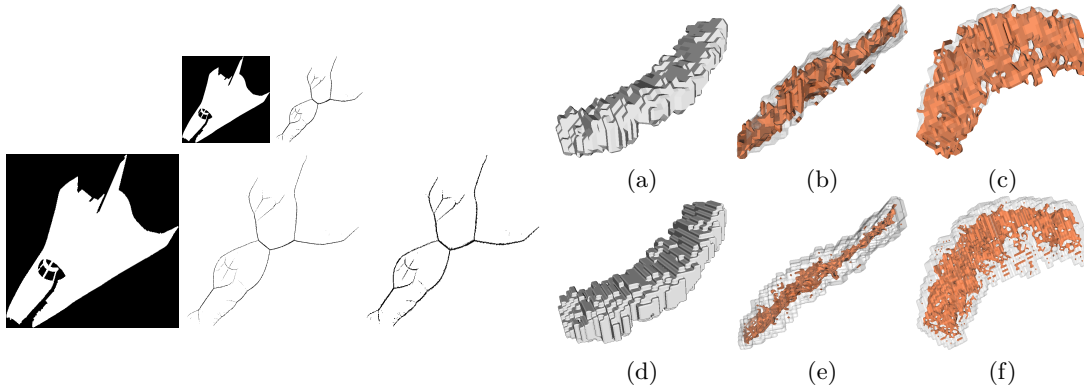


Fig. 7. LEFT: 2D HMA example. First row: the original object and its MA; second row from left to right: the object in doubled resolution, its HMA and, for comparison, the MA scaled to a double resolution. RIGHT: 3D HMA examples. Let X be the object, we have (a) 2D projection of X ; (b) and (c) two different views of X (transparent) and $\text{MA}(X)$ (opaque). (d) 2D projection of $\mathcal{H}(X)$; (e) and (f) two different views of $\mathcal{H}(X)$ (transparent) and $\text{HMA}(X)$ (opaque). Images are scaled for comparison of thinness.

As a practical evaluation of the HMA computation time, we have executed MA and HMA on several images similar to those presented in Figure 7. The estimations were performed on an AMD Athlon XP 2400+, 2.0 GHz, running Linux, without compiler optimizations. The 3D object on the right of Figure 7 is a hippocampus. It is a cerebral structure with particular interest in medical applications.

Let X be the object. We measured the times $t(X)$ and $t_h(X)$ for computing $\text{MA}(X)$ and $\text{HMA}(X)$, respectively.

For the 2D images, we have zoomed the images by factors of 0.5, 1 and 2 in order to have different ball sizes in similar shapes. The object sizes are 12445, 50157 and 112842 pixels. We obtained for $t(X)$: 0.187, 0.426, 0.662 and for $t_h(X)$: 0.487, 1.281, 2.906 (in seconds). The ratios between $t_h(X)$ and $t(X)$ are respectively 2.6, 3.0 and 4.4. The fact that we obtained ratios below four, whereas doubling the resolution multiplies the data volume by four in 2D, is mainly due to the relative cost of loading the lookup tables: this cost is significant for small images but is better amortized for large images. Notice, however, that only the parts of the lookup tables which are really needed are loaded.

For the 3D images, we used zooming factors of 1, 1.5 and 2, and the object sizes are 3530, 11799 and 24771 voxels. We obtained for $t(X)$: 0.077, 0.148, 0.330, and for $t_h(X)$: 0.422, 2.01, 5.36; hence the ratios: 5.45, 13.5, 16.2. Notice that in 3D, doubling the resolution multiplies the data volume by eight.

We also evaluated and compared the “thinness” of the HMA and the one of the MA. Let us denote by $T(X)$ the ratio: $\text{size}(\text{MA}(X))/\text{size}(X)$, and by $T_h(X)$ the ratio: $\text{size}(\text{HMA}(X))/\text{size}(\mathcal{H}(X))$. In 2D, we obtained for the three zoomed images: $T(X) = 0.091, 0.054, 0.042$, and $T_h(X) = 0.035, 0.022, 0.017$ respectively. In 3D, we obtained for the three zoomed images: $T(X) = 0.33, 0.26, 0.24$, and $T_h(X) = 0.067, 0.072, 0.077$ respectively.

It was interesting to note in the 2D case that the bigger is X , the thinner is $\text{MA}(X)$, and that the HMA offers better improvements for small objects. In 3D, the same observation may be done, and the improvements brought by the HMA are more sensible than in 2D.

6 Conclusion

We have defined the HMA - the exact Euclidean medial axis in higher resolution in a completely discrete framework. We showed that the HMA presents better thinness characteristics than the classical discrete Euclidean MA. We explained how to compute such axis in n -dimensions and we provided an efficient algorithm to compute it in 2D and 3D. The algorithm has been systematically proved and some results are compared to the MA. The HMA is based on a transformation to higher resolution which permits the application of further homotopic thinning for the computation of homotopic skeletons. We believe that a skeleton with better thinness properties, containing the HMA or a subset of it, may lead to better shape characterization and quantification.

References

1. Blum, H.: An associative machine for dealing with the visual field and some of its biological implications'. *Biological prototypes and synthetic systems* **1** (1961) 244–260
2. Davies, E., Plummer, A.: Thinning algorithms: a critique and a new methodology. *Pattern Recognition* **14** (1981) 53–63
3. Vincent, L.: Efficient computation of various types of skeletons. In: *Procs. Medical Imaging V, SPIE. Volume 1445*. (1991) 297–311
4. Talbot, H., Vincent, L.: Euclidean skeletons and conditional bisectors. In: *Procs. VCIP'92, SPIE. Volume 1818*. (1992) 862–876
5. Pudney, C.: Distance-ordered homotopic thinning: a skeletonization algorithm for 3D digital images. *Computer Vision and Image Understanding* **72**(3) (1998) 404–413
6. Couprie, M., Coeurjolly, D., Zrour, R.: Discrete bisector function and Euclidean skeleton in 2d and 3d. *Image and Vision Computing* (2006) submitted.
7. Bertrand, G.: Skeletons in derived grids. In: *procs. Int. Conf. Patt. Recogn.* (1984) 326–329
8. Kovalevsky, V.: Finite topology as applied to image analysis. *Computer Vision, Graphics and Image Processing* **46** (1989) 141–161
9. Khalimsky, E., Kopperman, R., Meyer, P.: Computer graphics and connected topologies on finite ordered sets. *Topology and its Applications* **36** (1990) 1–17
10. Kong, T.Y., Kopperman, R., Meyer, P.: A topological approach to digital topology. *American Mathematical Monthly* **38** (1991) 901–917
11. Bertrand, G.: New notions for discrete topology. In: *procs. DGCI, LNCS, Springer Verlag. Volume 1568*. (1999) 216–226

12. Bertrand, G., Couprie, M.: Two-dimensional parallel thinning algorithms based on critical kernels. Technical Report IGM2006-02, Université de Marne-la-Vallée (2006) submitted to CVIU.
13. Danielsson, P.: Euclidean distance mapping. *Computer Graphics and Image Processing* **14** (1980) 227–248
14. Meyer, F.: Cytologie quantitative et morphologie mathématique. PhD thesis, École des Mines de Paris, France (1979)
15. Hirata, T.: A unified linear-time algorithm for computing distance maps. *Information Processing Letters* **58**(3) (1996) 129–133
16. Meijster, A., Roerdink, J., Hesselink, W.: A general algorithm for computing distance transforms in linear time. In J. Goutsias, L.V., Bloomberg, D., eds.: *Mathematical morphology and its applications to image and signal processing 5th*. Volume 18 of *Computational Imaging and Vision*., Kluwer Academic Publishers (2000) 331–340
17. Rémy, E., Thiel, E.: Look-up tables for medial axis on squared Euclidean distance transform. In: *procs. DGCI, LNCS, Springer Verlag*. Volume 2886. (2003) 224–235
18. Cœurjolly, D.: d-dimensional reverse Euclidean distance transformation and Euclidean medial axis extraction in optimal time. In: *procs. DGCI, LNCS, Springer Verlag*. Volume 2886. (2003) 327–337
19. Rémy, E., Thiel, E.: Exact medial axis with Euclidean distance. *Image and Vision Computing* **23**(2) (2005) 167–175
20. Saito, T., Toriwaki, J.: New algorithms for Euclidean distance transformation of an n -dimensional digitized picture with applications. *Pattern Recognition* **27** (1994) 1551–1565
21. Hardy, G., Wright, E.: *An Introduction to the Theory of Numbers*. 5th edn. Oxford University Press (1978)
22. Blum, H.: A transformation for extracting new descriptors of shape. In Wathendunn, W., ed.: *Models for the Perception of Speech and Visual Form*. MIT Press (1967) 362–380

A Building the look-up tables

The `BuildMgLut` procedure builds the table $\mathcal{M}_{R_{max}}^g$, supposing we have already the function `calc_MA(X, \mathcal{M}^g)` which calculates $\text{MA}(X)$, given \mathcal{M}^g . The `BuildLut` procedure builds `Lut` for $\mathcal{M}_{R_{max}}^g$, supposing we have already $\mathcal{M}_{R_{max}}^g$. It is simpler than the one given in [19] thanks to the use of the table SQD_n . The `BuildSQD2` procedure builds SQD_2 for all integers lower than N . The `BuildMhLut` procedure builds the table $\mathcal{M}_{R_{max}}^h$, supposing we have already the function `calc_HMA(X, \mathcal{M}^h)` which calculates $\text{HMA}(X)$, given \mathcal{M}^h . Since the construction of \mathcal{M}^g depends on `Lut` and vice-versa, both tables must be constructed simultaneously, to avoid a deadlock.

<hr/> <p>Procedure BuildMgLut(R_{max})</p> <hr/> <pre> 1 $\mathcal{M}^g \leftarrow \emptyset$; 2 for $R \leftarrow 0$ to R_{max} do 3 $M \leftarrow \text{calc_MA}(B^<(0, R), \mathcal{M}^g)$; 4 foreach $x \in M, x \neq 0$ do 5 $\mathcal{M}^g \leftarrow \mathcal{M}^g \cup (x^g, R)$ </pre> <hr/>	<hr/> <p>Procedure BuildLut(R_{max})</p> <hr/> <pre> 1 foreach $v^g \in \mathcal{M}_{R_{max}}^g$ do 2 for $R \leftarrow 0$ to R_{max} do 3 $Lut[v^g, R] \leftarrow 0$; 4 foreach $x \in \text{SQD}_n(R)$ do 5 $Lut[v^g, R] \leftarrow$ 6 $\max\{Lut[v^g, R], (x + v^g)^2\}$; </pre> <hr/>
<hr/> <p>Procedure BuildMhLut(R_{max})</p> <hr/> <pre> 1 $\mathcal{M}^h \leftarrow \emptyset$; 2 $R \leftarrow 0$; 3 while $R \leq R_{max}$ do 4 for $i \leftarrow 0$ to n do 5 Let $x \in E_i$; 6 $H \leftarrow$ 7 $\text{calc_HMA}(N_n(B^<(x, R)), \mathcal{M}^h)$; 8 foreach $y \in H, y \neq x$ do 9 $\mathcal{M}^h \leftarrow \mathcal{M}^h \cup ((y - x)^g; R)$ 10 $R \leftarrow R^+$; </pre> <hr/>	<hr/> <p>Procedure BuildSQD2(N)</p> <hr/> <pre> 1 $n \leftarrow \lceil \sqrt{N} \rceil$; 2 for $i \leftarrow 0$ to N do $\text{SQD}_2[i] \leftarrow 0$; 3 for $x \leftarrow 0$ to n do 4 for $y \leftarrow 0$ to x do 5 $i \leftarrow x^2 + y^2$; 6 if $i \leq N$ then 7 $\text{SQD}_2[i] \leftarrow \text{SQD}_2[i] \cup \{(x, y)\}$ </pre> <hr/>

B Proof of Proposition 3

In this section we extend the proof of Proposition 3 for the 3D case.

Let $z = (z_1, z_2, z_3) \in A$. Without loss of generality, suppose that $z_1 - x_1 \geq z_2 - x_2 \geq z_3 - x_3 \geq 0$.

Case 1. If $z_3 - x_3 \geq 1$ (thus $z_2 - x_2 \geq 1$ and $z_1 - x_1 \geq 1$), then set $a'' = (z_1 - 1, z_2, z_3)$, $b'' = (z_1, z_2 - 1, z_3)$, $c'' = (z_1, z_2, z_3 - 1)$, $d'' = (z_1 - 1, z_2 - 1, z_3)$, $e'' = (z_1 - 1, z_2, z_3 - 1)$, $f'' = (z_1, z_2 - 1, z_3 - 1)$, $g'' = (z_1 - 1, z_2 - 1, z_3 - 1)$. Obviously $a'', b'', c'', d'', e'', f'', g'', z$ are all in A , furthermore at least one of these 8 points belongs to E_n .

Case 2. If $z_3 - x_3 = 0$ and $z_2 - x_2 \geq 1$ (thus and $z_1 - x_1 \geq 1$), then set $a' = (z_1 - 1, z_2, z_3)$, $b' = (z_1, z_2 - 1, z_3)$, $c' = (z_1, z_2, z_3 + 1)$, $d' = (z_1 - 1, z_2 - 1, z_3)$, $e' = (z_1 - 1, z_2, z_3 + 1)$, $f' = (z_1, z_2 - 1, z_3 + 1)$, $g' = (z_1 - 1, z_2 - 1, z_3 + 1)$. It can easily be seen that a', b', d', e', f', g' are all in A , as well as z . If c is also in A or if $\{z, a', b', d', e', f', g'\} \cap E_n \neq \emptyset$ (equivalent to $c' \notin E_n$) then we are done, suppose that $c' \notin A$ and that $c' \in E_n$. From $z \in A$ and $c' \notin A$ we deduce that $(z_1 - x_1)^2 + (z_2 - x_2)^2 \leq R$ and $(z_1 - x_1)^2 + (z_2 - x_2)^2 + 1 > R$, thus $(z_1 - x_1)^2 + (z_2 - x_2)^2 = R$.

From our hypothesis, there exists $y \in E_n(A)$ such that $(y - x)^2 = (y_1 - x_1)^2 + (y_2 - x_2)^2 + (y_3 - x_3)^2 = R$, with y_1, y_2, y_3 all even. From $c' \in E_n$, we deduce that z_1 and z_2 are even, and that z_3 is odd. Since $z_3 - x_3 = 0$, x_3 is also odd.

In all cases, if both x_1 and x_2 are even, or if both x_1 and x_2 are odd, or if one is even and the other is odd, we reach a contradiction (R both even and odd).

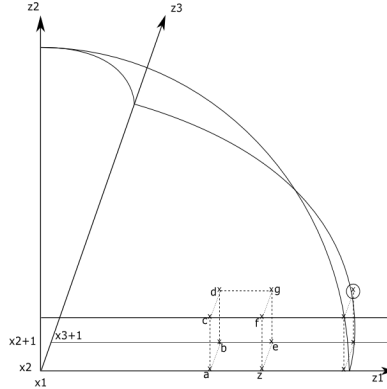


Fig. 8. Illustration for the proof of Proposition 3 in 3D.

Case 3. If $z_3 - x_3 = z_2 - x_2 = 0$, then set $a = (z_1 - 1, z_2, z_3)$, $b = (z_1 - 1, z_2, z_3 + 1)$, $c = (z_1 - 1, z_2 + 1, z_3)$, $d = (z_1 - 1, z_2 + 1, z_3 + 1)$, $e = (z_1, z_2, z_3 + 1)$, $f = (z_1, z_2 + 1, z_3 - 1)$, $g = (z_1, z_2 + 1, z_3 + 1)$ (see Figure 8). Let $l_1 = z_1 - x_1$, and let $r = R - 2$.

If $l_1^2 \leq r$, then we have the same argument as in case 1, otherwise $r = R - 2 < l_1^2 \leq R$ thus $l_1^2 = R$ or $l_1^2 = R - 1$.

Suppose $l_1^2 = R$: in this case, $\{z, a, b, c, d\} \subset A$ but $\{e, f, g\} \cap A = \emptyset$. If $\{z, a, b, c, d\} \cap E_n \neq \emptyset$ then we are done, suppose $\{z, a, b, c, d\} \cap E_n = \emptyset$.

- if $f \in E_n$ (idem $e \in E_n$): thus z_1 even, $x_2 = z_2$ odd, $x_3 = z_3$ even.
 l_1 even $\Rightarrow x_1$ even, thus $(x - y)^2 = (x_1 - y_1)^2 + (x_2 - y_2)^2 + (x_3 - y_3)^2 = R = l_1^2$ means $even + odd + even = even$, a contradiction.
 l_1 odd $\Rightarrow x_1$ odd, thus $(x - y)^2 = l_1^2$ means $odd + odd + even = odd$, a contradiction.
- if $g \in E_n$: thus z_1 even, $x_2 = z_2$ odd, $x_3 = z_3$ odd.
 l_1 even $\Rightarrow x_1$ even, thus $(x - y)^2 = l_1^2$ is of the form $(2\alpha)^2 + (2\beta + 1)^2 + (2\gamma + 1)^2 = (2\delta)^2$, which is impossible since the left term is congruent to 2 modulo 4 and the right term is congruent to 0 modulo 4.

l_1 odd $\Rightarrow x_1$ odd, thus $(x-y)^2 = l_1^2$ is of the form $(2\alpha+1)^2 + (2\beta+1)^2 + (2\gamma+1)^2 = (2\delta+1)^2$, which is impossible since the left term is congruent to 3 modulo 4 and the right term is congruent to 1 modulo 4.

Suppose $l_1^2 = R-1$: in this case, $\{z, a, b, c, d, e, f\} \subset A$ but $g \notin A$. If $\{z, a, b, c, d, e, f\} \cap E_n \neq \emptyset$ then we are done, suppose $\{z, a, b, c, d, e, f\} \cap E_n = \emptyset$. Thus $g \in E_n$, which implies z_1 even, $x_2 = z_2$ odd and $x_3 = z_3$ odd.

- l_1 even $\Rightarrow l_1^2$ even, hence x_1 even and R odd. Thus $(x-y)^2 = R$ means *even + odd + odd = odd*, a contradiction.
- l_1 odd $\Rightarrow l_1^2$ odd, hence x_1 odd and R even. Thus $(x-y)^2 = R$ means *odd + odd + odd = even*, a contradiction.