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 \( x_n = f(n) \mod 1 = f(n) - [f(n)] \) 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 vectors \( x_n = (x_n, x_{n+1}, \ldots, x_{n+d}) \), we can define a map \( T(x) = (x_{n+1}, x_{n+2}, \ldots, x_{n+d+1}) \) 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 \( r(t) = (t, t) \) is a line in the plane with slope \( \alpha \), then \( x_n = t \mod \alpha \) and \( F(z, \alpha) = (z, z+\alpha) \) is a Sturmian sequence.

The map \( T \) is a rotation on the circle. It is a prototype of what one calls an integrable system, examples 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 \( x_n = \gamma + \alpha x + \beta x^2 \mod 1 \). It leads to a measure preserving transformation on the two dimensional torus \( T^2 \).

\[
\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2a \\ 0 \end{bmatrix} = A^2 x \\ b
\]

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

QUADATIC CASE: \( p_2(x) = \gamma + 2x + 2x^2 \), \( p_1(x) = p_2(x+1) - p_2(x) = \alpha + 2\alpha x, p_0(x) = p_1(x+1) - p_1(x) = 2\alpha \).

We have a map \( T(x, y) = (x + 2\alpha, x + y) \).

WEAK CHAOS IN PARABOLIC SEQUENCES.

The map \( T \) has zero Lyapunov exponent \( \frac{1}{2} \lim \log |dT^T|/|dT^T| \). There is no sensitive dependence on initial conditions. If \( \alpha \) 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 INTEGRAL 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. Let's take a random variable \( f(x, y) = f(x) \) which is independent of \( y \). The random variables \( f(T), f(T^2), \ldots \) show some decay of correlations \( \int_0^1 f(T^k(x, y)) f(x, y) \, dx \to 0 \) as \( k \) progresses.

WHY CONSTRUCT LATTICE POINTS CLOSE TO CURVES?

0) The problem is relevant in cryptography.
1) Estimating points close to curves is a problem in the modern 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 Minkowski.
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.

The equation \( y^2 = ax^2 + b \) is a parabola. The tangent at \( (x, y) \) is \( y' = \frac{2ax}{2y} = \frac{ax}{y} \) like in the cat map. Still, a single orbit covers the torus densely.

FACTORIZATION ALGORITHMS. Some of the best factoring algorithms for a composite number \( n = pq \) are based on an idea of Fermat: find \( x \) such that \( x^2 \mod n \) is a small square \( y^2 \), then \( y^2 = x^2 - y^2 \mod n \) 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 \( x^2 \mod n \) of the order \( n^{1/2} \) for some \( \epsilon > 0 \) would improve factorization methods.

EXAMPLE PELL’S EQUATION.

With \( p(y, y) = x^2 \), the curve \( y^2 = x^2 - 1 \) is a hyperbola with asymptotes \( y = \pm x \). The equation \( y^2 + 1 = xz^2 \) is called Pell’s equation or Brouncker equation. Integer points close to the line \( x = y \) can be found using the continued fraction algorithm: if \( \sqrt{y} \approx y_1/y_2 \), then \( y_1^2 - y_2^2 = a \) and \( y_2 = a \mod n \). Because \( y_1 = y_2 + x^2 \mod n \) we have \( x_2 = y - y_1 = y_1^2 + x^2 \) and \( x_2 - y_1 = (x_1 y_1 + y_1)C/x = C + Cy_1^2 + C/x_2 \). Here \( \theta = 1/2 \).

EXAMPLE PARABOLA. \( p_2(x, y) = 2u + x \). The curve \( y^2 = x^2 + y^2 \) is a parabola. The tangent at \( (x, y) = (0, \sqrt{2} + 1) \) to the curve has slope \( n/\sqrt{8n^2 + 1} \). The Diophantine error is \( E(1/x) \). The nonlinearity error \( y^2(x)^2 \mod n \). We have \( y = O(n) \). In order that \( 1/x = n^{1/2} \mod n \), we must have \( x = n^{1/3} \). The error is then \( y_1/x = n^{1/3} \) so that \( \alpha = 2/3 \). If we could get rid of the quadratic or cubic error, \( \alpha \) 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 $M(n, \delta)/n^{1-\delta} \rightarrow C$.

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.

PROOF part (i) (Nonlinear error) On one of the small intervals, the discrepancy of the curve to a tangent line is bounded above by $K/n^{2-2\delta} < K/n^{1+\delta}/n$. This uses Taylor's formula $f(x + \delta) \approx f(x) + f'(x)\delta - K\delta^2$ (for $0 < \delta < 1/3$). It follows that if $M_{\text{loss}}(\delta)$ denotes the number of lattice points in a $1/n^{1+\delta}$ neighborhood $I_k$ of a line segment at $x$ above the interval $I_k$, then $(M_{\text{loss}}(\delta) - M_k(\delta))/n^{1-\delta} \rightarrow 0$.

PROOF part (ii) (Sufficiently many strongly Diophantine slopes). Let $h(n, \delta)$ denote the number of intervals $I_k$, in which we can find $x_2$ such that $f'(x_2) = [a_0; a_1, a_2, \ldots]$ satisfies $a_0 \leq \sqrt{K/n}$. Then $h(n, \delta)/\tau(n, \delta) \rightarrow 1$ for $n \rightarrow \infty$.

Reformulation: the set of all numbers $y = [u, v, a_0, a_1, a_2, \ldots]$ with $u, v, w \leq M$ is $1/M^2$ dense on a set $Y_M \subset [0, 1]$ with $|Y_M| \rightarrow 1$. A new reformulation: the set $f(u, v, x) = g(u)/(u + x + 1)$ 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 $f(x, r, v) = (1 + u/(u + v))^2$.

The answer is that there are $n^2$ lattice points.

PROOF part (iii) (Reformulation for a line segment). Each of the $h(n, \delta)$ parallelograms $J_k$ above $I_k$ has slope $\alpha_k$, thickness $\alpha_k^{-1}d$ and contains $\lceil n^2 \rceil$ 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 $n^2$ and thickness $\alpha_k^{-1}$ for which the continued fraction expansion of the slope $\alpha_k = f'(x_2) = \alpha_k = [a_0; a_1, a_2, \ldots]$ with $a_0 < n^2$.

The answer is that there are $n^2$ lattice points.

PROOF part iv) (Number of lattice points in a Diophantine parallelogram $J_k$). There exists $c_0(n, d_k(n))$ such that the line segment $J_k$ contains at least $c_0(n, \alpha_k^n)$ lattice points and maximally $c_0(n, \alpha_k^n)$ lattice points. Furthermore, $c_0(n) \rightarrow 1$ and $d_k(n) \rightarrow 1$ uniformly in $k$. There is a more general result of Schmidt and which even gives the error term.

AN OPEN PROBLEM. There is an efficient method to solve the dynamical logarithm problem for the map $T(x, y) = x + \alpha$, 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 $T(x, y) = x + \alpha$ 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 $y = ax^2 + bx + c$ with irrational $a$. Of course, we could just list all numbers $[an^2 + bn + c]$ and see which one is closest, this is not practical. While we can find in a few thousand computation steps an integer $n$ such that $[an]$ is smaller than $10^{-1000}$ (it is a $[P]$ problem) more than $10^{1000}$ computations seem needed in the parabolic case (is it a $[NP]$ problem?). Note that the big bang happened about $10^{17}$ seconds ago.