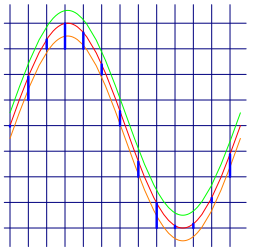
LATTICE POINT PROBLEMS — Math118, O. Knill

ABSTRACT. Finding lattice points close to curves leads to problems in dynamical systems theory.

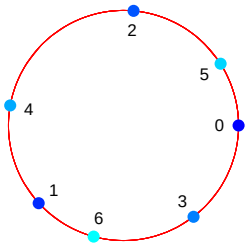
CURVES AND DYNAMICAL SYSTEMS. A curve $r(t) = (t, f(t))$ in the plane defines a sequence of points $x_n = f(n) \bmod 1 = f(n) - [f(n)]$ on the circle $T = R/Z$ and so a dynamical system $T : X \to X$, where X is the closure of all the translates of sequences $x = x_n$ and T is the shift.

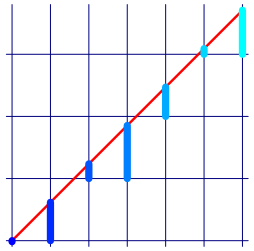
More generally, with the vectors $\vec{x}_n = (x_n, x_{n-1}, ..., x_{n-d})$, we can define a map $T(\vec{x}) = (x_{n+1}, x_n, ..., x_{n-d+1})$ on the d-dimensional torus $T^d = R^d/Z^d$. (For curves in space, there is a map on a higher dimensional torus, for two dimensional surfaces, time becomes two dimensional).



EXAMPLE STURMIAN SEQUENCES.

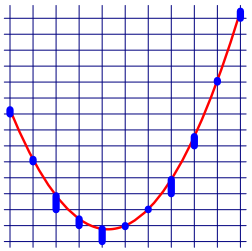
If $r(t) = (t, \alpha t)$ is a line in the plane with slope α, then $x_n = \alpha n \bmod 1$ and $\vec{x} = (..., n\alpha, ...)$ is called a **Sturmian sequence**. The map T is a rotation on the circle. It is a prototype of what one calls an **integrable system**, systems in which one can for example solve the dynamical logarithm problem.





EXAMPLE: PARABOLIC SEQUENCES.

For the parabola $r(t) = (t, \gamma + \alpha t + \beta t^2)$ we obtain the sequence $x_n = \gamma + n\alpha + n^2\beta \bmod 1$. it leads to a measure preserving transformation on the two dimensional torus $T(\begin{bmatrix} x \\ y \end{bmatrix}) = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} 2\alpha \\ 0 \end{bmatrix} = A\vec{x} + \vec{b}$

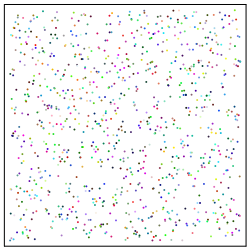


POLYNOMIALS If $p(x)$ is a polynomial of degree n, define $p_n(x) = p(x), p_{n-1}(x) = p_n(x+1) - p_n(x), p_{n-2} = p_{n-1}(x+1) - p_{n-1}(x), .., p_0(x) = \alpha$. Each p_i is a polynomial of degree i. If $T(x_1, x_2, ..., x_n) = (x_1 + \alpha, x + 2 + x_1, ..., x_n + x_{n-1})$, then $T(p_1(n), p_2(n), ..., p_d(n)) = (p_1(n+1), ..., p_d(n+1)) = (p_1(n) + \alpha, p_2(n) + p_1(n), ..., p_d(n) + p_{d-1}(n)$.

QUADATIC CASE: $p_2(x) = \gamma + \beta x + \alpha x^2, p_1(x) = p_2(x+1) - p_2(x) = \alpha + \beta + 2\alpha x, p_0(x) = p_1(x+1) - p_1(x) = 2\alpha$. We have a map $T(x, y) = (x + 2\alpha, x + y)$.

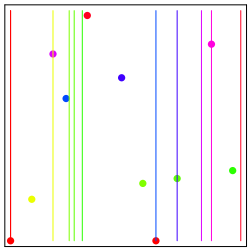
WEAK CHAOS IN PARABOLIC SEQUENCES.

The map $T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2\alpha \\ x + y \end{bmatrix}$ has zero Lyapunov exponent $\frac{1}{n} \lim(\log ||dT^n||)$. There is no sensitive dependence on initial conditions. If α is irrational, then the map has only one invariant measure, the area. The map is also minimal: every orbit is dense. It is not chaotic in the sense of Devaney. It does not have even one single periodic orbit. The map T is an example of a system exhibiting a "weak type of chaos". There is no hyperbolicity present like in the cat map. Still, a single orbit covers the torus densely.



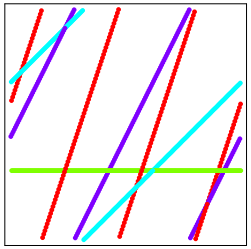
THE INTEGRABLE FACTOR IN PARABOLIC SEQUENCES.

If we look at the lines $y = const$, then these lines are tossed around in a regular way by the dynamics.

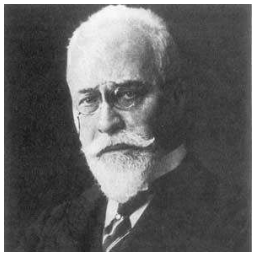


SOME DECAY OF CORRELATIONS.

The system also has mild chaotic behavior. A curve $y = const$ experiences a shear. Lets take a random variable $f(x, y) = f(x)$ which is independent of y. The random variables $f, f(T), ...f(T^n), ...$ show some decay of correlations $\int_{T^2} (f(T^n(x, y))f(x, y) - f(x, y)^2)\, dxdy \to 0$ as time progresses.



WHY CONSTRUCT LATTICE POINTS CLOSE TO CURVES?
0) The problem is relevant in **cryptology**.
1) Estimating points close to curves is a problem in the **matric theory of Diophantine approximation**.
2) Finding points close enough to algebraic curves like $z = \sqrt{p(x)}$ lead to actual rational points on the manifold solving **Diophantine equations**.
3) Estimating lattice points in regions is a problem in the **geometry of numbers**, a field founded by Hermann Minkoswki.
4) It relates to recurrence problems for classes of **dynamical systems**. It is a source for new type of dynamical systems.



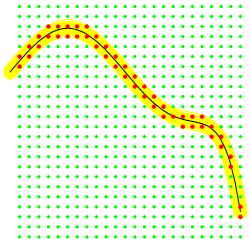
CRYPTOLOGICAL APPLICATION: FACTORING INTEGERS.
Given an integer $n = pq$ which is the product of two prime factors p, q, we want to find numbers y such that $y^2 = O(n^\alpha) \bmod(n)$, with α as small as possible. One way to do that is to look at numbers $[\sqrt{nx}]^2 \bmod n$. More generally, one can look at integer points (x, y) close to the curve $y^2 = np(x)$. As closer we are to the curve, as smaller $y^2 - np(x) = a$ is. Any algorithm which would find a of the order $O(n^\alpha)$ would with $\alpha < 1/2$ improve the speed of the current factorization algorithms.

FACTORING ALGORITHMS. Some of the best factoring algorithms for a composite number $n = pq$ are based on an idea of Fermat: find x such $x^2 \bmod n$ is a small square y^2, then $x^2 - y^2$ is a multiple of n and $gcd(x - y, n)$ likely a factor of n. Example of algorithms are the **Morrison Brillard algorithm**, the **quadratic sieve** or the **number field sieve**. These methods allow to construct x for which y is of the order $\sqrt{n}$. A method to construct numbers x with $x^2 \bmod n$ of the order $n^{1/2-\epsilon}$ for some $\epsilon > 0$ would improve factorization methods.

EXAMPLE: PELL'S EQUATION.
With $p(x, y) = x^2$, the curve $y^2 - nx^2 = 1$ is a hyperbola with asymptotes $y = \pm\sqrt{n}x$. The equation $y^2 = 1 + nx^2$ is called **Pells equation** or **Brouncker equation**. Integer points close to the line $y = \sqrt{n}x$ can be found using the continued fraction algorithm: if $\sqrt{n} \sim y_j/x_j$, then $y_j^2 - nx_j^2 = a$ and $y_j^2 = a \bmod n$. Because $\sqrt{n} = y/x + C/x^2$ we have $x\sqrt{n} - y = C/x$ and $x^2 n - y^2 = (x\sqrt{n} + y)C/x = C\sqrt{n} + Cy/x \sim 2C\sqrt{n}$. Here $\theta = 1/2$.

EXAMPLE PARABOLA. $p_n(x, y) = 2n + x$. The curve $y^2 = np_n(x)$ is a parabola. The tangent at $(x, y) = (0, \sqrt{2n^2 + 1})$ to the curve has slope $n/\sqrt{8n^2 + 1}$. The Diophantine error is $O(1/x)$. The nonlinearity error $y''(0)x^2 \sim x^2 n^2/y^3$. We have $y = O(n)$. In order that $1/x = n^2 x^2/y^3$, we must have $x = n^{1/3}$. The error is then $y/x = n^{2/3}$ so that $\alpha = 2/3$. If we could get rid of the quadratic or cubic erros, α would get smaller.

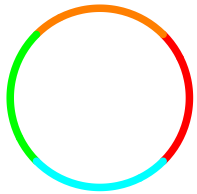
POINTS CLOSE TO A CURVE. The following result is a contribution to the **geometry of numbers**.



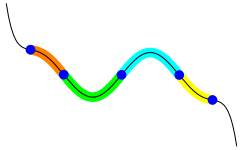
THEOREM. For every $0 \leq \delta < 1/3$ and every three times differentiable curve of finite length, there exists a positive constant C depending only on the curve, such that for all n, the number $M(n,\delta)$ of $1/n$-lattice points in a $1/n^{1+\delta}$ neighborhood of the curve satisfies $M(n,\delta)/n^{1-\delta} \to C$.

Remarks: if the curve is not a line, the constant C is positive. The constant can change under rotations of the curve, but does not change under translation of the curve.

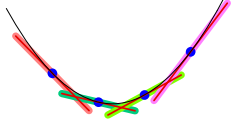
OUTLINE OF THE PROOF.



Cut the curve so that each piece is a graph



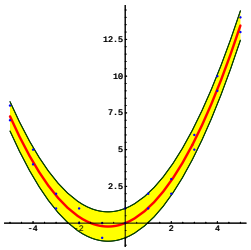
Cut the curve to have line segments or curves with nonzero curvature



Approximate the curve by a polygon with Diophantine slopes

Remark. The polygon pieces have to be large enough so that continued fraction algorithm finds lattice points. On the other hand, the pieces have to be small enough to get a small nonlinearity error. A compromise is possible for $\delta < 1/3$. This bound $1/3$ is a limitation of the method. Results in the **metric theory of Diophantine approximation** indicate that $\delta < 1/2$ should be possible. Numerical experiments suggest that one can go even higher. An approximation by polynomials of higher degree could also put the bound higher. But then the proof no more be **constructive**.

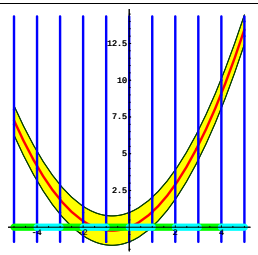
After cutting the curve into pieces, we can reformulate the theorem as follows:



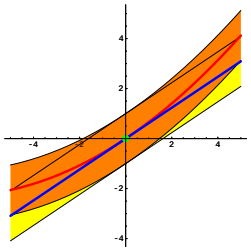
THEOREM (Same result reduced to graph) Given a curve which is the graph of a smooth function $f(t)$ such that $f''(t) \geq \epsilon > 0$ on $[0,1]$. If $M(n,\delta)$ is the number of $1/n$-lattice points between $f(t) - 1/n^{1+\delta}$ and $f(t) + 1/n^{1+\delta}$. Then there is a constant C such that

$$\frac{M(n,\delta)}{n^{1-\delta}} \to C \; .$$

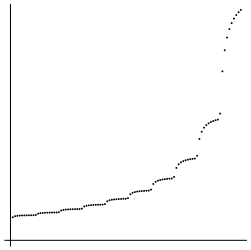
PROOF part (0). Let $[a,b] = f'[0,1]$ be the interval of possible slopes $f'(t)$ of f on $[0,1]$. Choose and fix a number $\delta < \theta < 1/3$ and call $\epsilon = 1/3 - \theta$. Let K be the maximum of $f''(x)$ on the interval $[0,1]$. For every n, divide the interval $[a,b]$ into $r(n,\theta) = [n^{1-\theta}]$ intervals I_k, called **small intervals**. The number of $1/n$-intervals in each of these intervals I_k is $[n^\theta]$. Call $M_k(n,\delta)$ the number of $1/n$ lattice points in the parallelepiped J_k above the interval I_k between $f(t) - 1/n^{1+\delta}$ and $f(t) + 1/n^{1+\delta}$.



RROOF part (i) (Nonlinear error) On one of the small intervals, the discrepancy of the curve to a tangent line is bounded above by $K/n^{2-2\theta} < K/n^{1+\theta+\epsilon}$. This uses Taylors formula $f(x+s) \in [f(x) + f'(x)s - Ks^2, f(x) + f'(x)s + Ks^2]$. It follows that if $M_{k,x}(n,\delta)$ denotes the number of lattice points in a $n^{-(1+\delta)}$ neighborhood J_k of a line segment at x above the interval I_k, then $(M_{k,x}(n,\delta) - M_k(n,\delta))/n^{1-\delta} \to 0$.



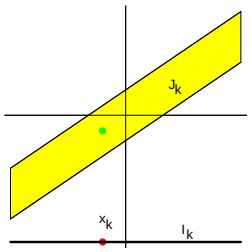
PROOF part (ii) (Sufficiently many strongly Diophantine slopes). Let $h(n,\delta)$ denote the number of intervals I_k, in which we can find x_k for which the slope $f'(x_k) = [a_0; a_1, a_2, ...]$ satisfies $a_i \leq \sqrt{r(n,\delta)}$. Then $h(n,\delta)/r(n,\delta) \to 1$ for $n \to \infty$.
Reformulation: the set of all numbers $y = [u, v, a_1, a_2, ...]$ with $u, v \leq M$ is $1/M^2$ dense on a set $Y_M \subset [0,1]$ with $|Y_M| \to 1$.
A new reformulation: the set $\{ f(u,v,x) = 1/u + 1/(v+x) = (v+x)/(u(v+x)+1) \mid u, v \leq M \}$ for $x \in [0,1]$ is $1/M^2$ dense on a set Y_M which has asymptotically full measure 1. This is a multivariable calculus problem: for $u, v \geq \sqrt{M}$, the distance from one point to the next is of the order $1/M^2$ because $f_v(u,v,x) = 1/(1+u(v+x))^2$.



PROOF part iii) (Reformulation for a line segment). Each of the $h(n,\theta)$ parallelograms J_k above I_k has slope α_k, thickness $n^{-1-\delta}$ and contains $[n^\theta]$ lattice units. In a scale, where the lattice size is 1, we have the following problem:

Estimate the number of lattice points in a parallelogram J_k of length $[n^\theta]$ and thickness $n^{-\delta}$ for which the continued fraction expansion of the slope $\alpha_k = f'(x_k) = \alpha_k = [a_1, a_2, ...]$, with $a_i < n^\delta$.

The answer is that that there are n^ϵ lattice points.



PROOF part iv) (Number of lattice points in a Diophantine parallelogram J_k). There exists $c_k(n), d_k(n)$ such that the line segment J_k contains at least $[c_k(n)n^\epsilon]$ lattice points and maximally $[c_k(n)n^\epsilon]$ lattice points. Furthermore, $c_k(n) \to 1$ and $d_k(n) \to 1$ uniformly in k. There is a more general result of Schmidt and which even gives the error term.

PROOF part v) (Putting things together) The total number $M_{k,x_k}(n,\delta)$ of lattice points is between $c(n)h(n,\delta)n^\epsilon$ and $d(n)h(n,\delta)n^\epsilon$. Because of ii), we know it is between $c(n)r(n,\delta)n^\epsilon = c(n)n^{1-\delta}$ and $d(n)r(n,\delta)n^\epsilon = c(n)n^{1-\delta}$. Dividing by $n^{1-\delta}$ and using $c(n), d(n) \to 1$, we get the result.

AN OPEN PROBLEM. There is an efficient method to solve the dynamical logarithm problem for the map $T(x) = x + \alpha$: the continued fraction expansion gave an efficient method to find lattice points close to a line.

Is there an efficient way to solve the dynamical logarithm problem for

$$T \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2\alpha \\ x + y \end{bmatrix} \; .$$

on the torus. A concrete problem: for $\alpha = \pi$, find n such that $T^n(0.5, 0.5)$ is within distance 10^{-1000} of $(0,0)$.

Geometrically, we look for an efficient method to find lattice points close to the parabola $y = \alpha x^2 + \beta x + \gamma$ with irrational α. Of course, we could just list all numbers $[\alpha n^2 + \beta n + \gamma]$ and see which one is close, this is not practical. While we can find in a few thousand computation steps an integer n such that $[\alpha n]$ is smaller than 10^{-1000} (it is a [P] problem) more then 10^{100} computations seem needed in the parabolic case (is it a [NP] problem?). Note that the big bang happend about 10^{17} seconds ago.