Lecture 2: More on cellular automata

- Surjective CA: balance, Garden-of-Eden -theorem
- Injectivity and surjectivity on periodic configurations
Garden-Of-Eden and orphans

Configurations that do not have a pre-image are called Garden-Of-Eden -configurations. Only non-surjective CA have GOE configurations.

A finite pattern consists of a finite domain $D \subseteq \mathbb{Z}^d$ and an assignment

$$p : D \rightarrow S$$

of states.

Finite pattern is called an orphan for CA $G$ if every configuration containing the pattern is a GOE.
From the compactness of $S^{\mathbb{Z}^d}$ we directly get:

**Proposition.** Every GOE configuration contains an orphan pattern.

Non-surjectivity is hence equivalent to the existence of orphans.
Balance in surjective CA

All surjective CA have **balanced** local rules: for every \( a \in S \)

\[ |f^{-1}(a)| = |S|^{n-1}. \]
All surjective CA have **balanced** local rules: for every $a \in S$

$$|f^{-1}(a)| = |S|^{n-1}.$$ 

Indeed, consider a non-balanced local rule such as rule 110 where five contexts give new state 1 while only three contexts give state 0:

<table>
<thead>
<tr>
<th>Input</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>0</td>
</tr>
<tr>
<td>110</td>
<td>1</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>1</td>
</tr>
<tr>
<td>010</td>
<td>1</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
</tr>
<tr>
<td>000</td>
<td>0</td>
</tr>
</tbody>
</table>
Consider finite patterns where state 0 appears in every third position. There are \(2^{2(k-1)} = 4^{k-1}\) such patterns where \(k\) is the number of 0’s.
Consider finite patterns where state 0 appears in every third position. There are $2^{2(k-1)} = 4^{k-1}$ such patterns where $k$ is the number of 0’s.

A pre-image of such a pattern must consist of $k$ segments of length three, each of which is mapped to 0 by the local rule. There are $3^k$ choices.

As for large values of $k$ we have $3^k < 4^{k-1}$, there are fewer choices for the red cells than for the blue ones. Hence some pattern has no pre-image and it must be an orphan.
One can also verify directly that pattern

\[ 01010 \]

is an orphan of rule 110. It is the shortest orphan.
Balance of the local rule is not sufficient for surjectivity. For example, the **majority** CA (Wolfram number 232) is a counter example. The local rule

\[ f(a, b, c) = 1 \text{ if and only if } a + b + c \geq 2 \]

is clearly balanced, but 01001 is an orphan.
The balance property of surjective CA generalizes to finite patterns of arbitrary shape:

**Theorem:** Let $G$ be surjective. Let $M, D \subseteq \mathbb{Z}^d$ be finite domains such that $D$ contains the neighborhood of $M$. Then every finite pattern with domain $M$ has the same number

$$n|D| - |M|$$

of pre-images in domain $D$, where $n$ is the number of states. □
The balance property of surjective CA generalizes to finite patterns of arbitrary shape:

**Theorem:** Let $G$ be surjective. Let $M, D \subseteq \mathbb{Z}^d$ be finite domains such that $D$ contains the neighborhood of $M$. Then every finite pattern with domain $M$ has the same number

$$n|D| - |M|$$

of pre-images in domain $D$, where $n$ is the number of states. □

The balance property means that the uniform probability measure is **invariant** for surjective CA. (Uniform randomness is preserved by surjective CA.)
Let us call configurations \( c_1 \) and \( c_2 \) asymptotic if the set

\[
\text{diff}(c_1, c_2) = \{ \vec{n} \in \mathbb{Z}^d \mid c_1(\vec{n}) \neq c_2(\vec{n}) \}
\]

of positions where \( c_1 \) and \( c_2 \) differ is finite.

A CA is called **pre-injective** if any asymptotic \( c_1 \neq c_2 \) satisfy

\[
G(c_1) \neq G(c_2).
\]
The Garden-Of-Eden -theorem by Moore (1962) and Myhill (1963) connects surjectivity with pre-injectivity.

**Theorem:** CA $G$ is surjective if and only if it is pre-injective.
The **Garden-Of-Eden -theorem** by Moore (1962) and Myhill (1963) connects surjectivity with pre-injectivity.

**Theorem:** CA $G$ is surjective if and only if it is pre-injective.

The proof idea can be easily explained using rule 110 as a running example.
1) \( G \) not surjective \( \implies \) \( G \) not pre-injective:

Since rule 110 is not surjective it has an orphan 01010 of length five. Consider a segment of length \( 5k - 2 \), for some \( k \), and configurations \( c \) that are in state 0 outside this segment. There are \( 2^{5k-2} = 32^k/4 \) such configurations.
1) $G$ not surjective $\implies$ $G$ not pre-injective:

The non-0 part of $G(c)$ is within a segment of length $5k$. Partition this segment into $k$ parts of length 5. Pattern 01010 cannot appear in any part, so only $2^5 - 1 = 31$ different patterns show up in the subsegments. There are at most $31^k$ possible configurations $G(c)$. 
1) $G$ not surjective $\implies G$ not pre-injective:

The non-0 part of $G(c)$ is within a segment of length $5k$. Partition this segment into $k$ parts of length $5$. Pattern $01010$ cannot appear in any part, so only $2^5 - 1 = 31$ different patterns show up in the subsegments. There are at most $31^k$ possible configurations $G(c)$.

As $32^k/4 > 31^k$ for large $k$, there are more choices for red than blue segments. So there must exist two different red configurations with the same image. 

□
2) $G$ not pre-injective $\implies G$ not surjective:

In rule 110

\[
\begin{array}{c}
p \\
0 0 1 1 0 1 0 0 \\
\downarrow \\
1 1 1 1 1 1 0
\end{array}
\quad
\begin{array}{c}
q \\
0 0 1 0 1 1 0 0 \\
\downarrow \\
1 1 1 1 1 1 0
\end{array}
\]

so patterns $p$ and $q$ of length 8 can be exchanged to each other in any configuration without affecting its image. There exist just

\[2^8 - 1 = 255\]

essentially different blocks of length 8.
2) \( G \) not pre-injective \( \implies \) \( G \) not surjective:

Consider a segment of \( 8k \) cells, consisting of \( k \) parts of length 8. Patterns \( p \) and \( q \) are exchangeable, so the segment has at most \( 255^k \) different images.
2) $G$ not pre-injective $\implies G$ not surjective:

Consider a segment of $8k$ cells, consisting of $k$ parts of length 8. Patterns $p$ and $q$ are exchangeable, so the segment has at most $255^k$ different images.

There are, however, $2^{8k-2} = 256^k/4$ different patterns of size $8k-2$. Because $255^k < 256^k/4$ for large $k$, there are blue patterns without any pre-image.
Garden-Of-Eden -theorem: CA $G$ is surjective if and only if it is pre-injective.
Garden-Of-Eden -theorem: CA $G$ is surjective if and only if it is pre-injective.

Corollary: Every injective CA is also surjective. Injectivity, bijectivity and reversibility are equivalent concepts.

Proof: If $G$ is injective then it is pre-injective. The claim follows from the Garden-Of-Eden -theorem.
G injective $\iff$ G bijective $\iff$ G reversible

G surjective $\iff$ G pre-injective
Examples:

The majority rule is not surjective: finite configurations

\[ \ldots 0000000 \ldots \quad \text{and} \quad \ldots 0001000 \ldots \]

have the same image, so $G$ is not pre-injective. Pattern

\[ 01001 \]

is an orphan.
Examples:

In Game-Of-Life a lonely living cell dies immediately, so $G$ is not pre-injective. GOL is hence not surjective.
Interestingly, no small orphans are known for Game-Of-Life. Currently, the smallest known orphan consists of 92 cells (56 life, 36 dead):

M. Heule, C. Hartman, K. Kwekkeboom, A. Noels (2011)
Examples:

The Traffic CA is the elementary CA number 226.

\[
\begin{align*}
111 & \rightarrow 1 \\
110 & \rightarrow 1 \\
101 & \rightarrow 1 \\
100 & \rightarrow 0 \\
011 & \rightarrow 0 \\
010 & \rightarrow 0 \\
001 & \rightarrow 1 \\
000 & \rightarrow 0
\end{align*}
\]

The local rule replaces pattern 01 by pattern 10.
111 → 1
110 → 1
101 → 1
100 → 0
011 → 0
010 → 0
001 → 1
000 → 0
The table shows a mapping of binary sequences to integers and colors:

- 111 → 1
- 110 → 1
- 101 → 1
- 100 → 0
- 011 → 0
- 010 → 0
- 001 → 1
- 000 → 0

Each row represents a binary sequence, and the corresponding integer or color is indicated.
<table>
<thead>
<tr>
<th>Binary</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>1</td>
</tr>
<tr>
<td>110</td>
<td>1</td>
</tr>
<tr>
<td>101</td>
<td>1</td>
</tr>
<tr>
<td>100</td>
<td>0</td>
</tr>
<tr>
<td>011</td>
<td>0</td>
</tr>
<tr>
<td>010</td>
<td>0</td>
</tr>
<tr>
<td>001</td>
<td>1</td>
</tr>
<tr>
<td>000</td>
<td>0</td>
</tr>
<tr>
<td>Four-Digit Value</td>
<td>Corresponding Value</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>111</td>
<td>→ 1</td>
</tr>
<tr>
<td>110</td>
<td>→ 1</td>
</tr>
<tr>
<td>101</td>
<td>→ 1</td>
</tr>
<tr>
<td>100</td>
<td>→ 0</td>
</tr>
<tr>
<td>011</td>
<td>→ 0</td>
</tr>
<tr>
<td>010</td>
<td>→ 0</td>
</tr>
<tr>
<td>001</td>
<td>→ 1</td>
</tr>
<tr>
<td>000</td>
<td>→ 0</td>
</tr>
</tbody>
</table>
The local rule is balanced. However, there are two finite configurations with the same successor:

![Diagram demonstrating two finite configurations with the same successor.]

and hence traffic CA is not surjective.
There is an orphan of size four:
G injective $\Leftrightarrow$ G bijective $\Leftrightarrow$ G reversible

G surjective $\Leftrightarrow$ G pre-injective
G injective ⇔ G bijective ⇔ G reversible

G surjective ⇔ G pre-injective

XOR
The xor-CA is the binary state CA with neighborhood \((0, 1)\) and local rule

\[ f(a, b) = a + b \pmod{2}. \]
The xor-CA is the binary state CA with neighborhood \((0, 1)\) and local rule

\[ f(a, b) = a + b \pmod{2}. \]

In the xor-CA every configuration has exactly two pre-images, so \(G\) is surjective but not injective:

One can freely choose one value in the pre-image, after which all remaining states are uniquely determined by the **left-permutativity** and the **right-permutativity** of xor.
The xor-CA is the binary state CA with neighborhood $(0, 1)$ and local rule

\[ f(a, b) = a + b \pmod{2}. \]

In the xor-CA every configuration has exactly two pre-images, so $G$ is surjective but not injective:

One can freely choose one value in the pre-image, after which all remaining states are uniquely determined by the **left-permutativity** and the **right-permutativity** of xor.
The xor-CA is the binary state CA with neighborhood \((0, 1)\) and local rule

\[ f(a, b) = a + b \pmod{2}. \]

In the xor-CA every configuration has exactly two pre-images, so \(G\) is surjective but not injective:

One can freely choose one value in the pre-image, after which all remaining states are uniquely determined by the left-permutativity and the right-permutativity of xor.
The xor-CA is the binary state CA with neighborhood \((0, 1)\) and local rule

\[ f(a, b) = a + b \pmod{2}. \]

In the xor-CA every configuration has exactly two pre-images, so \(G\) is surjective but not injective:

One can freely choose one value in the pre-image, after which all remaining states are uniquely determined by the left-permutativity and the right-permutativity of xor.
The xor-CA is the binary state CA with neighborhood \((0, 1)\) and local rule
\[
f(a, b) = a + b \pmod{2}.
\]

In the xor-CA every configuration has exactly two pre-images, so \(G\) is surjective but not injective:

One can freely choose one value in the pre-image, after which all remaining states are uniquely determined by the **left-permutativity** and the **right-permutativity** of xor.
The xor-CA is the binary state CA with neighborhood \((0, 1)\) and local rule 
\[
f(a, b) = a + b \pmod{2}.
\]

In the xor-CA every configuration has exactly two pre-images, so \(G\) is surjective but not injective:

One can freely choose one value in the pre-image, after which all remaining states are uniquely determined by the **left-permutatativity** and the **right-permutatativity** of xor.
The two pre-images of the finite configuration

\begin{align*}
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\end{align*}

are both infinite:

\begin{align*}
\begin{array}{cccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\end{array}
\end{align*}

So $G$ is not surjective on 0-finite configurations.
Surjectivity and injectivity of $G_P$

Let $G_P$ denote the restriction of cellular automaton $G$ on (fully) periodic configurations.

Implications

$G$ injective $\implies G_P$ injective

$G_P$ surjective $\implies G$ surjective

are easy. (Second one uses denseness of periodic configurations in $S^\mathbb{Z}^d$.)
We also have

\[ G_P \text{ injective } \implies G_P \text{ surjective} \]
We also have

\[ \mathbf{G}_P \text{ injective} \implies \mathbf{G}_P \text{ surjective} \]

Indeed, fix any \( d \) linearly independent periods, and let \( A \subseteq S^{\mathbb{Z}^d} \) be the set of configurations with these periods. Then

- \( A \) is finite,
- \( G \) is injective on \( A \),
- \( G(A) \subseteq A \).

We conclude that \( G(A) = A \), and every periodic configuration has a periodic pre-image.
Here we get the first \textbf{dimension sensitive} property. The following equivalences are only known to hold among one-dimensional CA:

\[ G \text{ injective} \iff G_P \text{ injective} \]
\[ G \text{ surjective} \iff G_P \text{ surjective} \]
Here we get the first **dimension sensitive** property. The following equivalences are only known to hold among one-dimensional CA:

\[
\begin{align*}
\text{G injective} & \iff \text{G}_P \text{ injective} \\
\text{G surjective} & \iff \text{G}_P \text{ surjective}
\end{align*}
\]

- The first equivalence is not true among two-dimensional CA: counter example **Snake-XOR** will be seen tomorrow.
- It is not known whether the second equivalence is true in 2D.
Only in 1D

G injective $\leftrightarrow$ G bijective $\leftrightarrow$ G reversible $\leftrightarrow$ $G_P$ injective

G surjective $\leftrightarrow$ G pre-injective $\leftrightarrow$ $G_P$ surjective

XOR
In 2D

G injective $\leftrightarrow$ G bijective $\leftrightarrow$ G reversible

G surjective $\leftrightarrow$ G pre-injective

$G_P$ injective

$G_P$ surjective

Snake-XOR

XOR

？
We have two proofs that injective CA are surjective:

\[ \text{G injective} \implies \text{G pre-injective} \implies \text{G surjective} \]

\[ \text{G injective} \implies \text{G}_P \text{ injective} \implies \text{G}_P \text{ surjective} \implies \text{G surjective} \]
We have two proofs that injective CA are surjective:

\[ G \text{ injective} \implies G \text{ pre-injective} \implies G \text{ surjective} \]

\[ G \text{ injective} \implies G_P \text{ injective} \implies G_P \text{ surjective} \implies G \text{ surjective} \]

It is good to have both implication chains available, if one wants to generalize results to cellular automata whose underlying grid is not \( \mathbb{Z}^d \) but some other group.

- The first chain generalizes to all \textbf{amenable} groups.
- The second chain generalizes to \textbf{residually finite} groups.

A group is called \textbf{surjunctive} if every injective CA on the group is also surjective. It is not known if all groups are surjunctive.