How to obtain a lattice basis from a discrete projected space

Nicolas Normand, Myriam Servières, Jean-Pierre Guédon

How to obtain a lattice basis from a discrete projected space

Nicolas Normand

IRCCyN/IVC UMR CNRS 6597

Abstract. Euclidean spaces of dimension n are characterized in discrete spaces by the choice of lattices. The goal of this paper is to provide a simple algorithm finding a lattice onto subspaces of lower dimensions onto which these discrete spaces are projected. This first obtained by depicting a tile in a space of dimension n – 1 when starting from an hypercubic grid in dimension n. Iterating this process across dimensions gives the final result.

```
@inproceedings{normand2005dgci,
  Author = {Normand, Nicolas and Servi{\'e}res, Myriam and Gu{\'e}don, JeanPierre},
  Booktitle = {Discrete Geometry for Computer Imagery},
  Date = {2005-04},
  Doi = {10.1007/b135490},
  Editor = {Andres, {\'E}ric and Damiand, Guillaume and Lienhardt, Pascal},
  Isbn = {3-540-25513-3},
  Month = apr,
  Pages = {153-160},
  Publisher = {Springer Berlin / Heidelberg},
  Series = {Lecture Notes in Computer Science},
  Title = {How to obtain a lattice basis from a discrete projected space},
  Volume = {3429},
  Year = {2005}}
```

The original publication is available at www.springerlink.com

How to Obtain a Lattice Basis from a Discrete Projected Space

Nicolas Normand, Myriam Servières and JeanPierre Guédon

IRCCyN/IVC, École polytechnique, University of Nantes
Rue Christian Pauc, 44306 Nantes

Abstract. Euclidean spaces of dimension n are characterized in discrete spaces by the choice of lattices. The goal of this paper is to provide a simple algorithm finding a lattice onto subspaces of lower dimensions onto which these discrete spaces are projected. This first obtained by depicting a tile in a space of dimension $n-1$ when starting from an hypercubic grid in dimension n. Iterating this process across dimensions gives the final result.

1 Introduction

Regular lattices constitute the cornerstone for the building of discrete geometry tools and also for bases of classical continuous space of functions. Of course, these regular lattices can be defined without any outside reference. However, the definition of the resulting lattice is not obvious when a problem is designed in a discrete space and when it is mandatory to go back and forth from this first space to an other discrete space using a given discrete transform. When the same problem is entirely defined in a discrete manner, the lattice identification problem can become even harder. This paradigm was used to construct a cryptographic/signature scheme using the NTRU lattice [1].In this case, the lattice identification leads to an NP-problem.

Lattice identifications have also been investigated by Conway and Sloane for sphere packing which results are mainly employed for vector quantization in the multimedia coding area [2]. In Sect. 2, the starting point to review the literature will lie into the continuous/discrete correspondence firstly established by Shannon and generalized by Unser-Aldroubi. This work allows to start with a basis through a tensorial product, to sample the continuous space to give a lattice onto which a Riesz functional basis will be defined.

The aim of this paper is then to demonstrate how to obtain an unitary tile with a regular lattice on the projection hyperplane with discrete projection directions. This will be performed in a general manner in Sect. 3. The fact that we restrict the projection operator to discrete projection is based on the attempt to get a simple way to obtain a lattice onto the hyperplane. The difficulty is then to extract the lattice from regular projection grids, *i.e.* not to oversample the hyperplane grid with unused points nor to undersample a grid from which the lattice would not be obtained.

In other words, each point of the discrete projection plane must have a predecessor in the initial space and each point of the initial lattice is projected onto an existing point.

2 Related Work

Starting with the construction of orthonormal bases that give regular tiling leads to the Gram-Schmidt orthonormalisation procedure that can be found in almost any algebra textbook [3]. Because of the normalization, the resulting basis can be easily discretised and replicated to give a regular tiling.

Following this path (starting from the continuous point of view and discretizing afterward) any n dimensional continuous space will give regular tiling from this unconstrained orthonormal continuous grid. As a matter of fact, Unser and Aldroubi have generalized the Shannon-Whittaker-Kotelnikov Sampling Theorem starting with this n-dimensional orthogonal basis then lattice [4, 5]. The initial purpose of this theorem is to use other functional bases than the Riesz bases $\{(\mathrm{sinc}\,(\mathrm{kx}), k \in \mathbb{Z})\}$.

This theorem is described in Fig. 1

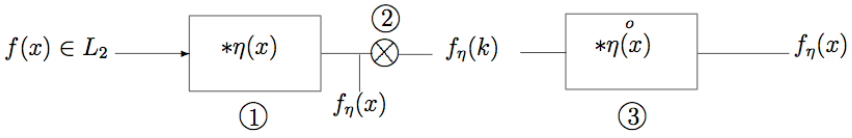

Fig. 1. Representation of the Unser-Aldroubi theorem

The first step corresponds to the orthogonal projection of the L_2 function $f(x)$ onto a closed subspace of functions generated by a Riesz basis $\{\eta(kx), k \in \mathbb{Z}\}$. In other words, these functions already need to be defined from a tiling (the first versions of the theorem corresponds to cardinal functions as the sinc for Shannon or cardinal splines for Unser-Aldroubi).

The second step also uses the same tiling but explicitly since it just picks up the values onto the tiling and throw out the rest of the continuous functions.

The third step re-generates this previous continuous function from three different informations:

1. the dual functional basis $\mathring{\eta}$ (defined onto the tile)
2. the sample $f_\eta(k)$ (defined onto the tile)
3. the tile which allows to perform the discrete convolution that lies onto the box 3.

There are two major points with this great theorem:

1. The tiling is the subsequent material that links continuous and discrete words. The strength of this theorem is to allow to work only into a discrete word $f_\eta(k)$ and go back into a continuous word only when mandatory.
2. The only tilling known to allow the conditions of the theorem are obtained by tensorial products over higher dimensions. In other words, the Riesz basis structure in one dimension $\{\eta(k-x), k \in \mathbb{Z}\}$ can not be used in two dimensions as $\{\eta(\sqrt{((k-l)^2+(l-y)^2)}), (k,l) \in \mathbb{Z}^2\}$ but the only known extension is $\{\eta(k-l).\eta(l-y), (k,l) \in \mathbb{Z}^2\}$. In this latter extension, Fig. 1 where x is a n-dimensional vector still holds.

As a consequence using specific discrete operator (in our case a projector operator) between step 2 and step 3 must be done with a correspondence between grids not to loose information and the benefits of the theorem. This correspondance has been applied for the continuous and discrete Radon transforms defined into spline spaces leading to new filtered backprojection algorithms [7, 8].

3 Obtaining a Tile in a m-Dimensional Space from a n-Dimensional Space

3.1 From n-Dimension to $(n-1)$-Dimension

The initial space $\mathcal{L}$ is a lattice in a Euclidean space. This n-dimensional discrete space can be seen as the regular sampling of a continuous n-dimensional space structured by a hypercubic grid $\{i_1, \ldots, i_n\}$. Each point $(b_1, \ldots, b_n) \in \mathbb{Z}^n$ in the discrete space corresponds to the point $b_1 \times i_1 + \ldots + b_n \times i_n$ in the continuous space (each lattice point is described by a n-dimensional vector $b = \{b_1, \ldots, b_n\}$ relative to the lattice basis $\{i_1, \ldots, i_n\}$). The continuous space is translation invariant according to any vector i_m or any integer combination of vectors $i_1, \ldots, i_n$.

By projecting the initial n-dimensional space along a line direction, we create a $(n-1)$-dimensional hyperplane. It can be easily seen (Fig. 2) that if the line direction is discrete (an integer combination of $i_1, \ldots, i_n$), then the hyperplane has a regular discrete structure: it is also a lattice. It is translation-invariant along any integer combination of $i'_1, \ldots, i'_n$, where each i'_m is the projection of i_m on the hyperplane. However, the set $\{i'_1, \ldots, i'_n\}$ is not a base (its dimension is $n-1$) and a $n-1$-vector subset does not generally define a tile.

The purpose is to extract a $n-1$-vector basis from $\{i'_1, \ldots, i'_n\}$ that defines a lattice basis for the projected hyperplane. Equivalently, it will lead to a discrete $(n-1) \times n$ projection matrix.

The proposed method will conceptually use the set of vectors $\{i'_1, \ldots, i'_n\}$, obtained by projecting $\{i_1, \ldots, i_n\}$ along the line direction $(v_1, \ldots, v_n)$ onto the hyperplane. The relationship that links these vectors together is given by the projection direction:

$$v_1 \times i'_1 + \ldots + v_n \times i'_n = 0 \ . \tag{1}$$

In the following, we will assume that the subset $\{i'_1, \ldots, i'_{n-1}\}$ is a vector basis (*i.e.* that i'_n is a linear combination of these vectors). Hence, $i'_1, \ldots, i'_{n-1}$

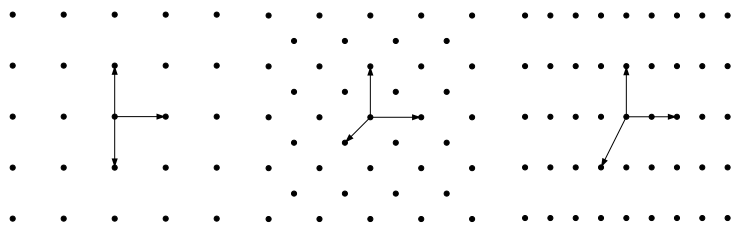

Fig. 2. Some examples of 3D projected grids with projection directions $(0, 1, 1)$, $(1, 1, 2)$ and $(1, 2, 2)$

generates the continuous projected hyperplane. This is always true except when the last component of the projection direction, v_n, is zero. In this particular case, (1) creates a linear dependence between the vectors $i'_1, \ldots, i'_{n-1}$. But since the projection direction is not the null vector, there is at least one non-zero v_m component. The previous assumption can be ensured by permuting the vectors twice: before applying the method in order to put i'_m at the end and after applying the method to put the vectors back in the initial order.

The method iteratively creates a set of lattice basis $(j_1, \ldots, j_k)$ with increasing dimension k. Each intermediate basis $(j_1, \ldots, j_k)$ generates the part of $\mathcal{L}$ contained in the space spanned by $(i'_1, \ldots, i'_k)$. At step k, the $k-1$ previously found vectors build a tile *i.e.* a parallelepiped which vertices correspond to projected discrete points and which interior does not contain any discrete points.

First Basis Vector. The first vector j_1 is chosen following the i'_1 direction from the origin point O. The end point of j_1 is the visible point in i'_1 direction (the closest point from O in this direction). Since the dimension of the projection matrix is $n-1$ for a line projection, there are exactly two linearly independant ways to follow this direction, either with i'_1 or with a linear combination of $i'_2, \ldots, i'_n$ according to (1):

$$v_1 \times i'_1 = -v_2 \times i'_2 - \ldots - v_n \times i'_n \ . \tag{2}$$

The second term of this equation can be written as an integral linear combination with a division by the greatest common divisor of its coefficients:

$$\frac{v_1}{\gcd(v_2, \ldots, v_n)} \times i'_1 = -\frac{v_2 \times i'_2 + \ldots + v_n \times i'_n}{\gcd(v_2, \ldots, v_n)} \ . \tag{3}$$

All the linear combinations of i'_1 and $v_1 i'_1 / \gcd(v_2, \ldots, v_n)$ are obviously collinear to i'_1. The visible point from the origin O in this direction is given by the minimal linear combination with integer coefficients. Let's remark that $\frac{\gcd(v_2,\ldots,v_n)}{\gcd(v_1,\ldots,v_n)}$ and $\frac{v_1}{\gcd(v_1,\ldots,v_n)}$ are integers and relatively prime. Following the Bézout's theorem, there exist $\alpha_1, \beta_1 \in \mathbb{Z}$ such that:

$$\alpha_1 \times \frac{\gcd(v_2,\ldots,v_n)}{\gcd(v_1,\ldots,v_n)} + \beta_1 \times \frac{v_1}{\gcd(v_1,\ldots,v_n)} = 1$$
$$\alpha_1 + \beta_1 \frac{v_1}{\gcd(v_2,\ldots,v_n)} = \frac{\gcd(v_1,\ldots,v_n)}{\gcd(v_2,\ldots,v_n)} \quad . \tag{4}$$

The minimal integral combination of i'_1 and $\frac{v_1 i'_1}{\gcd(v_1,\ldots,v_n)}$ is then chosen as the first vector of the projected lattice basis:

$$j_1 = \frac{\gcd(v_1,\ldots,v_n)}{\gcd(v_2,\ldots,v_n)} i'_1 \quad .$$

From α_1 and β_1 (obtained with the extended Euclidean algorithm) we can find two points that project onto j_1:

$$A_1 = \left(\alpha_1, -\beta_1 \frac{v_2}{\gcd(v_2,\ldots,v_n)}, \ldots, -\beta_1 \frac{v_n}{\gcd(v_2,\ldots,v_n)}\right) \quad ,$$
$$B_1 = \left(\alpha_1 + \beta_1 \frac{v_1}{\gcd(v_2,\ldots,v_n)}, \underbrace{0,\ldots,0}_{n-1}\right) \quad . \tag{5}$$

Conversely to B_1, A_1 always has integer components and thus belongs to $\mathcal{L}$.

The k^{th} Basis Vector. Let assume that vectors j_1 to j_{k-1} have already been found. The lattice spanned by $(j_1,\ldots,j_{k-1})$ is the subset of $\mathcal{L}$ restricted to the continuous subspace generated by $(i'_1,\ldots,i'_{k-1})$.

The vector i'_k introduces a new dimension because $i'_1,\ldots,i'_k$ are linearly independent. j_k must have the smallest non null component in this new direction. There are two independent ways to move along i'_k, following i'_k itself or a linear combination of $i'_{k+1},\ldots,i'_n$ according to (1):

$$\frac{v_1 i'_1 + \ldots + v_k i'_k}{\gcd(v_{k+1},\ldots,v_n)} = -\frac{v_{k+1} i'_{k+1} + \ldots + v_n i'_n}{\gcd(v_{k+1},\ldots,v_n)} \quad . \tag{6}$$

The closeness of the hyperplanes to the origin is measured by the projection onto i'_k and gives respectively 1 and $\frac{v_k}{\gcd(v_{k+1},\ldots,v_n)}$. The minimum integral combination is given by α_k and β_k:

$$\alpha_k + \beta_k \frac{v_k}{\gcd(v_{k+1},\ldots,v_n)} = \frac{\gcd(v_k,\ldots,v_n)}{\gcd(v_{k+1},\ldots,v_n)} \quad . \tag{7}$$

The new basis vector j_k is directly derived:

$$j_k = \alpha_k i'_k + \beta_k \frac{v_1 i'_1 + \ldots + v_k i'_k}{\gcd(v_{k+1},\ldots,v_n)} \quad . \tag{8}$$

Two antecedents of j_k can be obtained by:

$$A_k = \left(\underbrace{0,\ldots,0}_{k-1}, \alpha_k, -\beta_k \frac{v_{k+1}}{\gcd(v_{k+1}..v_n)}, \ldots, -\beta_k \frac{v_n}{\gcd(v_{k+1}..v_n)} \right) \quad ,$$

$$B_k = \left(\frac{\beta_k v_1}{\gcd(v_{k+1}..v_n)}, \ldots, \frac{\beta_k v_{k-1}}{\gcd(v_{k+1}..v_n)}, a_k + \frac{\beta_k v_k}{\gcd(v_{k+1}..v_n)}, \underbrace{0,\ldots,0}_{n-k} \right) \quad .(9)$$

Projection Matrix. Any point $M(a_1,\ldots,a_n)$ in $\mathcal{L}$ is projected on the hyperplane to a point $p(M) = M'$ with integer coordinates $(b_1,\ldots,b_{n-1})$ in the $(j_1,\ldots,j_{n-1})$ basis. The preimage of M' is the set of points in $\mathcal{L}$ that are aligned with M relative to the projection direction V. These points can be reached from the known point $b_1A_1 + \ldots + b_{n-1}A_{n-1}$:

$$p^{-1}(M') = \{m | p(m) = M'\} = \left\{ b_1A_1 + \ldots + b_{n-1}A_n + k\frac{V}{\gcd(v_1..v_n)}, k \in \mathbb{Z} \right\} \quad . \tag{10}$$

$(A_1,\ldots,A_{n-1}, V/\gcd(v_1..v_n))$ is a basis of the initial lattice $\mathcal{L}$. An extra row corresponding to the direction of the projection is added:

$$\begin{aligned} A &= \left[A_1 | \ldots | A_{n-1} | \frac{V}{\gcd(v_1..v_n)} \right] \\ &= \begin{bmatrix} \alpha_1 & 0 & \ldots & 0 & \frac{v_1}{\gcd(v_1..v_n)} \\ -\beta_1 \frac{v_2}{\gcd(v_2..v_n)} & \alpha_2 & \ddots & \vdots & \\ -\beta_1 \frac{v_3}{\gcd(v_2..v_n)} & -\beta_2 \frac{v_3}{\gcd(v_3..v_n)} & \ddots & 0 & \vdots \\ \vdots & & & \alpha_{n-1} & \frac{v_{n-1}}{\gcd(v_1..v_n)} \\ -\beta_1 \frac{v_n}{\gcd(v_2..v_n)} & -\beta_2 \frac{v_n}{\gcd(v_3..v_n)} & \ldots & -\beta_{n_1} \frac{v_n}{\gcd(v_{n-1},v_n)} & \frac{v_n}{\gcd(v_1..v_n)} \end{bmatrix} \end{aligned} \quad . \tag{11}$$

$$P = [Id_{n-1}|0].A^{-1} \quad . \tag{12}$$

Figure 3 pictures the results of our algorithm for a simple 3D to 2D projection of angle direction $(6, 10, 15)$. The projection matrix is given by:

$$P = \begin{bmatrix} 5 & 6 & -6 \\ 0 & 3 & -2 \end{bmatrix} \quad ,$$

and

$$A = \begin{bmatrix} -1 & 0 & 6 \\ -2 & 1 & 10 \\ -3 & 1 & 15 \end{bmatrix} \quad .$$

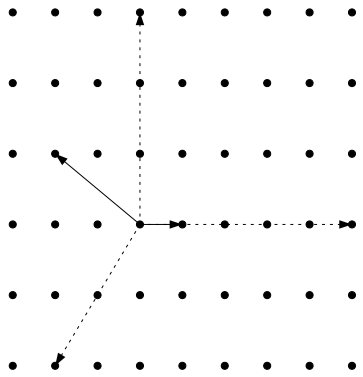

Fig. 3. The result of the projection of a 3D lattice with angle direction $(6, 10, 15)$. The three dashed lines vectors represent the projection of the initial 3D basis vectors whereas the two plain lines vectors are the result of the computed lattice

3.2 From $(n-1)$-Dimension to m-Dimension

To go from a n-dimensional space to a m-dimensional space ($m \geq 1$), there are $(n-m)$ projection directions V:

$$V = \begin{bmatrix} v_{1,1} & \dots & v_{1,n} \\ \vdots & & \vdots \\ v_{n-m,1} & \dots & v_{n-m,n} \end{bmatrix} . \tag{13}$$

The described method is followed along the first direction:

$$V_1 = [v_{1,1} \ \dots \ v_{1,n}] \ , \tag{14}$$

and gives the transformation of the basis $(i_1, \dots, i_n)$ to $(j_1, \dots, j_{n-1})$. Each $V_i, i \in \{2, \dots, (n-m)\}$ is projected onto $(j_1, \dots, j_{n-1})$. They give the projection directions in the $(n-1)$-dimensional space with the $(j_1, \dots, j_{n-1})$ basis. The process is iterated to reach a m-dimensional space.

4 The Projection Matrix

We will define the projection matrix from a n-dimensional space onto a m-dimensional space on the regular grid defined before.

To obtain the final projection matrix, the projection directions can be followed in different order. One projection direction is chosen, the other projection directions are projected following this first direction and the projection matrix following this direction is derivated. In the projected direction, an other direction is chosen and the same process is iterated. Finally the projection matrix

from the n-dimensional space to the m-dimensional space is obtained by putting together the intermediate matrix.

To go from a n-dimensional space to an m-dimensional space ($m \geq 1$), there are $(n - m)$ projection directions V_k.

To obtain the projection matrix from a n-dimensional to an m-dimensional space we will calculate the projection matrix step by step by lowering the dimension. The final nD to mD projection matrix is composed by products of all the projection matrices describing hyperplane lattices. This matrix being the product of integer matrices has only integer coefficients.

5 Conclusion

Tiling a discrete projected space from higher dimensional Euclidean spaces was the subject of this paper. We first demonstrated how to obtain a tile in a $(n - 1)$-dimensional space from the Euclidean hypercubic grid of dimension n. The generalization across dimensions is quite straightforward. The obtained results are directly useful for discrete Radon transforms.

References

1. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman: NTRU A Ring-Based Public Key Cryptosystem. in Algorithmic Number Theory (ANTS III), Portland, OR, June 1998, J.P. Buhler (ed.), Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998, 267-288.
2. John H. Conway and N.J.A. Sloan: Sphere Packings, Lattices and Groups. Springer(1998)
3. Harris, J.W., Stocker, H.: Handbook of Mathematics and Computational Science. Springer(1998)
4. Aldroubi, A., Unser, M: Sampling procedures in function spaces and asymptotic equivalence with Shannonś sampling theory. Numer. Funct. Anal. and Optimiz. **15**(1994)1–21
5. Unser, M., Aldroubi, A., Eden, M.: Polynomial Spline Signal Approximations: Filter Desing and Assymptotic Equivalence with Shannonś Sampling Theorem. IEEE Transaction on Information theory **38**(1992)95–103
6. Guédon, JP., Bizais, Y.: Separable and radial bases for medical image processing. SPIE lmage Processing **1898**(1993)652–661
7. Guédon, JP., Bizais, Y.: Bandlimited and Haar Filtered Back-Projection Reconstuction. IEEE Transaction on Medical Imaging **13**(1994)430–440
8. Guédon, J.P., Unser, M., Bizais, Y.: Pixel Intensity Distribution Models for Filtered Back-Projection. Conference Record of the 1991 IEEE Nuclear Science Symposium and Medical Imaging Conference