MATHEMATICS OF COMPUTATION
Volume 71, Number 237, Pages 319–332
S 0025-5718(01)01331-X
Article electronically published on September 17, 2001

PROVING THE DETERMINISTIC PERIOD BREAKING OF LINEAR CONGRUENTIAL GENERATORS USING TWO TILE QUASICRYSTALS

LOUIS-SÉBASTIEN GUIMOND AND JIŘÍ PATERA

Abstract. We describe the design of a family of aperiodic PRNGs (APRNGs). We show how a one-dimensional two tile cut and project quasicrystal (2TQC) used in conjunction with LCGs in an APRNG generates an infinite aperiodic pseudorandom sequence. In the suggested design, any 2TQC corresponding to unitary quadratic Pisot number combined with either one or two different LCGs can be used.

Introduction

For the past decade, a lot of efforts have been made to build statistically robust pseudorandom number generators (PRNGs) with huge period. Indeed, known PRNGs are periodic and the requirements of today's simulations and Monte Carlo methods motivate the need for PRNGs with extremely large period.

APRNGs are a family of aperiodic PRNGs and were introduced in [3]. Their novelty consists in using *quasicrystals* to combine several PRNGs. *One-dimensional two tile quasicrystals* (2TQCs) are geometrically aperiodic infinite point sets on the real line from which an aperiodic binary sequence can be generated. Unfortunately, this binary sequence has bad statistics since, for instance, it has many more ones than zeroes. In the suggested design, the aperiodic sequence is used to combine two suitable chosen LCGs and form an infinite aperiodic sequence with good statistical behaviour. Indeed, the aperiodic binary sequence is used to break the periodicity of LCGs while LCGs are used to eliminate the nonuniformity of the binary sequence. Implementation and statistical study of APRNGs are not treated here and may be found in [4].

The prime motivation for this research was the use of quasicrystal generation in cryptographic systems [6]. The design and study of the APRNG is a first step in the building of such cryptographic systems.

The paper is organised as follows. In Section 1 we give some basic facts concerning quasicrystals. In Section 2 we describe the suggested design of APRNGs and we state the result from which follows the aperiodicity of a class of APRNGs. Finally, the proofs of our results are given in Section 3. In conclusion, we address some remarks concerning parallelisation and also suggest research avenues.

Received by the editor October 15, 1999 and, in revised form, March 14, 2000.
2000 *Mathematics Subject Classification.* Primary 65C10, 82D99; Secondary 68U99.
Key words and phrases. Aperiodic pseudorandom number generator, Monte Carlo method, linear congruential generator, pseudorandom number generator, quasicrystal, simulation.
This work was supported by NSERC of Canada and FCAR of Québec.

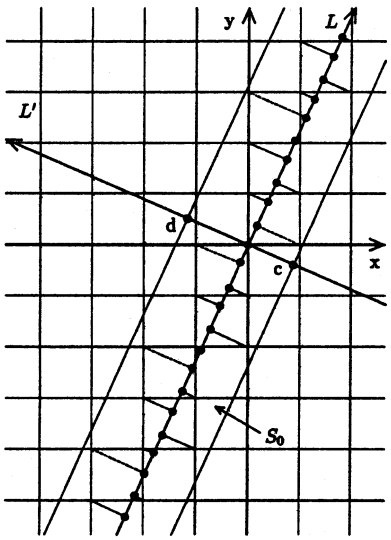

FIGURE 1. One-dimensional quasicrystal with $\beta' < 0$.

1. Quasicrystals

Good introductions to the mathematics of quasicrystals can be found in [1, 2, 11] while the web page [12] provides an introduction to the physics of quasicrystals. This section is a brief summary of the first chapter of Jan Patera's Diploma Thesis [9] on quasicrystals and their computer generation.

In 1984, Schechtman et al. [10] discovered a metallic alloy of aluminium and manganese which had an aperiodic crystalline configuration: the alloy consisted, unlike crystals, in an aperiodic arrangement of atoms. Physicists later found that there were many such alloys which arise from rapid cooling of melted metals. Even though the diffraction patterns of these materials are not periodic in the stronger sense [8], they have a common peculiar structure and are referred to as *generalised crystals*, *aperiodic crystals* or *quasicrystals* in the literature.

To describe the structure of these diffraction patterns, several mathematical models were introduced. In this paper we consider the *cut and project scheme* model which is illustrated in Figure 1. We will only consider one-dimensional quasicrystals[1] obtained from a two-dimensional lattice even though the cut and project scheme can be generalised to any finite-dimension lattices. Multidimensional quasicrystals will be briefly discussed in the conclusion.

Geometrically, a quasicrystal is the projection of a set of points S_0 from a two-dimensional lattice (e.g., $\mathbb{Z}^2$) on a straight line L through the origin of irrational slope β with respect to the orientation of the lattice. The results we obtain in this paper are valid when β is a *unitary quadratic Pisot number*, i.e., when there exists a pair $(m, n) \in \mathbb{Z} \times \{-1, 1\}$ such that $x^2 = mx + n$ has two real solutions the greater of which is β. If β' is the second solution[2] of $x^2 = mx + n$, then $0 < |\beta'| < 1 < \beta = m - \beta'$.

[1] Unless specified otherwise, throughout the paper we refer to quasicrystals as cut and project quasicrystals.

[2] The solutions β and β' are said to be the *algebraic conjugates*.

The set S_0 is defined as follows. Let L' be the line of slope β' passing through the origin; let $\Omega = [c, d)$ be a segment of L'. S_0 is the set of points of the lattice included in the strip $\Omega \times L$ (see Figure 1). For a given β (or equivalently a given line L), Ω is called the *acceptance window* of the quasicrystal $\Sigma(\beta, \Omega)$. The algebraic descriptions of the sets S_0 and $\Sigma(\beta, \Omega)$ are the following:

$$S_0 = \Big\{ X = (a, b) \in \mathbb{Z}^2 \,\Big|\, a + b\beta' \in \Omega \Big\}$$

and

$$\Sigma(\beta, \Omega) = \Big\{ a + b\beta \,\Big|\, (a, b) \in \mathbb{Z}^2 \text{ and } a + b\beta' \in \Omega \Big\}.$$

Let us introduce the following notation:

$$\mathbb{Z}[\beta] = \big\{ a + b\beta \,\big|\, a, b \in \mathbb{Z} \big\},$$

and, if $x = a + b\beta \in \mathbb{Z}[\beta]$,

$$g(x) = a + b\beta'.$$

$g(x)$ is called the *Galois conjugate*[3] of x and is noted $g(x) = x'$.

Proposition 1.1 ([1])**.** *Let $\Sigma(\beta, \Omega)$ be a quasicrystal. $\Sigma(\beta, \Omega)$ has the following properties:*

1. *Shifting property: $\Sigma(\beta, \Omega + \lambda') = \Sigma(\beta, \Omega) + \lambda$, for any $\lambda \in \mathbb{Z}[\beta]$;*
2. *Scaling property: $\Sigma(\beta, \beta^i \Omega) = (\beta')^i \Sigma(\beta, \Omega)$, for any $i \in \mathbb{Z}$.*

Corollary 1.2. *Let $\Sigma(\beta, \Omega)$ be a quasicrystal. Up to shifting and scaling, we can assume $0 \in \Omega = [c, d)$ with $1 \leq d - c < \beta$, $c, d \in \mathbb{R}$.*

(Note: in cases where $n = 1$, the scalings for odd i not only scale the quasicrystal but also flip the direction of the quasicrystal.)

Proposition 1.3 ([7])**.** *Let β a unitary quadratic Pisot number associated to (m, n), and $\Sigma(\beta, \Omega)$ a quasicrystal with $\Omega = [c, d)$, $1 \leq d - c < \beta$. Generically, there exist three possible distances between any two adjacent points in $\Sigma(\beta, \Omega)$. These distances are $1, L(\beta) - 1$ and $L(\beta)$. When $n = 1$ (resp. $n = -1$), there exist m (resp. $m - 1$) limit cases with only two possible distances.*

The expression of $L(\beta)$ is given in [7] (and stated below) along with the limit cases conditions: $d - c = 1$ and $d - c = \beta - j$ for $j = 1, 2, \cdots, m - 1$ when $n = 1$, and $j = 1, 2, \cdots, m - 2$ when $n = -1$. The two possible distances in the limit cases are given below in Corollary 1.7.

Let us use the following notation: $\Sigma(\beta, \Omega) = \{x_i\}_{i \in \mathbb{Z}}$ ($\Sigma(\beta, \Omega)$ is a countable ordered point set). The distances between adjacent points in a quasicrystal are often referred to as *tiles*. Indeed, if $S(\beta) < M(\beta) < L(\beta)$ are the ordered distances, the set $\big\{[x_i, x_{i+1})\big\}_{i=-\infty}^{+\infty}$ defines a covering of the real line having three types of tiles noted S, M and L (for Short, Medium and Long) of length $S(\beta)$, $M(\beta)$ and $L(\beta)$ respectively.

Definition 1.4. Quasicrystals for which there exist exactly three tile types are called *three tile quasicrystals* while the other ones are called *two tile quasicrystals* (2TQCs).

[3] $\mathbb{Q}[\beta]$ is a *Galois extension* of the field $\mathbb{Q}$ and $g(\cdot)$ is an automorphism of $\mathbb{Q}[\beta]$ mapping β (resp. β') to its algebraic conjugate β' (resp. β). For more details see, for instance, [5].

Let, when $n = 1$,

$$\phi_j(\beta) = \begin{cases} \beta - j & \text{for } j = 0, 1, \cdots, m-1, \\ 1 & \text{for } j = m \end{cases}$$

and, when $n = -1$,

$$\phi_j(\beta) = \begin{cases} \beta - j + 1 & \text{for } j = 1, 2, \cdots, m-1, \\ 1 & \text{for } j = m. \end{cases}$$

Then $\phi_{j+1}(\beta) < \phi_j(\beta)$ and

$$\bigcup_{j<m} \big[\phi_{j+1}(\beta), \phi_j(\beta)\big) = [1, \beta).$$

Each $\phi_j(\beta)$ corresponds to one of the limit cases conditions referred to in Proposition 1.3, except for $\phi_0(\beta)$ when $n = 1$ and $\phi_1(\beta)$ when $n = -1$.

Definition 1.5. We say that a quasicrystal is of type $\mathcal{I}$ if $d-c \in \big[\phi_m(\beta), \phi_{m-1}(\beta)\big) = \big[1, \phi_{m-1}(\beta)\big)$. Otherwise, we say it is of type $\mathcal{II}$.

Proposition 1.6. *Let $c, d \in \mathbb{R}$, $1 \le d - c < \beta$. Define Σ_1, Σ_{L-1} and Σ_L as the following sets:*

$$\Sigma_1 = \big\{x_i \in \Sigma(\beta, \Omega) \mid x_{i+1} - x_i = 1\big\},$$
$$\Sigma_{L-1} = \big\{x_i \in \Sigma(\beta, \Omega) \mid x_{i+1} - x_i = L(\beta) - 1\big\},$$
$$\Sigma_L = \big\{x_i \in \Sigma(\beta, \Omega) \mid x_{i+1} - x_i = L(\beta)\big\}.$$

If $d - c$ is such that $\phi_{j+1}(\beta) \le d - c < \phi_j(\beta)$, the following equalities hold:

$$\Sigma_1 = \Big\{x \in \mathbb{Z}[\beta] \mid x' \in \Omega_1 = \big[c, d-1\big)\Big\},$$
$$\Sigma_{L-1} = \Big\{x \in \mathbb{Z}[\beta] \mid x' \in \Omega_{L-1} = \big[c+1-L'(\beta), d\big)\Big\},$$
$$\Sigma_L = \Big\{x \in \mathbb{Z}[\beta] \mid x' \in \Omega_L = \big[d-1, c+1-L'(\beta)\big)\Big\}.$$

Proof. From the remark preceding Proposition 1.6, there exists a unique j such that $\phi_{j+1}(\beta) \le d - c < \phi_j(\beta)$. Moreover, $L'(\beta) = 2 - \phi_j(\beta)$ (follows from [7, Propositions 3.4 and 3.5]).

Let $S(\beta) < M(\beta) < L(\beta)$ be the three ordered tile lengths.[4] The generation of point $x_{i+1} \in \Sigma(\beta, \Omega)$, the right neighbour of $x_i \in \Sigma(\beta, \Omega)$, can be done as follows:

Step 1: If $x_i' + S'(\beta) \in \Omega$, then $x_{i+1} = x_i + S(\beta)$.
Step 2: If $x_i' + S'(\beta) \notin \Omega$ and $x_i' + M'(\beta) \in \Omega$, then $x_{i+1} = x_i + M(\beta)$.
Step 3: Otherwise, $x_{i+1} = x_i + L(\beta)$.

We need only consider the following cases.

I. Let $x_i \in \Sigma_1$; then

$$c \le x_i' = x_{i+1}' - 1 < d - 1,$$

i.e., $x_i' \in \big[c, d-1\big)$.
Conversely, let $x_i' \in \big[c, d-1\big)$; then

$$x_i' + 1 \in \big[c+1, d\big) \subseteq \Omega$$

[4] If $n = -1$ and $j = 1$, $S(\beta) = L(\beta) - 1$, $M(\beta) = 1$; otherwise $S(\beta) = 1$ and $M(\beta) = L(\beta) - 1$ (see [7, Propositions 3.4 and 3.5]).

and $x_i \in \Sigma_1$. Indeed, either $S(\beta) = 1$ in which case the result follows from step 1, or $j = 1 = -n$, $S(\beta) = L(\beta) - 1$ and

$$x'_i + S'(\beta) = x'_i + L'(\beta) - 1 < d - 2 + L'(\beta) = d - \phi_1(\beta) < d + c - d = c,$$

i.e., $x'_i + S'(\beta) \notin \Omega$ and the result follows from step 2.

II. Let $x_i \in \Sigma_{L-1}$; then

$$c + 1 - L'(\beta) \le x'_i = x'_{i+1} + 1 - L'(\beta) < d,$$

i.e., $x'_i \in \big[c + 1 - L'(\beta), d\big)$.
Conversely, let $x'_i \in \big[c + 1 - L'(\beta), d\big)$; then

$$x'_i - 1 + L'(\beta) \in \big[c, d - 1 + L'(\beta)\big)$$

and $x_i \in \Sigma_{L-1}$. Indeed, either $S(\beta) = L(\beta) - 1$, in which case the result follows from step 1, or $S(\beta) = 1$ and

$$x'_i + 1 \ge c + 2 - L'(\beta) = c + \phi_j(\beta) > c + d - c = d,$$

i.e., $x'_i + 1 \notin \Omega$ and the result follows from step 2.

□

Corollary 1.7. *Let $\Sigma(\beta, \Omega)$ be a 2TQC.*

1. *If $\Sigma(\beta, \Omega)$ is of type $\mathcal{I}$, then $\Sigma_1 = \emptyset$: the possible tile lengths are $L(\beta) - 1$ and $L(\beta)$.*
2. *If $\Sigma(\beta, \Omega)$ is of type $\mathcal{II}$, then $\Sigma_{L-1} = \emptyset$: the possible tile lengths are 1 and $L(\beta)$.*

Definition 1.8. Let $\Sigma(\beta, \Omega)$ be a quasicrystal such that $1 \le d - c < \beta$. The *stepping function* $f : \Omega \to \Omega$ is a function such that, for all $i \in \mathbb{Z}$, if $x_i \in \Sigma(\beta, \Omega)$, then $x'_{i+1} = f(x'_i)$.

The function f is called the "stepping function" since it walks (in the acceptance window Ω) from the Galois conjugate x'_i of a quasicrystal point x_i to the Galois conjugate x'_{i+1} of the adjacent quasicrystal point to the right of x_i (see Figure 2).

Corollary 1.9. *Let $\Sigma(\beta, \Omega)$ be a quasicrystal such that $1 \le d - c < \beta$. Then the stepping function $f : \Omega \to \Omega$ is given by*

$$f(x') := \begin{cases} x' + 1 & \text{for } x' \in \Omega_1, \\ x' + L'(\beta) - 1 & \text{for } x' \in \Omega_{L-1}, \\ x' + L'(\beta) & \text{for } x' \in \Omega_L. \end{cases} \tag{1.1}$$

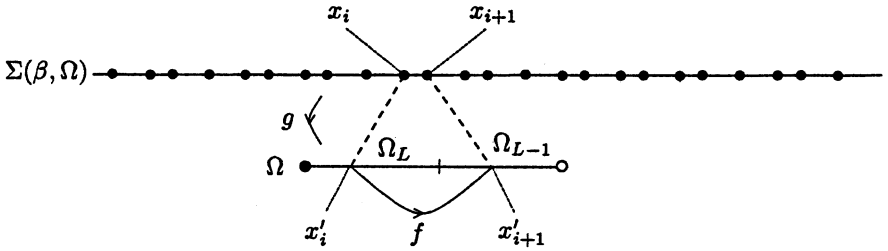

FIGURE 2. Stepping function f for a two tile quasicrystal $\Sigma(\beta, \Omega)$ of type $\mathcal{I}$.

2. Design of APRNGs

We describe the present design of APRNGs based on one 2TQC and two LCGs. The aperiodicity of the generated sequence is stated in Theorem 2.1 which is proven in Section 3.

The construction of the aperiodic sequence $\{n_i\}_{i=0}^{\infty}$ of pseudorandom numbers in $[0,1)$ uses an aperiodic binary sequence $S(\beta,\Omega)$ (obtained from a subset of the 2TQC $\Sigma(\beta,\Omega)$) to combine two (possibly identical) LCGs, LCG_1 and LCG_2.

- Let $\Sigma(\beta,\Omega)$ be a two tile quasicrystal with tile lengths $O(\beta)$ and $L(\beta)$.[5] The aperiodic binary sequence $S(\beta,\Omega)$ is constructed from the tiling generated by $\Sigma(\beta,\Omega)$ on the right of a seed point x_0:

$$S(\beta,\Omega) = \{s_i\}_{i=0}^{\infty}, \tag{2.1}$$

  where the elements s_i are defined, for $i \geq 0$, by the recursive relation:

$$s_i = \begin{cases} 0 & \text{if } x_{i+1} - x_i = O(\beta), \\ 1 & \text{if } x_{i+1} - x_i = L(\beta), \end{cases}$$

  with x_{i+1} the right neighbour of x_i in $\Sigma(\beta,\Omega)$.

- For $j = 1, 2$, let $(a_j, c_j, m_j, k_0^{(j)})$ be the parameters of LCG_j, where a_j is the multiplier, c_j the increment, m_j the modulus and $k_0^{(j)}$ the seed point. Let $K^{(j)}$ be the set of positive integers generated by LCG_j:

$$K^{(j)} = \{k_i^{(j)}\}_{i=0}^{\infty},$$

  where the elements $k_i^{(j)}$ are defined by the recursive relation:

$$k_i^{(j)} = a_j k_{i-1}^{(j)} + c_j \pmod{m_j} \quad i \geq 1.$$

The incrementation of the LCGs is done in the following way. Using the binary sequence $S(\beta,\Omega)$ and starting at $i = 0$, the state of LCG_1 (resp. LCG_2) is incremented by one at step i if $s_i = 1$ (resp. $s_i = 0$). Therefore, the state of LCG_j is given, at any level ℓ in $S(\beta,\Omega)$, by the number of 1's that occur in the finite sequence $\{s_i\}_{i=0}^{\ell}$. This number is denoted $\rho_\ell(\beta,\Omega)$:

$$\rho_\ell(\beta,\Omega) = \big|\{s_i \in S(\beta,\Omega) \mid i = 0, 1, \cdots, \ell \text{ and } s_i = 1\}\big|.$$

The pseudorandom numbers $n_i \in [0,1)$ are defined as follows (see Figure 3):

$$n_i = \begin{cases} \dfrac{k_{\rho_i}^{(1)}}{m_1} & \text{if } s_i = 1, \\ \dfrac{k_{i-\rho_i}^{(2)}}{m_2} & \text{if } s_i = 0. \end{cases} \tag{2.2}$$

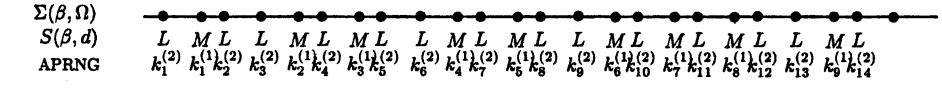

Figure 3. The structure of an APRNG.

The following results are valid when the LCG moduli are bigger than 1 and the other parameters are such that the LCGs generate at least two distinct values.

[5] The value of $O(\beta)$ is $L(\beta) - 1$ if $\Sigma(\beta,\Omega)$ is of type $\mathcal{I}$ and 1 otherwise.

Theorem 2.1. *Let $\Sigma(\beta,\Omega)$ be a two tile quasicrystal (i.e., with $d-c=\phi_{j+1}(\beta)$ for some $j=0,1,\cdots,m-1$), $S(\beta,\Omega)$ a binary sequence constructed as described in equation (2.1), and the sequence $\{n_i\}_{i=0}^{\infty}$ with n_i defined as in (2.2). For any given $i,P\in\mathbb{N}^{>0}$, there exists $N\in\mathbb{N}^{>0}$ such that*

$$n_{i+NP}\neq n_{i+(N-1)P}.$$

Corollary 2.2. *The sequence $\{n_i\}_{i=0}^{\infty}$ is aperiodic in the strongest sense: it has no periodic subset. This property is independent of the seed point x_0 from which the binary sequence is generated.*

3. Proof of Theorem 2.1

The proof of Theorem 2.1 is done in two main steps: we first prove that the sequence $S(\beta,\Omega)$ is aperiodic in the strongest sense (Proposition 3.1), and then we show that some specific patterns must occur if the sequence $\{n_i\}_{i=0}^{\infty}$ has a periodic subset (Proposition 3.2). These specific patterns occur if and only if the sequence $S(\beta,\Omega)$ has a periodic subset, and therefore the result in Theorem 2.1 follows from a contradiction.

Assume the following two propositions hold (the proofs are given below in Sections 3.1 and 3.2 respectively).

Proposition 3.1. *For any s_i in $S(\beta,\Omega)$ and $P\in\mathbb{N}^{>0}$, there exists $J\in\mathbb{N}$ such that $s_i\neq s_{i+JP}$: $S(\beta,\Omega)$ has no periodic subset.*

Proposition 3.2. *Let $P\in\mathbb{N}^{>0}$. Under the hypothesis of Theorem 2.1, if there exist integers i_0 and P such that $n_{i_0+kP}=n_{i_0}$ for all $k\in\mathbb{N}$, then both the patterns 00 and 11 occur in the sequence $\{s_{i_0+kP}\}_{k=0}^{\infty}$. Moreover, there exist only two possible distances D_1 and D_2 ($D_1'<0<D_2'$) between any two quasicrystal points $x_{i+(k+1)P}$ and x_{i+kP}, where k is any positive integer:*

$$x_{i+(n+1)P}-x_{i+nP}=\begin{cases}D_1 & \text{if } x_{i+(n+1)P}\in\Sigma_L,\\ D_2 & \text{if } x_{i+(n+1)P}\in\Sigma_{L-1}\end{cases} \tag{3.1}$$

if $\Sigma(\beta,\Omega)$ is of type $\mathcal{I}$; otherwise

$$x_{i+(n+1)P}-x_{i+nP}=\begin{cases}D_1 & \text{if } x_{i+(n+1)P}\in\Sigma_1,\\ D_2 & \text{if } x_{i+(n+1)P}\in\Sigma_L.\end{cases} \tag{3.2}$$

Proof of Theorem 2.1. The proof is obtained by contradiction. Let i_0 and P be positive integers such that $n_{i_0+kP}=n_{i_0}$ for all $k\in\mathbb{N}$.

From Proposition 3.2, there exist $k_1,k_2,n_1,n_2\in\mathbb{N}$ with $k_2,n_2\geq 2$ such that

$$\begin{aligned}&s_{i_0+k_1P}=s_{i_0+(k_1+k_2+1)P}=s_{i_0+(n_1+n)P}=0 \quad \text{for } n=1,2,\cdots,n_2;\\ &s_{i_0+n_1P}=s_{i_0+(n_1+n_2+1)P}=s_{i_0+(k_1+k)P}=1 \quad \text{for } k=1,2,\cdots,k_2.\end{aligned}$$

In other words, patterns $0\underbrace{1\ \cdots\ 1}_{k_2\text{ ones}}0$ and $1\underbrace{0\ \cdots\ 0}_{n_2\text{ zeroes}}1$ occur.

1. Let $\Sigma(\beta,\Omega)$ be of type $\mathcal{I}$. From equation (3.1), $0\underbrace{1\ \cdots\ 1}_{k_2\text{ ones}}0$ occurs and

$$\begin{aligned}&x'_{i_0+k_1P}\geq c+L'(\beta)-1,\quad x'_{i_0+k_1P}+k_2D_1'+D_2'\geq c+L'(\beta)-1,\ \text{and}\\ &\qquad x'_{i_0+k_1P}+kD_1'<c+L'(\beta)-1 \quad \text{for all } 1\leq k\leq k_2,\end{aligned} \tag{3.3}$$

and also, since $1\underbrace{0\ \cdots\ 0}_{n_2 \text{ zeroes}}1$ occurs we have

$$\begin{gathered} x'_{i_0+n_1P} < c + L'(\beta) - 1, \quad x'_{i_0+n_1P} + n_2D'_2 + D'_1 < c + L'(\beta) - 1, \text{ and} \\ x'_{i_0+n_1P} + nD'_2 \geq c + L'(\beta) - 1 \quad \text{for all } 1 \leq n \leq n_2. \end{gathered} \tag{3.4}$$

This is a contradiction since from equation (3.3) $D'_2 > -(k_2-1)D'_1 \geq -D'_1$, and from equation (3.4) $-D'_1 > (n_2-1)D'_2 \geq D'_2$.

2. Let $\Sigma(\beta,\Omega)$ be of type $\mathcal{II}$. From equation (3.2), $1\underbrace{0\ \cdots\ 0}_{n_2 \text{ zeroes}}1$ occurs and

$$\begin{gathered} x'_{i_0+k_1P} < d - 1, \quad x'_{i_0+k_1P} + k_2D'_2 + D'_1 < d - 1, \text{ and} \\ x'_{i_0+k_1P} + kD'_2 \geq d - 1 \quad \text{for all } 1 \leq k \leq k_2, \end{gathered} \tag{3.5}$$

and also since $0\underbrace{1\ \cdots\ 1}_{k_2 \text{ ones}}0$ occurs we have

$$\begin{gathered} x'_{i_0+n_1P} \geq d - 1, \quad x'_{i_0+n_1P} + n_2D'_1 + D'_2 \geq d - 1, \text{ and} \\ x'_{i_0+n_1P} + nD'_1 < d - 1 \quad \text{for all } 1 \leq n \leq n_2. \end{gathered} \tag{3.6}$$

This again is a contradiction since from equation (3.5) $-D'_1 > (k_2-1)D'_2 \geq D'_2$, and from equation (3.6) $D'_2 > -(n_2-1)D'_1 \geq -D'_1$.

□

3.1. **Proof of Proposition 3.1.** The proof follows from the next 4 lemmas. The three first lemmas are used to prove that for any nth-iterate of the stepping function f, there exists a positive integer k $\big(\text{resp. } \overline{k}\big)$ such that $f^{(kn)}$ $\big(\text{resp. } f^{(\overline{k}n)}\big)$ is strictly increasing (resp. decreasing) on $[c, c+\overline{g}_1)$ $\big(\text{resp. } [c+\overline{g}_1, d)\big)$; see Lemma 3.6.

Lemma 3.3. *Let $\Sigma(\beta,\Omega)$ be a 2TQC with stepping function f. If $n \in \mathbb{N}$, then*

$$f^{(n)}(x') = \begin{cases} x' + g_n & \text{if } x' \in \big[c, c+\overline{g}_n\big), \\ x' - \overline{g}_n & \text{if } x' \in \big[c+\overline{g}_n, d\big), \end{cases} \tag{3.7}$$

with $c + \overline{g}_n = d - g_n$, g_n and $\overline{g}_n$ are positive constants which depend on β.

Proof. The proof is done by induction on n. Let the stepping function f

$$f(x') := \begin{cases} x' + g_1 & \text{for } x' \in \big[c, c+\overline{g}_1\big), \\ x' - \overline{g}_1 & \text{for } x' \in \big[c+\overline{g}_1, d\big), \end{cases}$$

where g_1 and $\overline{g}_1$ are positive constants which depend on β. We have that $c + \overline{g}_1 = d - g_1$. Indeed, either $\Sigma(\beta,\Omega)$ is of type $\mathcal{I}$ ($c \leq 0,\ d = c+1 > 0$) and from equation (1.1)

$$f(x') := \begin{cases} x' + L'(\beta) & \text{for } x' \in \big[c, c+1-L'(\beta)\big), \\ x' + L'(\beta) - 1 & \text{for } x' \in \big[c+1-L'(\beta), c+1\big), \end{cases} \tag{3.8}$$

either $\Sigma(\beta,\Omega)$ is of type $\mathcal{II}$ and from equation (1.1)

$$f(x') := \begin{cases} x' + 1 & \text{for } x' \in [c, d-1), \\ x' + L'(\beta) & \text{for } x' \in [d-1, d), \end{cases} \tag{3.9}$$

i.e., $g_1 = 1$ and $-\overline{g}_1 = L'(\beta) = 2 - \phi_i(\beta) = 1 - d + c$ and

$$c + \overline{g}_1 = d - 1 = d - g_1.$$

Assume equation (3.7) holds for $n = N$. Then

$$f^{(N)}\big([c, c+\overline{g}_N)\big) = [c+g_N, d),$$
$$f^{(N)}\big([c+\overline{g}_N, d)\big) = [c, d-\overline{g}_N) = [c, c+g_N).$$

Indeed, we have the following two cases.

- If $\overline{g}_1 < g_N$, then $c+\overline{g}_1 < c+g_N$ and thus $[c+g_N, d) \subset [c+\overline{g}_1, d)$ and

$$f^{(N+1)}(x') = \begin{cases} x' + g_N - \overline{g}_1, & x' \in [c, c+\overline{g}_N), \\ x' - \overline{g}_N + g_1, & x' \in [c+\overline{g}_N, c+\overline{g}_N+\overline{g}_1), \\ x' - \overline{g}_N - \overline{g}_1, & x' \in [c+\overline{g}_N+\overline{g}_1, d), \end{cases} \tag{3.10}$$

  where $g_1 - \overline{g}_N = d - c - \overline{g}_1 - (d - c - g_N) = g_N - \overline{g}_1 > 0$. Thus $g_{N+1} = g_N - \overline{g}_1$ and $\overline{g}_{N+1} = \overline{g}_N + \overline{g}_1$.
- If $\overline{g}_1 > g_N$, then $c+\overline{g}_1 > c+g_N$ and thus $[c, c+g_N) \subset [c, c+\overline{g}_1)$ and

$$f^{(N+1)}(x') = \begin{cases} x' + g_N + g_1, & x' \in [c, c+\overline{g}_1 - g_N), \\ x' + g_N - \overline{g}_1, & x' \in [c+\overline{g}_1 - g_N, c+\overline{g}_N), \\ x' - \overline{g}_N + g_1, & x' \in [c+\overline{g}_N, d). \end{cases} \tag{3.11}$$

  Thus $g_{N+1} = g_N + g_1$ and $\overline{g}_{N+1} = \overline{g}_1 - g_N$.

Note that for any positive integer N, $\overline{g}_1 \neq g_N$. Indeed, from equations (3.9) and (3.8), $\overline{g}_1 \neq g_1$, and since $L'(\beta)$ is irrational, $k_1 g_1 - k_2 \overline{g}_1 = \overline{g}_1$ with $k_i \in \mathbb{Z}$ if and only if $k_1 = 0, k_2 = -1$. Moreover, from the previous arguments, there exist two positive integers $\alpha_N > 0$ and $\overline{\alpha}_N$ such that $g_N = \alpha_N g_1 - \overline{\alpha}_N \overline{g}_1$; therefore $g_N \neq \overline{g}_1$. □

Lemma 3.4. *Let $\Sigma(\beta, \Omega)$ be a 2TQC with stepping function f and $n \in \mathbb{N}$. Then for any $k \in \mathbb{N}$:*

1. *If $g_{kn} < \overline{g}_n$,*

$$f^{((k+1)n)}(x') = \begin{cases} x' + g_{kn} + g_n & \text{if } x' \in [c, c+\overline{g}_n - g_{kn}), \\ x' + g_{kn} - \overline{g}_n & \text{if } x' \in [c+\overline{g}_n - g_{kn}, d); \end{cases} \tag{3.12}$$

2. *If $g_{kn} > \overline{g}_n$,*

$$f^{((k+1)n)}(x') = \begin{cases} x' + g_{kn} - \overline{g}_n & \text{if } x' \in [c, c+\overline{g}_{kn} + \overline{g}_n), \\ x' - (\overline{g}_{kn} + \overline{g}_n) & \text{if } x' \in [c+\overline{g}_{kn} + \overline{g}_n, d). \end{cases} \tag{3.13}$$

Proof. The proof is a simple generalisation of equations (3.10) and (3.11) in the proof of Lemma 3.3.

1. Case $g_{kn} < \overline{g}_n$. From Lemma 3.3,

$$\begin{aligned} f^{((k+1)n)}(x') &= \begin{cases} f^{(kn)}(x') + g_n & \text{if } f^{(kn)}(x') \in \big[c, c+\overline{g}_n\big), \\ f^{(kn)}(x') - \overline{g}_n & \text{if } f^{(kn)}(x') \in \big[c+\overline{g}_n, d\big) \end{cases} \\ &= \begin{cases} f^{(kn)}(x') + g_n & \text{if } x' \in [c+\overline{g}_{kn}, d), \\ f^{(kn)}(x') + g_n & \text{if } x' \in [c, c+\overline{g}_{kn} - g_n), \\ f^{(kn)}(x') - \overline{g}_n & \text{if } x' \in\in [c+\overline{g}_{kn} - g_n, c+\overline{g}_{kn}) \end{cases} \\ &= \begin{cases} x' - \overline{g}_{kn} + g_n & \text{if } x' \in [c+\overline{g}_{kn}, d), \\ x' + g_{kn} + g_n & \text{if } x' \in [c, c+\overline{g}_{kn} - g_n), \\ x' + g_{kn} - \overline{g}_n & \text{if } x' \in [c+\overline{g}_{kn} - g_n, c+\overline{g}_{kn}). \end{cases} \end{aligned}$$

Equation (3.12) follows using $d-c = g_{kn}+\overline{g}_{kn} = g_n+\overline{g}_n$, i.e., $g_{kn}-\overline{g}_n = g_n-\overline{g}_{kn}$.

2. Case $g_{kn} > \overline{g}_n$. From Lemma 3.3

$$f^{((k+1)n)}(x') = \begin{cases} f^{(kn)}(x')+g_n & \text{if } x' \in [c+\overline{g}_{kn}, c+\overline{g}_{kn}+g_n), \\ f^{(kn)}(x')-\overline{g}_n & \text{if } x' \in [c+\overline{g}_{kn}+g_n, d), \\ f^{(kn)}(x')-\overline{g}_n & \text{if } x' \in [c, c+\overline{g}_{kn}) \end{cases}$$

$$= \begin{cases} x'-\overline{g}_{kn}+g_n & \text{if } x' \in [c+\overline{g}_{kn}, c+\overline{g}_{kn}+g_n), \\ x'-\overline{g}_{kn}-\overline{g}_n & \text{if } x' \in [c+\overline{g}_{kn}+g_n, d), \\ x'+g_{kn}-\overline{g}_n & \text{if } x' \in [c, c+\overline{g}_{kn}). \end{cases}$$

Again the result follows using $d-c = g_{kn}+\overline{g}_{kn} = g_n+\overline{g}_n$.

□

Lemma 3.5. *For all positive integers n, there exist two positive integers k and $\overline{k}$ such that*

$$0 < \overline{g}_{\overline{k}n} \le \overline{g}_1 \le \overline{g}_{kn} < d-c.$$

Proof. We show that if $\overline{g}_n < \overline{g}_1$, then there exists $K \in \mathbb{N}$ such that $\overline{g}_{Kn} \ge \overline{g}_1$. (The converse statement is proven similarly.)

Let $\overline{g}_{kn} < \overline{g}_1$ for all $k \in \mathbb{N}$; then $g_{kn} < \overline{g}_1$ for all $k \in \mathbb{N}$. Indeed, if there exists k such that $g_{kn} \ge \overline{g}_1 > \overline{g}_{kn}$, then there exists $j \in \mathbb{N}$ such that

$$(j+1)\overline{g}_{kn} \ge g_{kn} > j\overline{g}_{kn},$$

and using Lemma 3.4 j times ($k \to 1$, $n \to kn$ in Lemma 3.4),

$$g_{jkn} = g_{kn} - (j-1)\overline{g}_{kn},$$

$$\overline{g}_{(j+1)kn} = (j+1)\overline{g}_{kn} \ge g_{kn} > \overline{g}_1, \qquad g_{(j+1)kn} = g_{kn} - j\overline{g}_{kn}.$$

Moreover, $g_{kn-j} < \overline{g}_1$ for all $j \le k$, i.e., $g_N < \overline{g}_1$ for all $N \in \mathbb{N}$. Indeed, let $k, j \in \mathbb{N}$ and such that j is the smallest number (if it exists) such that $g_{kn-j-1} > \overline{g}_1$; then by Lemma 3.4

$$\overline{g}_{kn-j} = \overline{g}_{kn-j-1} + \overline{g}_1 > \overline{g}_1$$

which contradicts the fact that j is the smallest such number.

Finally, if $g_N < \overline{g}_1$ for all $N \in \mathbb{N}$, then from Lemma 3.4

$$g_j = j g_1 \tag{3.14}$$

for all $j \in \mathbb{N}$. This is again a contradiction since $g_j \le d-c$. It follows that there exists $K \in \mathbb{N}$ such that $\overline{g}_{Kn} \ge \overline{g}_1$.

Lemma 3.4 follows by setting $\overline{k} = 1$ and $k = K$.

(In the proof of the converse statement, equation (3.14) becomes $\overline{g}_j = j\overline{g}_1$.) □

Lemma 3.6. *Let $\Sigma(\beta, \Omega)$ be a two tile quasicrystal with tile lengths $O(\beta)$ and $L(\beta)$; let f be its stepping function. For each $n \in \mathbb{N}$, there exist two positive integers k and $\overline{k}$ such that*

$$f^{(kn)}(x') = x' + g_{kn}, \quad x' \in \big[c, c+\overline{g}_1\big),$$

$$f^{(\overline{k}n)}(x') = x' - \overline{g}_{\overline{k}n}, \quad x' \in \big[c+\overline{g}_1, d\big),$$

with either $k = 1$ or $\overline{k} = 1$, and g_{kn} and $\overline{g}_{\overline{k}n}$ are positive constants which depend on β with $g_{kn} + \overline{g}_{\overline{k}n} = d-c$.

Proof. Consider equation (3.7) of Lemma 3.3. From Lemma 3.5, there exists a positive integer k such that

$$f^{(kn)}(x') = x + g_{kn} \quad \text{for } x \in \big[c, c+\overline{g}_1\big) \subset \big[c, c+\overline{g}_{kn}\big).$$

Similarly, from Lemma 3.5, there exists a positive integer $\overline{k}$ such that

$$f^{(\overline{k}n)}(x') = x - \overline{g}_{\overline{k}n} \quad \text{for } x \in \big[c+\overline{g}_1, d\big) \subset [c+\overline{g}_{\overline{k}n}, d).$$

□

Proof of Proposition 3.1. We show that Ω cannot be bounded if $f^{(kn)}$ $\big($resp. $f^{(\overline{k}n)}\big)$ is strictly increasing (resp. decreasing).

Assume $s_i = 0$, i.e. $x'_i \in \Omega_O$. From Lemma 3.5, there exists k such that

$$f^{(kP)}(x') = x' \pm g_{kP}.$$

Let P be such that $s_{i+kP} = 0$ for all $k \in \mathbb{N}$ and consider the sequence $\{y_j\}_{j=0}^{\infty}$ with

$$y_j = f^{(jkP)}(x'_i).$$

If $P > 0$, then for a sufficiently large J

$$|y_J - y_0| = |x'_{Jkp+i} - x'_i| = Jg_{kP} \geq d - c.$$

This is a contradiction; therefore $P = 0$.

Similarly, if $x'_i \in \Omega_L$, one obtains that if $P > 0$, then for sufficiently large $\overline{J}$

$$|y_0 - y_{\overline{J}}| = \overline{J} g_{kP} \geq d - c.$$

□

3.2. **Proof of Proposition 3.2.** This proof follows from the next lemma. We use the notation

$$x_{i_0+kP} = L_{kP}L(\beta) + O_{kP}O(\beta) + x_{i_0}. \tag{3.15}$$

Lemma 3.7. *Let $P \in \mathbb{N}^{>0}$. Under the hypothesis of Theorem 2.1, there exist two possible distances D_1 and D_2 $(D'_1 < 0 < D'_2)$ between any two quasicrystal points x_{i_0+kP} and $x_{i_0+(k+1)P}$, where k is any positive integer.*

Proof. Let $d - c = \phi_{j+1}(\beta)$ and $x_{i_0+(k+1)P} - x_{i_0+kP} = l_{kP}L(\beta) + o_{kP}O(\beta)$ with $P = l_{kP} + o_{kP}$. There exists j with $0 \leq j \leq m-1$ and such that

$$0 < |x'_{i_0+(k+1)P} - x'_{i_0+kP}| = \big|l_{kP}L'(\beta) + o_{kP}O'(\beta)\big| < \phi_{j+1}(\beta).$$

Therefore,

$$\begin{aligned}
& -\phi_{j+1}(\beta) < l_{kP}L'(\beta) + o_{kP}O'(\beta) < \phi_{j+1}(\beta) \\
\implies \quad & -\phi_{j+1}(\beta) - PO'(\beta) < l_{kP}\big(L'(\beta) - O'(\beta)\big) < \phi_{j+1}(\beta) - PO'(\beta) \\
\implies \quad & \frac{PO'(\beta)}{\phi_{j+1}(\beta)} - 1 < l_{kP}\frac{O'(\beta) - L'(\beta)}{\phi_{j+1}(\beta)} < 1 + \frac{PO'(\beta)}{\phi_{j+1}(\beta)}. \qquad (3.16)
\end{aligned}$$

Since $L'(\beta) = 2 - \phi_j(\beta)$, when $O(\beta) = 1$, then $j = m - i$ and

$$L'(\beta) - O'(\beta) + \phi_{j+1}(\beta) = 0,$$

and when $j = m-1$, then $L'(\beta) = O'(\beta) + 1$ and

$$L'(\beta) - O'(\beta) - \phi_m(\beta) = 0.$$

In all cases $|L'(\beta)-O'(\beta)| = \phi_{j+1}(\beta)$, and equation (3.16) has two integer solutions $L_a(\beta)$ and $L_b(\beta) = L_a(\beta)+1$. To insure $D'_1 < 0$, let

$$\big(L_1(\beta), L_2(\beta)\big) = \begin{cases} \big(L_a(\beta), L_b(\beta)\big) & \text{if } j = m-1, \\ \big(L_b(\beta), L_a(\beta)\big) & \text{if } j \neq m-1. \end{cases}$$

The possible distances are then

$$\begin{aligned} D_1 &= L_1(\beta)L(\beta) + \big(P - L_1(\beta)\big)O(\beta), \\ D_2 &= L_2(\beta)L(\beta) + \big(P - L_2(\beta)\big)O(\beta), \end{aligned}$$

with $D'_1 < 0 < D'_2$. □

Proof of Proposition 3.2. The proof is made by contradiction. The set $\{s_{i_0}s_{i_0+P}\}$ is not periodic (from Proposition 3.1); thus there exists k_1 such that

$$\big\{s_{i_0+k_1P}s_{i_0+(k_1+1)P}\big\}$$

is either $\{11\}$ or $\{00\}$.

1. Let $\Sigma(\beta,\Omega)$ be of type $\mathcal{I}$. If $\{11\}$ occurs, then $L_{(k_1+1)P} = L_{k_1P} + L_1(\beta)$ and since $n_{i_0} = n_{i_0+kP}$, then $L_1(\beta) = 0 \pmod{m_1}$. Similarly, if $\{00\}$ occurs, then $P - L_2(\beta) = 0 \pmod{m_2}$.
   Consider the case where $\{11\}$ occurs and $\{00\}$ never occurs. For any k_1 such that $s_{i_0+k_1P} = 0$, then $s_{i_0+(k_1\pm1)P} = 1$. Thus using notation (3.15)

$$\begin{aligned} L_{(k_1+1)P} &= L_{(k_1-1)P} + L_2(\beta) + L_1(\beta) \pmod{m_1} \\ &= L_2(\beta) \pmod{m_1} \\ &= 0 \pmod{m_1}. \end{aligned} \tag{3.17}$$

   This is a contradiction since $L_2(\beta) = L_1(\beta) + 1 = 1 \pmod{m_1}$ (we assume $m_i > 1$); therefore $\{00\}$ occurs.
   Moreover, let $x_{i_0+(k+1)P} \in \Sigma_L$ and $x_{i_0+(k+1)P} - x_{i_0+kP} = D_2$. Since $D'_2 > 0$, $x_{i_0+kP} \in \Sigma_L$. Again, since $n_{i_0} = n_{i_0+kP}$, then

$$\begin{aligned} L_{(k+1)P} &= L_{kP} + L_2(\beta) \pmod{m_1} \\ &= 0 \pmod{m_1}. \end{aligned}$$

   This is the same contradiction as above and the result follows.
   Similarly, if $\{00\}$ occurs and $\{11\}$ never occurs, we obtain that $P - L_1(\beta) = 0 \pmod{m_2}$ and therefore $\{11\}$ occurs. Moreover, if $x_{i_0+(k+1)P} \in \Sigma_1$ and $x_{i_0+(k+1)P} - x_{i_0+kP} = D_1$, since $D'_1 < 0$, $x_{i_0+kP} \in \Sigma_{L-1}$ and we must have $P - L_2(\beta) = 0 \pmod{m_2}$ which is a contradiction and from which the result follows.
2. Let $\Sigma(\beta,\Omega)$ be of type $\mathcal{II}$. The argument follows as in the previous case interchanging 00 with 11 and $L_2(\beta)$ with $L_1(\beta)$.

□

Conclusion

We showed how two tile quasicrystals can be used with two LCGs to produce aperiodic PRNGs. Any pair of LCGs can be used to produce an APRNG (provided the modulus is greater than 1). However the choice of LCGs influences the statistics of the APRNGs: for example, choosing the two LCGs having bad statistical properties would produce an APRNG with "bad" statistical properties (the dependency of the statistical properties of the APRNG on the choice of the LCGs is treated in

[4]). The actual design of the APRNG could be easily modified to combine any two periodic PRNGs. Less trivial modifications can also be performed: for instance, the combination of more than two PRNGs (see [3]).

The results we have obtained are given for 2TQCs defined by unitary quadratic Pisot numbers. It is believed by the authors that three tile quasicrystals (3TQCs) defined by unitary quadratic Pisot numbers can be used as well to break the periodicity of PRNGs, but the proofs presented here do not easily generalise to such quasicrystals. Indeed, the number of discontinuities of the iterates $f^N(x)$ of the stepping function $f(x)$ can become very large as each iteration can introduce as many as two additional discontinuities. Therefore the function f^N cannot be written in a form as nice as equation (3.7). The proof of the result for 3TQCs requires a different approach, and the authors are presently working on this problem. The use of 3TQCs may not offer great improvements on the statistics of APRNGs, but it could improve their cryptographic security. Z. Masáková, J. Patera and E. Pelantová are presently working on the properties of quasicrystals defined by irrationalities of higher degree. It is also believed by the authors that such quasicrystals could be used to construct APRNGs.

As mentioned in [3], the quasicrystal generation can be made much faster using parallelism since any quasicrystal can be generated simultaneously from several (many) seed points. The APRNG is then easily amenable to parallelism generation if the state of each LCG at all seed points is given.

The APRNG design is also amenable to multidimensional PRNGs construction. Indeed, as mentioned in Section 1, the cut and project quasicrystal model can be generalised to any finite dimension N thus generating N-dimensional aperiodic point sets. Generalising the design of APRNGs using these multidimensional point sets gives multidimensional PRNGs. Even though the generalisation of the design is simple, obtaining the properties of these multidimensional PRNGs is a very hard task since virtually nothing is known about the properties of N-dimensional cut and project quasicrystals.

Acknowledgments

The authors would like to thank Claude Crépeau, Zuzana Masáková and Edita Pelantová for their stimulating discussions and remarks, and also Jan Patera for all the programming support and insight. The first author would like to thank the Department of Mathematics of the Czech Technical Institute in Prague where part of this work was done.

References

1. S. Berman and R. V. Moody, *The algebraic theory of quasicrystals with five-fold symmetry*, J. Phys. A: Math. Gen. **27** (1994), 115–130. MR **95j:**52039
2. E. Bombieri and J. E. Taylor, *Quasicrystals, tilings and algebraic number theory: some preliminary connections*, Contemp. Math. **64** (1987), 241–260. MR **89a:**82031
3. L.-S. Guimond, Jan Patera, and Jiří Patera, *Combining random number generators using cut and project sequences*, Czechoslovak J. Phys. **51** # 4 (2001), 305–311.
4. ———, *Statistics and implementation of an APRNG*, Preprint (2000), 22 pages.
5. S. Lang, *Algebra*, 3^{rd} ed., Addison-Wesley, Massachussetts USA, 1993.
6. Z. Masáková, J. Patera, and E. Pelantová, *Patent pending # 09/327633*, filing date: June 8, 1999.
7. ———, *Quadratic irrationalities and geometric properties of one-dimensional quasicrystals*, Preprint CRM-2565, 1998.

8. R. V. Moody and J. Patera, *Quasicrystals and icosians*, J. Phys. A: Math. Gen. **26** (1994), 2829–2853. MR **94f:**52030
9. Jan Patera, *Methods of computer-based generation of quasicrystals*, Master's thesis, Czech Technical University, 1999, email: patera@km1.fjfi.cvut.cz.
10. D. Schechtman, I. Blech, D. Gratias, and J. W. Cahn, *Metallic phase with long-range orientational order and no translational symmetry*, Physical Review Letters **53** (1984), 1951–1953.
11. M. Senechal, *Quasicrystals and geometry*, Cambridge Univ. Press, Cambridge, UK, 1995. MR **96c:**52038
12. S. Webber, *What are quasicrystals*, Web page maintained by S. Webber: http://www.nirim.go.jp/~weber/qc.html#1.

Centre de Recherches Mathématiques, Université de Montréal, c.p. 6128, succ. centre-ville, Montréal (Québec), Canada, H3C-3J7
E-mail address: guimond@CRM.UMontreal.CA

Centre de Recherches Mathématiques, Université de Montréal, c.p. 6128, succ. centre-ville, Montréal (Québec), Canada, H3C-3J7
E-mail address: patera@CRM.UMontreal.CA