Combinatorics on words for Markoff numbers

One World Combinatorics on Words Seminar

Laurent Vuillon

and Christophe Reutenauer, July 2020





UMR 5127

More than 100 years

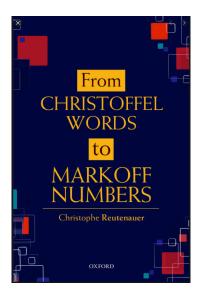
Martin Aigner

Markov's Theorem and 100 Years of the Uniqueness Conjecture

A Mathematical Journey from Irrational Numbers to Perfect Matchings

Laurent Vuillon

D Springer



Outline

1) Approximations of real numbers







Dirichlet's Theorem

Theorem [Dirichlet, 1855]

Let $\alpha \in \mathbb{R}$ and $N \in \mathbb{N}$. There exists $\frac{p}{q} \in \mathbb{Q}$ with $q \leq N$ such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qN} \quad \left(\leq \frac{1}{q^2} \right)$$

Corollary

If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, then there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ with

$$\alpha - \frac{p}{q} \bigg| \le \frac{1}{q^2}.$$

Number Theory

A complex number α is called *algebraic of degree d* if α is the root of a polynomial with integer coefficients of degree *d*, and *d* is the smallest degree for which such a polynomial exists.

 $\sqrt{2}$ is algebraic of degree 2 because it is solution of $x^2 - 2 = 0$.

Number Theory

A complex number α is called *algebraic of degree d* if α is the root of a polynomial with integer coefficients of degree *d*, and *d* is the smallest degree for which such a polynomial exists.

 $\sqrt{2}$ is algebraic of degree 2 because it is solution of $x^2 = 2$.

If there is no such polynomial for any degree, then α is called *transcendental*.

For example,

are transcendental.

Liouville's Theorem

Theorem [Liouville,1836]

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be algebraic of degree *d*. Then there is a constant C > 0 such that

$$rac{m{C}}{m{q}^{m{d}}} < \left| lpha - rac{m{p}}{m{q}}
ight|$$
 for all $rac{m{p}}{m{q}} \in \mathbb{Q}.$

This implies a nice link between rational approximation and degree of the algebraic number.

Roth's Theorem

Theorem [Liouville,1836]

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ be algebraic of degree *d*. Then there is a constant C > 0 such that

$$rac{m{C}}{m{q}^{m{d}}} < \left| lpha - rac{m{p}}{m{q}}
ight|$$
 for all $rac{m{p}}{m{q}} \in \mathbb{Q}.$

On the opposite

Theorem [Roth, 1955]

Let α be a real number and $\epsilon > 0$. If there are infinitely many $\frac{p}{q} \in \mathbb{Q}$ with

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{2+\epsilon}}$$

then α is transcendental.

Lagrange spectrum

In general we cannot improve the exponent 2...

Consider all real numbers L > 0 such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{Lq^2}$$

holds for infinitely many $\frac{p}{q} \in \mathbb{Q}$.

Definition

Given $\alpha \in \mathbb{R}$, $L(\alpha) = \sup L$ over all *L* that satisfy $\left| \alpha - \frac{p}{q} \right| < \frac{1}{Lq^2}$ is called the *Lagrange number* of α .

 $\mathcal{L} = {L(\alpha) : \alpha \in \mathbb{R} \setminus \mathbb{Q}}$ is the Lagrange spectrum.

The Lagrange spectrum below 3 is $\mathcal{L}_{<3} = \{L(\alpha) \in \mathcal{L} : L(\alpha) < 3\}.$

First value of the Lagrange spectrum

Theorem [Hurwitz, 1891]

Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Then there are infinitely many rational numbers $\frac{p}{q}$ such that

$$\left|\alpha-\frac{p}{q}\right|<\frac{1}{\sqrt{5}q^2}.$$

And in fact
$$L\left(\frac{1+\sqrt{5}}{2}\right) = \sqrt{5}$$
.

Thus $\frac{1+\sqrt{5}}{2}$ is the most badly approximated quadratic number and $\sqrt{5}$ is the first element of the Lagrange spectrum ...

First value of the Lagrange spectrum

In fact
$$L\left(\frac{1+\sqrt{5}}{2}\right) = \sqrt{5}$$
.

Thus $\frac{1+\sqrt{5}}{2}$ is the most badly approximated quadratic number and $\sqrt{5}$ is the first element of the Lagrange spectrum ...

In fact all cousins of the golden ratio are badly approximated : two real numbers α and β are cousin if $\beta = \frac{a\alpha+b}{c\alpha+d}$ where $a, b, c, d \in \mathbb{Z}$ and $ad - bc = \pm 1$. Using homography transformations we find the same Lagrange number : if two real numbers α and β are cousin then $L(\alpha) = L(\beta)$.

Second value of the Lagrange spectrum

If we exclude $\frac{1+\sqrt{5}}{2}$ and all its cousins, then we find the second Lagrange number :

Theorem [Markoff, 1880]

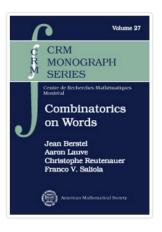
Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ which is neither $\frac{1+\sqrt{5}}{2}$ nor a cousin of $\frac{1+\sqrt{5}}{2}$. Then there are infinitely many rational numbers $\frac{p}{a}$ such that

$$\left| lpha - rac{p}{q}
ight| < rac{1}{\sqrt{8}q^2}.$$

Thus $\sqrt{8}$ is the second value of the Lagrange spectrum and in fact $L(1 + \sqrt{2}) = \sqrt{8}$ is the second badly approximated quadratic number.

We could find the third value of the Lagrange spectrum which is $\frac{\sqrt{221}}{5}$ and so on ...

Link with continued fractions



Link with continued fractions

Suppose $\alpha \in \mathbb{R}$. The (simple) **continued fraction representation** of α is the sequence of integers a_0, a_1, a_2, \ldots constructed recursively as follows: let

$$\beta_0 = \alpha$$
 and $a_0 = \lfloor \beta_0 \rfloor;$

if i > 0 and $a_{i-1} \neq \beta_{i-1}$, then let

$$eta_i = rac{1}{eta_{i-1} - a_{i-1}} \quad ext{ and } \quad a_i = \lfloor eta_i
floor;;$$

if i > 0 and $a_{i-1} = \beta_{i-1}$, then the recursion terminates. The continued fraction representation of α is commonly denoted by

$$lpha = a_0 + rac{1}{a_1 + rac{1}{a_2 + rac{1}{a_3 + rac{1}{\ddots}}}}$$

or more compactly by $\alpha = [a_0, a_1, a_2, a_3, \ldots].$

$$\frac{1+\sqrt{5}}{2} = [1, 1, \cdots, 1, \cdots]; 1 + \sqrt{2} = [2, 2, \cdots, 2, \cdots]; [1, 2, \cdots, 1, 2, \cdots].$$

Diophantine equation

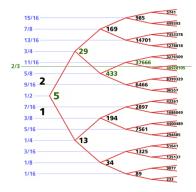
Tree of Markoff triples

Theorem [Markoff, 1880]

Let $\mathcal{M} =$

 $\{1, 2, 5, 13, 29, 34, 89, 169, 194, 233, 433, 610, 985, 1325, \cdots\}$ be the sequence of Markoff numbers. The Lagrange spectrum

below 3 is given by
$$\mathcal{L}_{<3} = \left\{ rac{\sqrt{9m^2-4}}{m} : m \in \mathcal{M}
ight\}.$$



Markoff's Theorem

Theorem [Markoff, 1880]

Let $\mathcal{M} =$

 $\{1,2,5,13,29,34,89,169,194,233,433,610,985,1325,\cdots\}$ be the sequence of Markoff numbers. The Lagrange spectrum below 3 is given by

$$\mathcal{L}_{<3} = \left\{ \frac{\sqrt{9m^2 - 4}}{m} : m \in \mathcal{M} \right\}.$$

And to define the sequence of Markoff numbers, we consider the solutions of the following Diophantine equation :

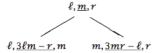
$$x^2 + y^2 + z^2 = 3xyz$$
 with $x, y, z \in \mathbb{N}^*$.

First triples

The triplets (1,1,1) and (1,1,2) are solutions of the equation

$$x^2 + y^2 + z^2 = 3xyz$$
 with $x, y, z \in \mathbb{N}^*$.

The triple (1,2,5) is a solution with non repeated values. In fact, if we note the maximal value in the middle of the triples, we find a recursive rule in order to generate new solutions :



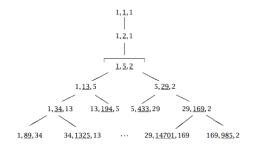
Markoff tree



The recursive rule gives birth to an infinite tree



Frobenius' conjecture All the Markov numbers appear in the Markoff tree.



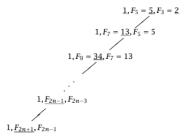
The Frobenius' conjecture asserts that :

Conjecture [Frobenius, 1913]

Each Markoff number is the **maximum of a unique Markoff triple** in the Markoff tree.

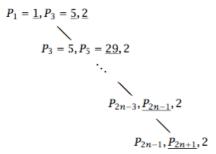
Left branch of the Markoff tree

Consider the Fibonacci numbers F_n , with $F_0 = 0$, $F_1 = 1$, and the recurrence $F_{n+1} = F_n + F_{n-1}$ $(n \ge 1)$. The first values are $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \cdots$ and F_{2n+1} with $n \ge 1$ are in the left branch of the Markoff tree :



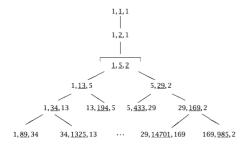
Right branch of the Markoff tree

Consider the Pell numbers P_n , with $P_0 = 0$, $P_1 = 1$, and the recurrence $P_{n+1} = 2P_n + P_{n-1}$ $(n \ge 1)$. The first values are 0, 1, 2, 5, 12, 29, 70, 169, 408, 985 · · · and P_{2n+1} with $n \ge 1$ are in the right branch of the Markoff tree :



Fibonacci and Pell numbers

The **Frobenius' conjecture** asserts that each Markoff number is the **maximum of a unique Markoff triple** in the Markoff tree !



It is not easy to prove that the sets $\{F_{2n+1} : n \ge 1\}$ and $\{P_{2n+1} : n \ge 1\}$ are distinct except for the value 5 (see the paper in 2009 of Y. Bugeaud, C. Reutenauer, S. Siksek).

Palindrome Definition

A *word* w is a finite sequence of letters $w_1 w_2 \cdots w_n$ on a finite alphabet Σ .

The set of all finite words on the alphabet Σ is denoted by Σ^* .

w = aabb is a word on the alphabet $\Sigma = \{a, b\}$.

Definitions

A prefix of a word $w = w_1 w_2 \cdots w_n$ with $w_i \in \Sigma$ is a word $p = w_1 w_2 \cdots w_j$ where $j \le n$. The *reversal* of a word $w = w_1 w_2 \cdots w_n$ with $w_i \in \Sigma$ is the word $\widetilde{w} = w_n w_{n-1} \cdots w_1$. A word *w* is a *palindrome* if it is equal to its reversal (that is $w = \widetilde{w}$).

w = aba is a palindrome on the alphabet $\Sigma = \{a, b\}$. p = ab is a prefix of w.

Palindromic closure

Definition [de Luca, 1997]

The palindromic closure of a word *x* on the alphabet $\Sigma = \{a, b\}$ is the shortest palindrome having *x* as a prefix, it exists and is unique, it is denoted by $x^{(+)}$.

For example, if x = a, then $x^{(+)} = a$ because x is a palindrome. If x = ab, then $x^{(+)} = aba$.

It is known that $x^{(+)} = x'y\tilde{x'}$ where x = x'y with y the longest palindrome suffix of x. A *suffix* of a word $w = w_1w_2\cdots w_n$ with $w_i \in \Sigma$ is a word $s = w_jw_{j+1}\cdots w_n$ where $j \ge 1$.

Iterated palindromic closure

Definition [de Luca, 1997]

We consider the iterated palindromic closure, denoted by Pal(d), is defined recursively by $Pal(d_1d_2\cdots d_n) = (Pal(d_1d_2\cdots d_{n-1})d_n)^{(+)}, d_i \in \Sigma$, with the initial condition $Pal(\epsilon) = \epsilon$, where ϵ denotes the empty word. The word *d* is called the *directive word* of Pal(d).

For example Pal(aba) = abaaba; indeed Pal(a) = a and $Pal(ab) = (Pal(a)b)^{(+)} = (ab)^{(+)} = aba$ and then $Pal(aba) = (Pal(ab)a)^{(+)} = (abaa)^{(+)} = abaaba = \underline{a} \underline{b} \underline{a} \underline{a} \underline{b} \underline{a}.$

Thue-Morse substitution and the main theorem

We also use the *Thue-Morse substitution*, denoted by $\theta = (ab, ba)$ that maps the letter *a* to *ab* and the letter *b* to *ba*.

Theorem[C. Reutenauer, LV, 2017]

For each word $v \in \{a, b\}^*$, the number $|Pa| \circ \theta \circ Pal(av)| + 2$ is a Markoff number $\neq 1, 2$.

The mapping defined in this way from $\{a, b\}^*$ into the set of Markoff numbers different from 1, 2 is surjective. Injectivity of this mapping is equivalent to the Frobenius' conjecture.

The Markoff number m = 5 is given by $v = \epsilon$; indeed Pal(a) = a, thus $\theta \circ Pal(a) = ab$ and then Pal $\circ \theta \circ Pal(a) = Pal(ab) = aba$, which is of length 3.

Thue-Morse substitution and the main theorem

We also use the *Thue-Morse substitution*, denoted by $\theta = (ab, ba)$ that maps the letter *a* to *ab* and the letter *b* to *ba*.

Theorem[C. Reutenauer, LV, 2017]

For each word $v \in \{a, b\}^*$, the number $|Pa| \circ \theta \circ Pal(av)| + 2$ is a Markoff number $\neq 1, 2$.

The Markoff number m = 13 is given by v = a; indeed Pal(aa) = aa, thus $\theta \circ Pal(aa) = abab$ and then Pal $\circ \theta \circ Pal(aa) = Pal(abab) = \underline{a} \underline{b} a \underline{a} ba \underline{b} aaba$, which is of length 11.

Thue-Morse substitution and the main theorem

We also use the *Thue-Morse substitution*, denoted by $\theta = (ab, ba)$ that maps the letter *a* to *ab* and the letter *b* to *ba*.

Theorem[C. Reutenauer, LV, 2017]

For each word $v \in \{a, b\}^*$, the number $|Pa| \circ \theta \circ Pal(av)| + 2$ is a Markoff number $\neq 1, 2$.

The Markoff number m = 29 is given by v = b indeed Pal(ab) = aba, thus $\theta \circ Pal(aba) = abbaab$ and then Pal $\circ \theta \circ Pal(ab) = Pal(abbaab) =$

<u>a ba ba a</u>baba <u>a</u>baba <u>b</u>aababaababaa, which is of length 27.

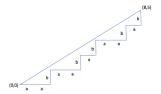
Christoffel words

The Markoff number m = 13 is given by v = a and Pal $\circ \theta \circ$ Pal $(aa) = \underline{a} \underline{b} a \underline{a} b a \underline{b} a a b a$. The word a Pal $\circ \theta \circ$ Pal(av)b is a Christoffel word :

Definition

A Christoffel word coding of a discrete segment from (0, 0) to (i, j) where *i* and *j* are co-prime (i.e. gcd(i, j) = 1).

For v = a we compute C = a abaababaaba b



More on Christoffel words

Definition 1.2. Suppose $a \perp b$ and $(a, b) \neq (0, 1)$. The **label** of a point (i, j) on the (lower) Christoffel path of slope $\frac{b}{a}$ is the number $\frac{ib-ja}{a}$. That is, the label of (i, j) is the vertical distance from the point (i, j) to the line segment from (0, 0) to (a, b).

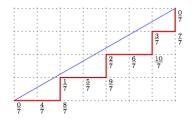


FIGURE 1.3: The labels of the points on the Christoffel path of slope $\frac{4}{7}$.

Definition 1.4. Suppose $a \perp b$. Consider the Cayley graph of $\mathbb{Z}/(a+b)\mathbb{Z}$ with generator b. It is a cycle, with vertices $0, b, 2b, 3b, \ldots, a, 0 \mod (a+b)$. Starting from zero and proceeding in the order listed above,

- (i) label those edges (s, t) satisfying s < t by x;
- (ii) label those edges (s, t) satisfying s > t by y;
- (*iii*) read edge-labels in the prescribed order, i.e., $0 \xrightarrow{x} b \xrightarrow{*} \cdots \xrightarrow{*} a \xrightarrow{y} 0$.

The lower Christoffel word of slope $\frac{b}{a}$ is the word $x \cdots y$ formed above.

Example. Pick a = 7 and b = 4. Figure 1.4 shows the Cayley graph of $\mathbb{Z}/11\mathbb{Z}$ with generator 4 and edges $u \to v$ labelled x or y according to whether or not u < v. Reading the edges clockwise from 0 yields the word xxyxxyxyy,

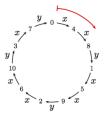


FIGURE 1.4: The Cayley graph of $\mathbb{Z}/(7{+}4)\mathbb{Z}$ with generator 4 and the associated Christoffel word.

Example. From the previous example, the continued fraction representation of $\frac{10}{23}$ is given by the sequence [0, 2, 3, 3]. Therefore, the continuants of $\frac{10}{23}$ are

$$0 + \frac{1}{2} = \frac{1}{2}, \quad 0 + \frac{1}{2 + \frac{1}{3}} = \frac{3}{7}, \quad 0 + \frac{1}{2 + \frac{1}{3 + \frac{1}{3}}} = \frac{10}{23}.$$
(7.1)

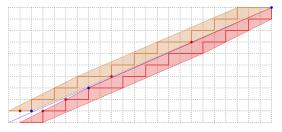


FIGURE 7.1: The convex hulls of the lower Christoffel path from (0,1) to (23,10) and the upper Christoffel path from (1,0) to (23,10).

Theorem[C. Reutenauer, LV, 2017]

Consider $d = \theta \circ \text{Pal}(av)$ with $v \in \{a, b\}^*$. We write $d = d_1 d_2 \cdots d_{|d|}$ with $d_i \in \{a, b\}$. We let $L_0 = L_1 = 1$ and $L_2 = L_1 + L_0 = 2$. For $j \ge 3$ we define recursively the L_j :

$$L_{j} = \begin{cases} L_{j-1} & \text{if } d_{j} = d_{j-1}, \\ L_{j-1} + L_{j-2} & \text{if } d_{j} \neq d_{j-1} \neq d_{j-2}, \\ L_{j-1} + L_{j-2} + L_{j-3} & \text{if } d_{j} \neq d_{j-1} = d_{j-2}. \end{cases}$$

Then the Markoff number m_v is given by

$$m_{\nu}=1+\sum_{j=0}^{|d|}L_j.$$

Consider
$$d_{v} = \theta \circ \text{Pal}(av)$$
 with $v \in \{a, b\}^{*}$.
 $L_{j} = \begin{cases} L_{j-1} & \text{if } d_{j} = d_{j-1}, \\ L_{j-1} + L_{j-2} & \text{if } d_{j} \neq d_{j-1} \neq d_{j-2}, \\ L_{j-1} + L_{j-2} + L_{j-3} & \text{if } d_{j} \neq d_{j-1} = d_{j-2}. \end{cases}$
 $d_{\epsilon} = \theta(a) = ab \text{ and then } \begin{cases} d_{\epsilon} = a & b \\ 1 & 1 & 2 \end{cases}$ and thus $m_{\epsilon} = 1 + (1 + 1 + 2) = 5. \end{cases}$

Consider
$$d_v = \theta \circ \text{Pal}(av)$$
 with $v \in \{a, b\}^*$.
 $L_j = \begin{cases} L_{j-1} & \text{if } d_j = d_{j-1}, \\ L_{j-1} + L_{j-2} & \text{if } d_j \neq d_{j-1} \neq d_{j-2}, \\ L_{j-1} + L_{j-2} + L_{j-3} & \text{if } d_j \neq d_{j-1} = d_{j-2}. \end{cases}$
 $d_{\epsilon} = \theta(a) = ab \text{ and then } \begin{cases} d_{\epsilon} = a & b \\ 1 & 1 & 2 \end{cases}$ and thus $m_{\epsilon} = 1 + (1 + 1 + 2) = 5.$
 $d_a = \theta(aa) = abab \text{ and then } \begin{cases} d_a = a & b & a & b \\ 1 & 1 & 2 & 3 & 5 \end{cases}$
and thus $m_a = 1 + (1 + 1 + 2 + 3 + 5) = 13.$

$L_{j} = \begin{cases} L_{j-1} & \text{if } d_{j} = d_{j-1}, \\ L_{j-1} + L_{j-2} & \text{if } d_{j} \neq d_{j-1} \neq d_{j-2}, \\ L_{j-1} + L_{j-2} + L_{j-3} & \text{if } d_{j} \neq d_{j-1} = d_{j-2}. \end{cases}$
$d_{\epsilon} = heta(a) = ab$ and then $\begin{array}{ccc} d_{\epsilon} = & a & b \\ 1 & 1 & 2 \end{array}$ and thus
$m_{\epsilon} = 1 + (1 + 1 + 2) = 5.$
$d_a = \theta(aa) = abab$ and then $\begin{array}{cccc} d_a = & a & b & a & b \\ 1 & 1 & 2 & 3 & 5 \end{array}$
and thus $m_a = 1 + (1 + 1 + 2 + 3 + 5) = 13$.
$d_{aa}= heta(aaa)=ababab$ and then
d _{aa} = a b a b a b 1 1 2 3 5 8 13 and thus
$m_{aa} = 1 + (1 + 1 + 2 + 3 + 5 + 8 + 13) = 34.$

The directive words $d_{aa\cdots a}$ compute the Markoff numbers that are Fibonacci numbers...

Consider
$$d_v = \theta \circ \text{Pal}(av)$$
 with $v \in \{a, b\}^*$.
 $L_j = \begin{cases} L_{j-1} & \text{if } d_j = d_{j-1}, \\ L_{j-1} + L_{j-2} & \text{if } d_j \neq d_{j-1} \neq d_{j-2}, \\ L_{j-1} + L_{j-2} + L_{j-3} & \text{if } d_j \neq d_{j-1} = d_{j-2}. \end{cases}$
 $d_b = \theta(aba) = abbaab \text{ and then}$
 $d_b = a \ b \ b \ a \ a \ b \\ 1 \ 1 \ 2 \ 2 \ 5 \ 5 \ 12 & \text{and thus}$
 $m_{aa} = 1 + (1 + 1 + 2 + 2 + 5 + 5 + 12) = 29.$

The directive words d_{b^k} compute the Markoff numbers that are Pell numbers...

Consider $d_v = \theta \circ \text{Pal}(av)$ with $v \in \{a, b\}^*$. $L_j = \begin{cases} L_{j-1} & \text{if } d_j = d_{j-1}, \\ L_{j-1} + L_{j-2} & \text{if } d_j \neq d_{j-1} \neq d_{j-2}, \\ L_{j-1} + L_{j-2} + L_{j-3} & \text{if } d_j \neq d_{j-1} = d_{j-2}. \end{cases}$ $d_b = \theta(aba) = abbaab \text{ and then}$ $d_b = a \ b \ b \ a \ a \ b \\ 1 \ 1 \ 2 \ 2 \ 5 \ 5 \ 12 & \text{and thus}$ $m_{aa} = 1 + (1 + 1 + 2 + 2 + 5 + 5 + 12) = 29.$

The directive words d_{b^k} compute the Markoff numbers that are Pell numbers...

$$d_{ab} = \theta(aabaa) = ababbaabab and then$$

 $d_{ab} = a \ b \ a \ b \ b \ a \ a \ b \ a \ b$
1 1 2 3 5 5 13 13 31 44 75
 $m_{ab} = 194.$

Conclusion

We are able to compute all the Markoff numbers by Iterated palindromic closures.

How to prove that the words $Pal \circ \theta \circ Pal(av)$ have two by two distinct lengths?

What are the properties of the L_i 's?

How to use discrete geometry and Christoffel words in order to prove the Frobenius' conjecture ?