Fibonacci, Kronecker and Hilbert

NKS 2007

Klaus Sutner
Carnegie Mellon University
www.cs.cmu.edu/~sutner

Overview

- Fibonacci, Kronecker and Hilbert ???
- Logic and Decidability
- Additive Cellular Automata
- A Knuth Question
- Some Questions

Hilbert

Entscheidungsproblem

The Entscheidungsproblem is solved when one knows a procedure by which one can decide in a finite number of operations whether a given logical expression is generally valid or is satisfiable. The solution of the Entscheidungsproblem is of fundamental importance for the theory of all fields, the theorems of which are at all capable of logical development from finitely many axioms.

D. Hilbert, W. Ackermann
Grundzüge der theoretischen Logik, 1928

Model Checking

The Entscheidungsproblem for the 21. Century.

Shift to computer science, even commercial applications.

Fix some suitable logic $\mathcal{L}$ and collection of structures $\mathcal{A}$.

Find efficient algorithms to determine

$$\mathfrak{A} \models \varphi$$

for any structure $\mathfrak{A} \in \mathcal{A}$ and sentence φ in $\mathcal{L}$.

Variants: fix φ, fix $\mathfrak{A}$.

CA as Structures

Discrete dynamical systems, minimalist description:

$$\mathfrak{A}_\rho = \langle \mathcal{C}, \rightarrow \rangle$$

where $\mathcal{C} \subseteq \Sigma^{\mathbb{Z}}$ is the space of *configurations* of the system and $\rightarrow$ is the "next configuration" relation induced by the local map ρ.

Use standard first order logic (either relational or functional) to describe properties of the system.

Some Formulae

$$\forall\, x \exists\, y\, (y \to x)$$

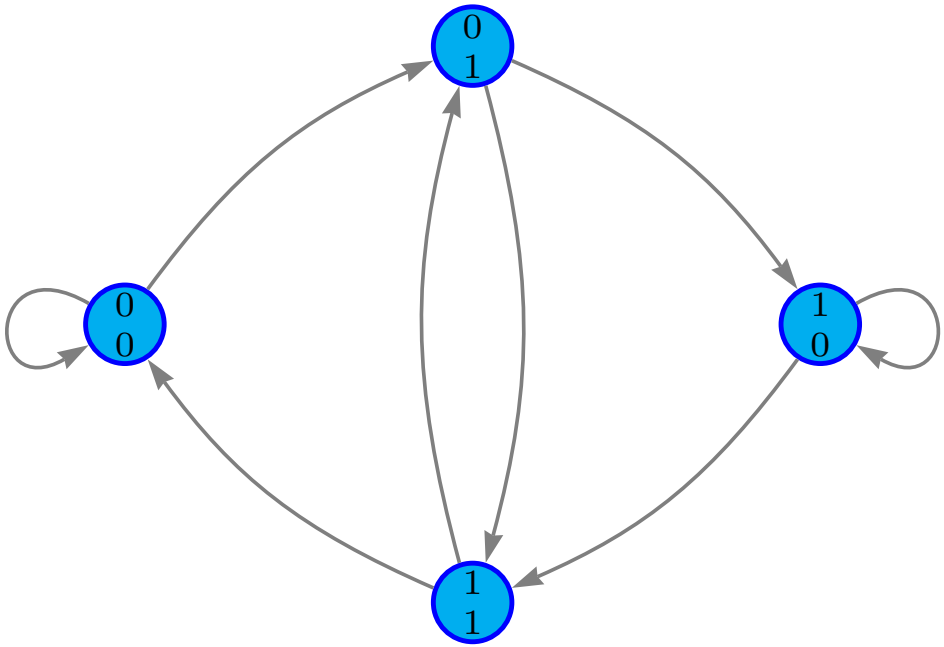
$$\forall\, x, y, z\, (x \to z \wedge y \to z \Rightarrow x = y)$$

$$\forall\, x \exists\, y, z\, (y \to x \wedge z \to x \wedge \forall\, u\, (u \to x \Rightarrow u = y \vee u = z))$$

There is no computability requirement for configurations, in $x \to y$ both x and y may be complicated.

∞-Automata

Express $x \to y$ in terms of finite state machines on infinite words, ditto for equality.



Local map $\rho(x, y, z) = y \oplus z$.

Automata to Logic

These are essentially Büchi automata.

Much like ordinary FSMs, but the acceptance condition involve infinitary quantifiers.

The emptiness problem for these automata is easily decidable.

Regular languages on infinite words are closed under union, complementation and projection, corresponding operations on automata are effective.

Theorem. *Model checking is decidable in this case.*

Comments

- Amoroso and Patt 1972: decidability of reversibility and surjectivity using a combinatorial argument.
- KS 1991: efficient quadratic time algorithm.
- J. Kari 1990: undecidable in dimensions 2 and higher.

Orbits

Unfortunately, the reachability relation

$$x \xrightarrow{*} y$$

is undecidable, even in dimension 1. So for any logic strong enough to express orbits (MSO, TrCl, . . .) model checking is undecidable.

Stronger classifications are even more hopeless. E.g.

- decidability of orbits is Σ_3-complete,
- computationally universality is Σ_4-complete.

Scaling Back

How about considering only finite grids?

Then reachability

$$x \xrightarrow{*} y$$

is PSPACE-complete.

Caution, though: uniform problems may still be undecidable. E.g.

$$\forall\, x \,\exists\, z \,(x \xrightarrow{*} z \wedge z \to z)$$

is Π_1-complete.

Fibonacci and Kronecker

Additive CA

Scale back much further: consider only additive local rules on finite grids.

For simplicity consider only $\mathbb{F}_2$.

Generalize the classical elementary CA 150 and 90.

σ-Automata

Let $G = \langle V, E \rangle$ be some locally finite undirected graph, $\mathcal{C} = V \to \mathbf{2}$ the space of all configurations over G.

$$\sigma : \mathcal{C} \longrightarrow \mathcal{C}$$

$$\sigma(X)(v) = \sum_{u \in N(v)} X(u) \bmod 2.$$

where $N(v)$ is the closed neighborhood of v (including v). Open neighborhood: σ^-.

Boring

In a sense, these CA are boring (predictable): for n cells we can determine the state of a cell at time t in

$$O(n^3 \log t)$$

steps, so we are far from usual PSPACE-completeness.

But not too boring . . .

Not Too Boring

Finding predecessors is just linear algebra over $\mathbb{F}_2$, can be done in time polynomial in $n = |V|$.

Theorem. *Existence of a predecessor of bounded cardinality over* $\mathbb{F}_2$ *is* $\mathbb{NP}$*-complete.*

Let $M = \langle a, a^2 = a^3 \rangle$ (three element abelian monoid $\{0, 1, a\}$).

Theorem. *Existence of a predecessor over* M *is* $\mathbb{NP}$*-complete.*

Transition Diagram

We want a computationally simple description of the transition diagram, or pattern space

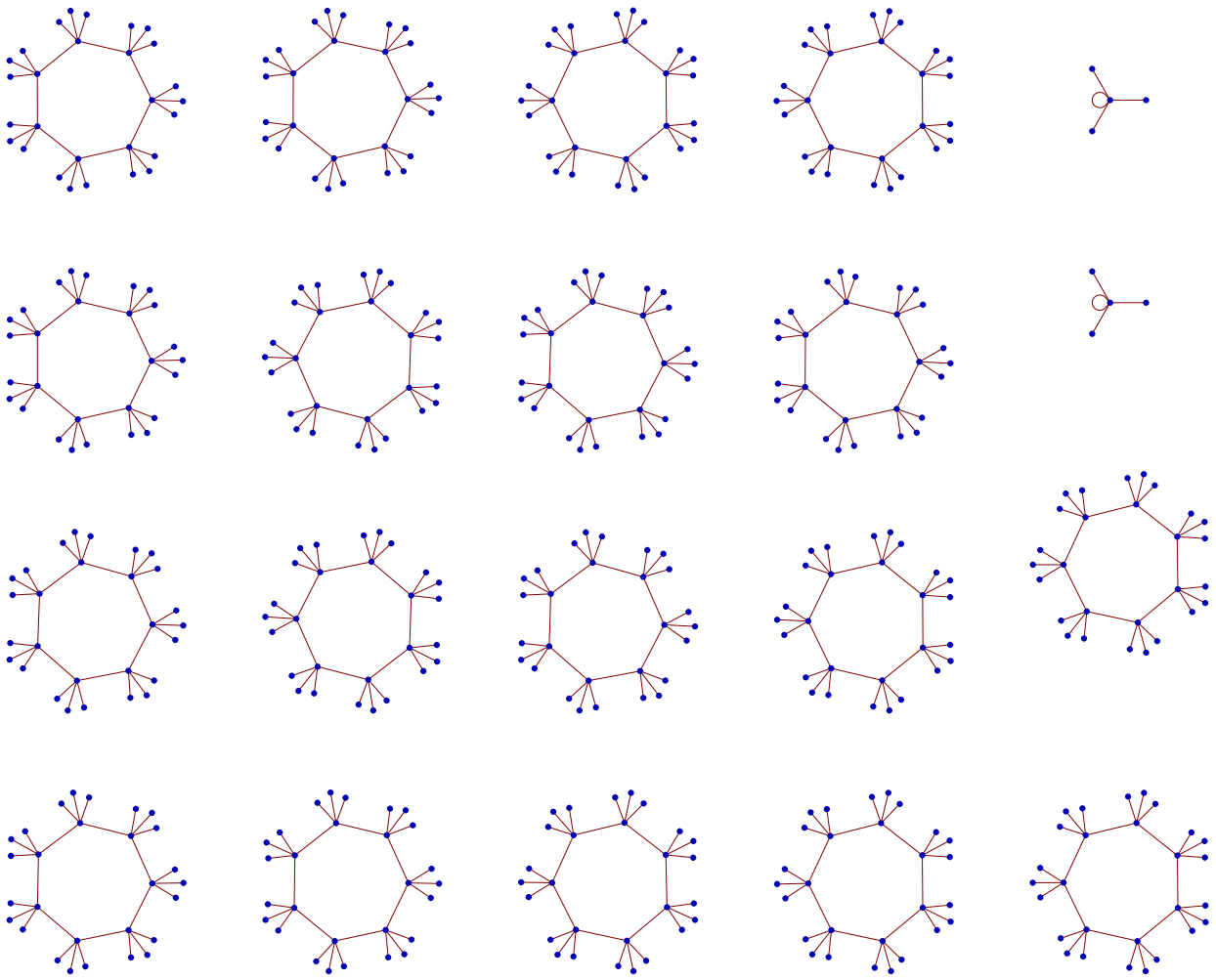
$$\langle \mathcal{C}, \sigma \rangle \text{ where } \mathcal{C} = V \to \mathbf{2}$$

Fitting-decomposition:

$$\mathcal{C} = K \oplus E$$

where K is the nilpotent part and E the regular part (with respect to linear operator σ).

Transition Diagram



Fibonacci

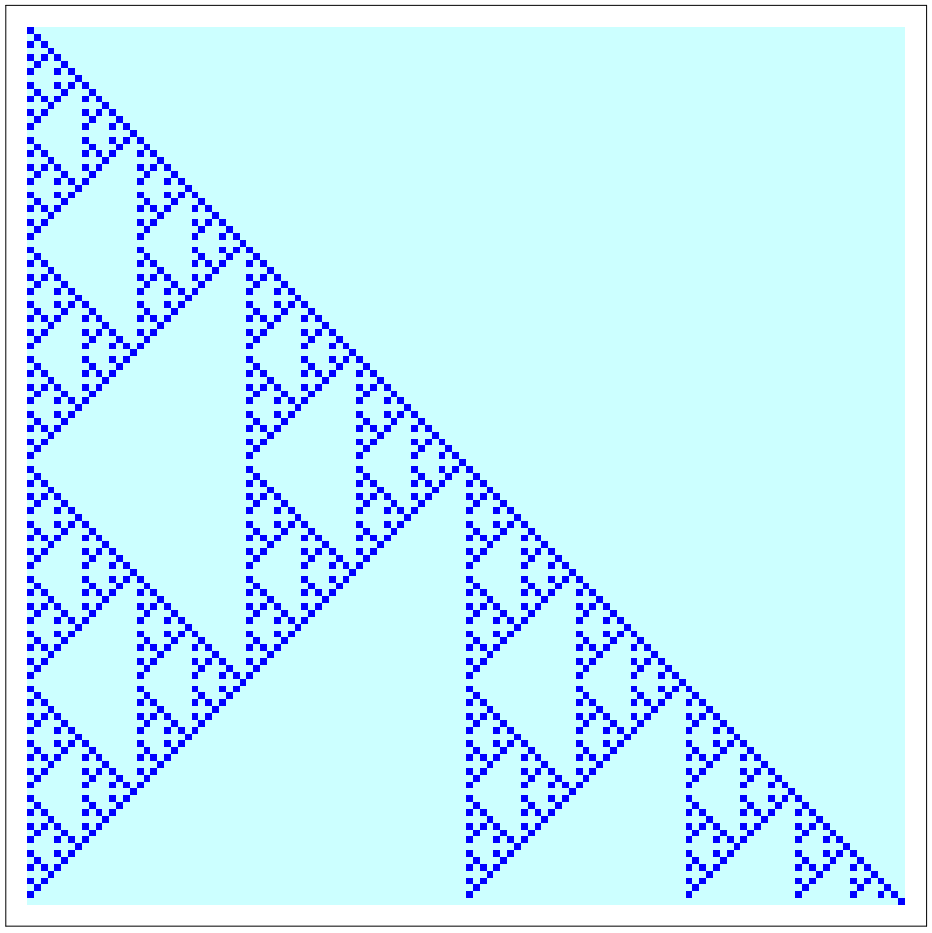
Define the *binary Fibonacci polynomials* over $\mathbb{F}_2[x]$ as follows:

$$\begin{aligned}\pi_0(x) &= 0,\\ \pi_1(x) &= 1,\\ \pi_n(x) &= x \cdot \pi_{n-1}(x) + \pi_{n-2}(x).\end{aligned}$$

For example, $\pi_{111}(x)$ has the form

$$1+x^8+x^{12}+x^{14}+x^{16}+x^{64}+x^{72}+x^{76}+x^{78}+x^{80}+x^{96}+x^{104}+x^{108}+x^{110}$$

Coefficients of Fibonacci Polynomials



Minimal Polynomials for Dim 1

For one-dimensional paths P_n we can determine the minimal polynomials.

Theorem. *The minimal polynomial of σ^- on a path of length n is $\pi_{n+1}(x)$. For cyclic boundary condition we have $\sqrt{x\,\pi_n(x)}$ for even n, and $x\sqrt{\pi_n(x)}$ for odd n.*

The minimal polynomials for σ are then $\pi_{n+1}(x+1)$ and so forth.

Note that $x \mapsto x+1$ is an involution of $\mathbb{F}_2[x]$, so the multiplicative structure of the Fibonacci polynomials is preserved.

Higher Dimensions

How about grid graphs $P_{n,m}$, with pattern space

$$\langle \mathcal{C}, \sigma \rangle \quad \text{where} \quad \mathcal{C} = [n] \times [m] \to \mathbf{2}$$

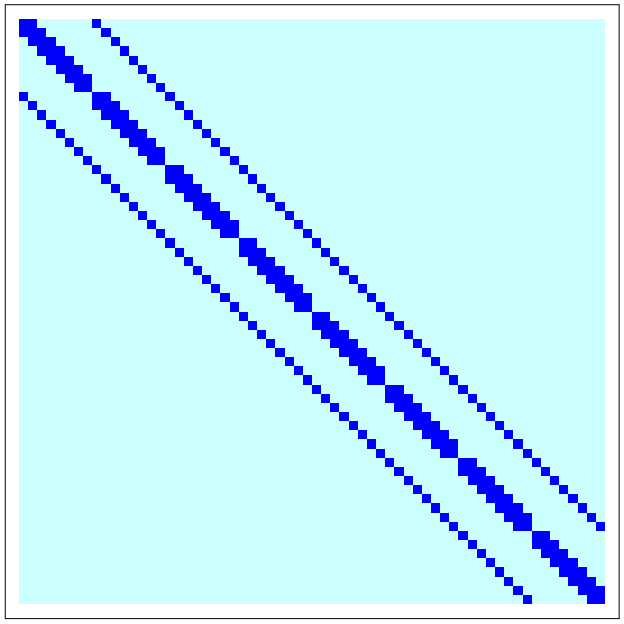
For simplicity, focus on just one question:

- How hard is it to check reversibility on an n by m grid?

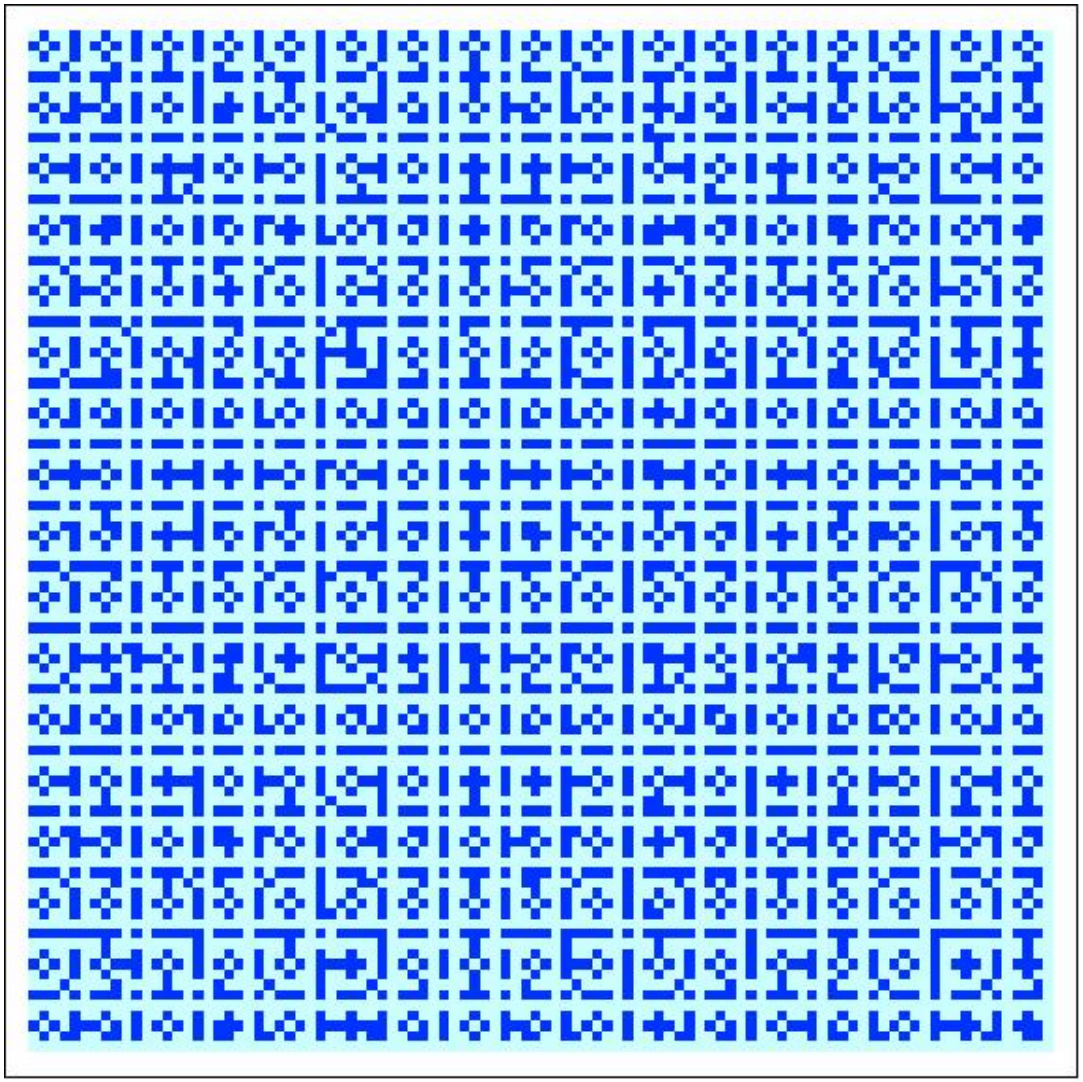
Kronecker

The matrix representation of σ is a Kronecker matrix, the adjacency matrix of the grid graph, plus the diagonal.

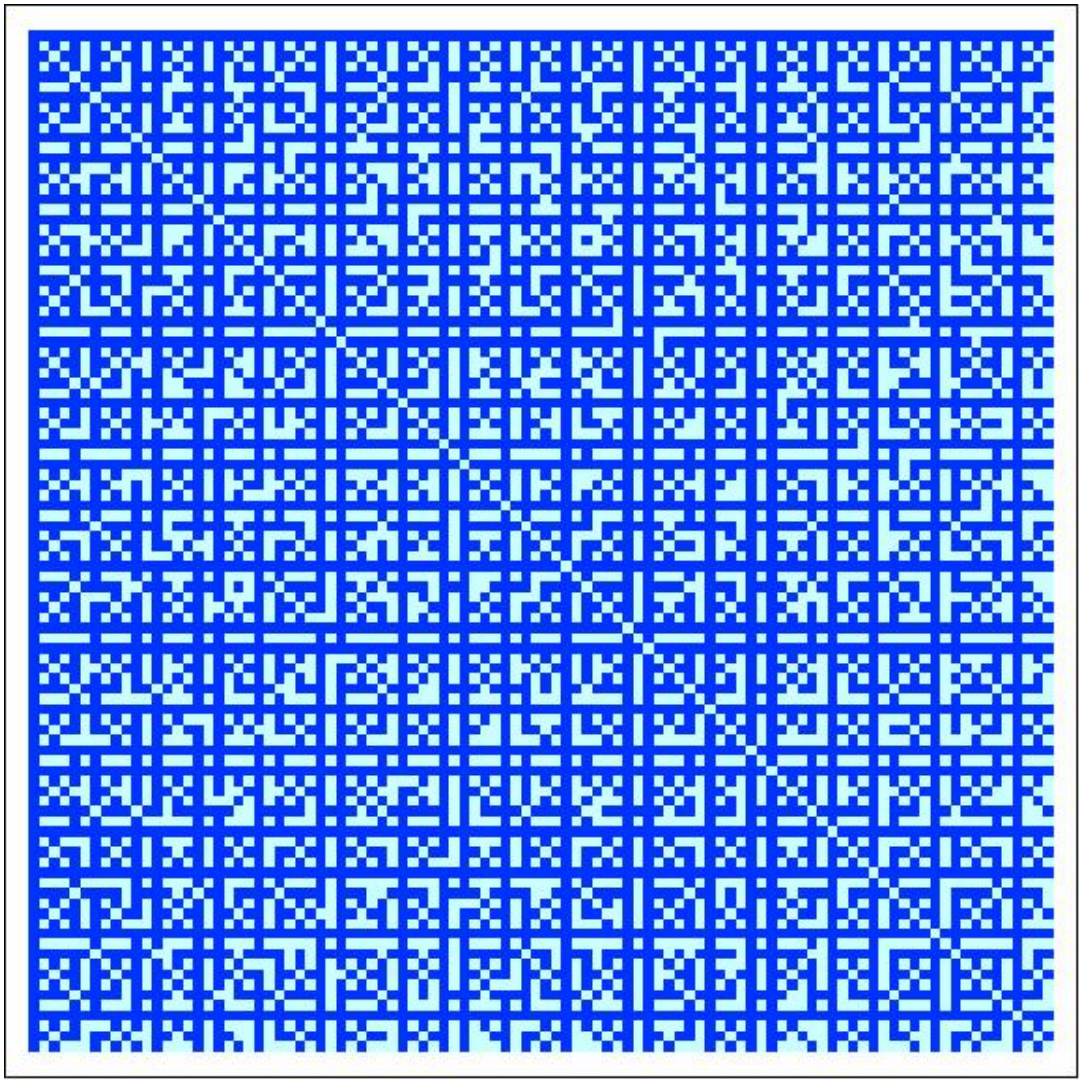
So we need to compute the nullspace of this matrix.



Reversibility



Reversibility with σ^-



Divisibility

Much better: the dimension of the kernel of σ^- on $P_{n,m}$ is just

$$\gcd(n+1, m+1) - 1.$$

For σ^- simple divisibility of integers is insufficient.

The necessary computations can be handled in time polynomial in $\log nm$.

So reversibility here is easy even given a succinct representation.

How much more difficult can $\sigma = \sigma^- + I$ be?

Characterizing Reversibility

Theorem. *The dimension of the kernel of σ on $P_{n,m}$ is*

$$\deg \gcd(\, \pi_{n+1}(x), \pi_{m+1}(x+1)\,).$$

Note the involution $x \mapsto x+1$.

Again a divisibility problem, but time polynomial in $\log nm$ no longer suffices.

But perhaps we can analyze the divisibility properties of the binary Fibonacci polynomials to find a computational shortcut?

The involution preserves irreducibles, so a factorization would be useful.

Rank of Apparition

Every irreducible polynomial τ divides some π_n so so there is a notion of *rank of apparition*:

$$\mathrm{rap}(\tau) = \min\big(\, k \mid \tau \text{ divides } \pi_k \,\big)$$

Dates back at least to work by M.Ward and L.K.Durst, Lucas-Lehmer Test.

Factorization

Theorem. *Let $n = 2^k \cdot m$, m odd. Then*

$$\pi_n(x) = x^{2^k-1} \prod_{d|m} \rho_d^{2^k}(x) = x^{2^k-1} \prod_{d|m} \rho_d(x^{2^k})$$

Here the $\rho_d(x)$ are (squares of) products of irreducibles of rank d.

For odd n we have

$$\pi_n(x) = \prod_{d|n} \rho_d(x)$$

The Source of All Evil

. . . is the involution $x \mapsto x + 1$.

$$\pi_n(x) = \ldots \tau(x) \ldots$$
$$\pi_n(x+1) = \ldots \tau(x+1) \ldots$$

Clearly $\tau(x+1)$ is again irreducible and has the same degree as $\tau(x)$.

But what happens to the rank of apparition of $\tau(x+1)$?

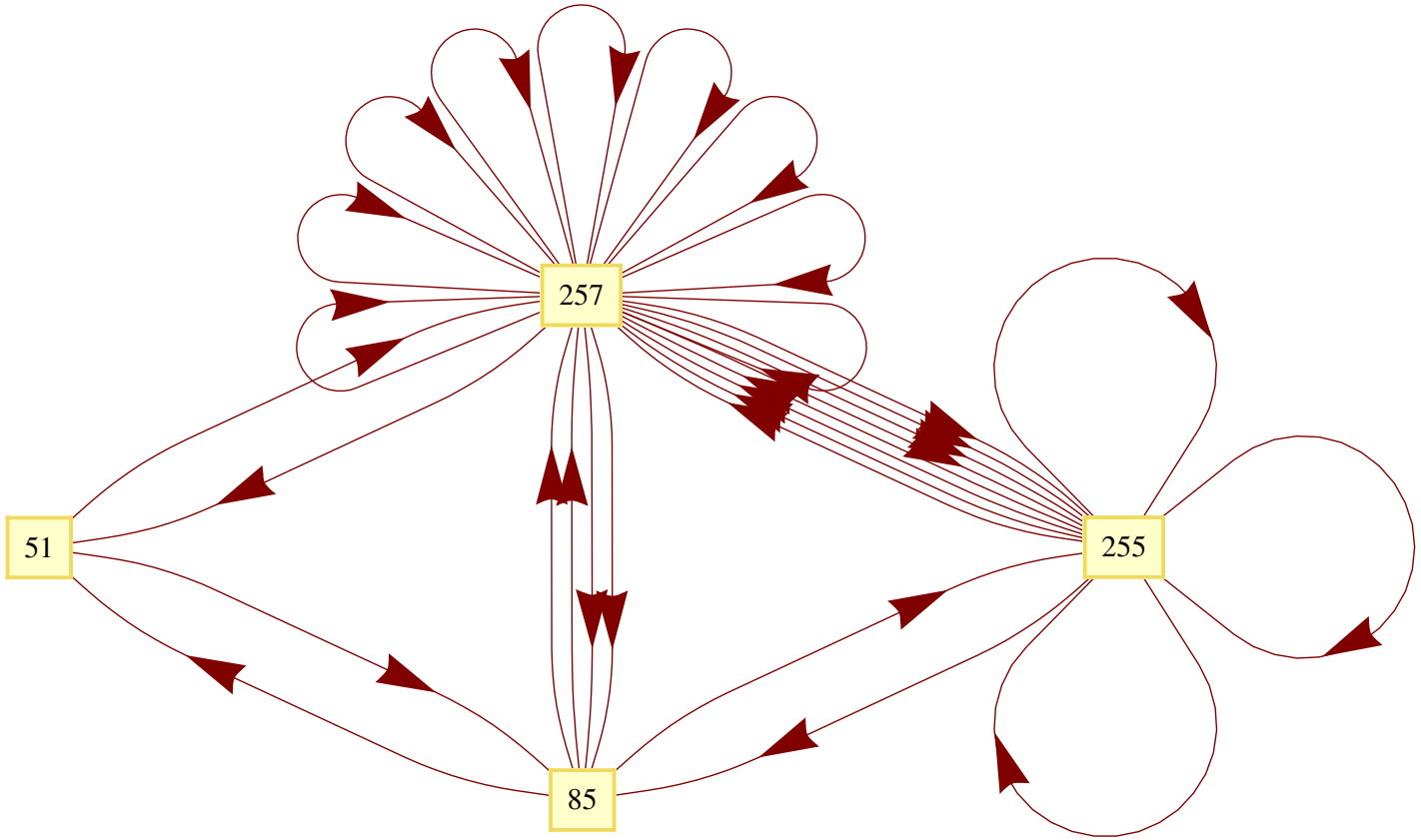
Pinning Down Rank

Little can be said about the rank of τ.

Theorem. *Let $\tau \in \mathbb{F}_2[x]$ be an irreducible polynomial of degree d and k its rank of apparition. Then k divides $2^d - 1$ if, and only if, the linear term in τ vanishes, and $2^d + 1$ otherwise.*

In either case, d is the suborder of 2 in the multiplicative group $\mathbb{Z}_k^*$.

Changing Rank



Application: Reversibility Test

Theorem. *For any fixed $m \geq 1$ there are positive integers $t_1, \ldots, t_r$ such that rule σ on $P_{n,m}$ is reversible if, and only if, none of the t_i divides $n+1$.*

The test can be handled in time polynomial in $\log n$, but computation of the t_i appears to require

- the factorization of $\pi_{m+1}(x)$,
- computation of the rank of apparition of the corresponding irreducible factors.

Application: Total Irreversibility

The dimension of the kernel of σ on $P_{n,m}$ is at most $\min(n, m)$. Call the automaton totally irreversible if it attains this bound.

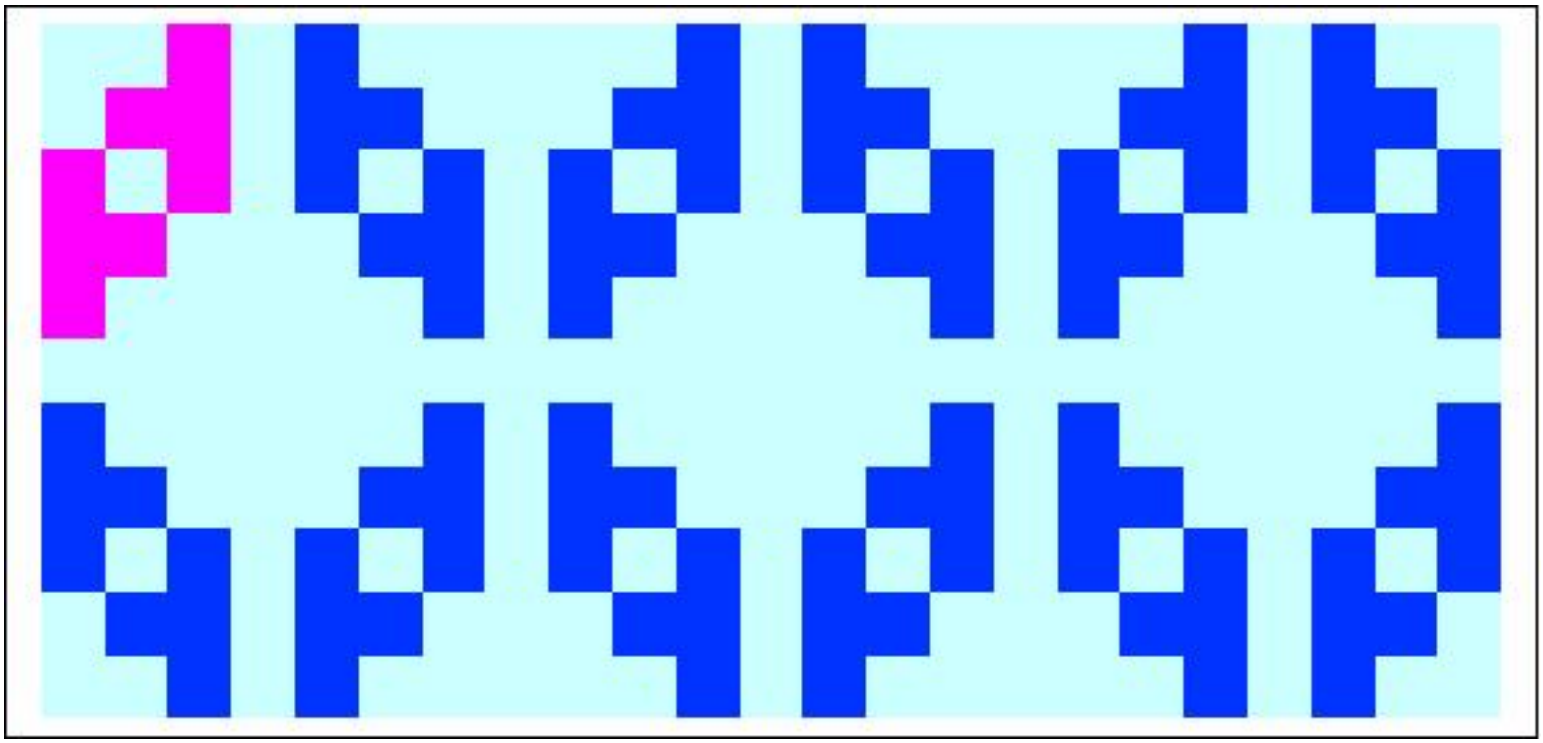
Theorem. *P. Sarkar*

$n = 4$ *is the only totally irreversible square.*

Proof quite hard.

A Knuth Question

Kernel Patterns



From 5×3 to 11×23.

A Multiplicative Sequence

For simplicity consider only irreversible squares:

$$\mathsf{Irr} = \{\, n \mid \gcd(\pi_n(x), \pi_n(x+1)) \neq 1 \,\}$$

so that the first few terms of Irr are

$$5, 6, 10, 12, 15, 17, 18, 20, 24, 25, 30, 31, 33, 34, 35, 36, 40, 42, 45, 48, 50, 51, \ldots$$

The sequence is multiplicatively closed, so the question arises: what are the generators:

$$5, 6, 17, 31, 33, 63, 127, 129, 171, 257, 511, 683, 2047, 2731, 2979, 3277, \ldots$$

Not Finitely Generated

Theorem. *The sequence* Irr *is not finitely generated.*

$n \in$ Irr iff for some irreducible τ_1, τ_2 factors of π_n: $\tau_1(x) = \tau_2(x+1)$.

Sketch of proof:

Focus on $\tau(x) = \tau(x+1)$: translation invariant irreducible polynomial.

So we only need to find lots of TIPs.

TIPs

The number of TIPS of degree d is $2^{d/2+1}$ for even d, and 0 otherwise.

Consider the invariant

$$\widehat{f}(x) = f(x(x+1))$$

Lemma. *Let f be irreducible of degree d.*

Then either $\widehat{f}$ is TIP or $\widehat{f}(x) = f_1(x)\, f_2(x)$ where the f_i's are TIP.

Moreover, $\widehat{f}$ is TIP iff $[x^{d-1}]\widehat{f} = 1$.

Counting Irreducibles

Building on work by Niederreiter one can count irreducible polynomials of degree d with fixed coefficients c_1 and c_{d-1}.

Let $\omega_{1/2} = (-1 \pm i\sqrt{7})/2$ be the two complex roots of $x^2 - x + 2 = 0$.

Lemma. *Let $k \geq 4$ and write $k = k_0 k_1$ where k_0 is a power of 2 and k_1 is odd.*

$$N_k^{ab} = \frac{1}{4k} \sum_{d \mid k} \mu(k_1/d) \left(2^{k_0 d} + (-1)^{a+b}(1 - \omega_1^{n_0 d} - \omega_2^{n_0 d}) - [a = b = 0, k_1 = 1]\, 4 \cdot 2^{n_0/2d} \right)$$

Infinitely Many Generators

For any odd prime k there is a TIP g_k of degree $2k$ whose rank of apparition divides $2^{2k} - 1$.

But then there cannot be finitely many generators:

$$d \mid \gcd(\operatorname{rap} g_{k_1}, \operatorname{rap} g_{k_2}) \mid \gcd(2^{2k_1} - 1, 2^{2k_2} - 1) = 3.$$

Pinning Down Rank

Lemma. *Let $d = \mathrm{sord}_n(2)$ where $n > 2$. Then the number of irreducible polynomials of degree d and rank of apparition n is $\varphi(n)/2d$.*

Main idea: attack Fibonacci polynomials via bivariate cyclotomic polynomials

$$\Phi_n(x, y) = \Pi_{k \mid n}(x^k + y^k)^{\mu(n/k)}$$

More precisely, express the critical factor ρ_n in terms of symmetric reducts of Φ_n:

$$\rho_n^2 = \mathsf{SR}(\Phi_n(x, y)) \Big|_{y=1}$$

Questions

Logic

- What is the complexity of model checking for CA with FOL?
- Is there any interesting logic $\mathcal{L}$ with decidable model checking for one-dimensional CA?
- How about subclasses of CA?
- How about finite CA (finite grids)?
- Is the theory of Wolfram Class III the same as Class IV?

Additive Automata

- Understand the rank of apparition of $\tau(x+1)$.
- Is reversibility testing for two-dimensional σ-automata polynomial in $\log nm$?
- Pin down the complexity of analyzing reversibility for algebraic dynamical systems.
- Pin down the complexity of analyzing the transition diagram for algebraic dynamical systems.