# Cryptographic applications of very large cardinals

Joseph Van Name

2017

# Topics

B

L

Algebra-Self-distributive algebras

Set theory-Rank-into-rank cardinals

T

# Laver-like algebras

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and
2. whenever $x_n \in X$ for $n \in \omega$, there is some $N \in \omega$ with $x_0 * \cdots * x_N \in \mathrm{Li}(X)$ (Parentheses are grouped on the left. i.e. $x * y * z = (x * y) * z$).

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and
2. whenever $x_n \in X$ for $n \in \omega$, there is some $N \in \omega$ with $x_0 * \cdots * x_N \in \mathrm{Li}(X)$ (Parentheses are grouped on the left. i.e. $x * y * z = (x * y) * z$).

If $(X, *)$ is a Laver-like algebra, then define the Fibonacci terms $t_n$ for $n \geq 1$ by letting $t_1(x, y) = y, t_2(x, y) = x$, and $t_{n+2}(x, y) = t_{n+1}(x, y) * t_n(x, y)$. Then for all $x, y$ there is some $n$ where $t_n(x, y) \in \mathrm{Li}(X)$.

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and
2. whenever $x_n \in X$ for $n \in \omega$, there is some $N \in \omega$ with $x_0 * \cdots * x_N \in \mathrm{Li}(X)$ (Parentheses are grouped on the left. i.e. $x * y * z = (x * y) * z$).

If $(X, *)$ is a Laver-like algebra, then define the Fibonacci terms $t_n$ for $n \geq 1$ by letting $t_1(x, y) = y, t_2(x, y) = x$, and $t_{n+2}(x, y) = t_{n+1}(x, y) * t_n(x, y)$. Then for all $x, y$ there is some $n$ where $t_n(x, y) \in \mathrm{Li}(X)$. Define an associative operation $\circ$ on $X \setminus \mathrm{Li}(X)$ by letting $x \circ y = t_{n+1}(x, y)$ where $n$ is chosen such that $t_n(x, y) \in \mathrm{Li}(X)$.

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and
2. whenever $x_n \in X$ for $n \in \omega$, there is some $N \in \omega$ with $x_0 * \cdots * x_N \in \mathrm{Li}(X)$ (Parentheses are grouped on the left. i.e. $x * y * z = (x * y) * z$).

If $(X, *)$ is a Laver-like algebra, then define the Fibonacci terms $t_n$ for $n \geq 1$ by letting $t_1(x, y) = y, t_2(x, y) = x$, and $t_{n+2}(x, y) = t_{n+1}(x, y) * t_n(x, y)$. Then for all $x, y$ there is some $n$ where $t_n(x, y) \in \mathrm{Li}(X)$. Define an associative operation $\circ$ on $X \setminus \mathrm{Li}(X)$ by letting $x \circ y = t_{n+1}(x, y)$ where $n$ is chosen such that $t_n(x, y) \in \mathrm{Li}(X)$.

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and
2. whenever $x_n \in X$ for $n \in \omega$, there is some $N \in \omega$ with $x_0 * \cdots * x_N \in \mathrm{Li}(X)$ (Parentheses are grouped on the left. i.e. $x * y * z = (x * y) * z$).

If $(X, *)$ is a Laver-like algebra, then define the Fibonacci terms $t_n$ for $n \geq 1$ by letting $t_1(x, y) = y, t_2(x, y) = x$, and $t_{n+2}(x, y) = t_{n+1}(x, y) * t_n(x, y)$. Then for all $x, y$ there is some $n$ where $t_n(x, y) \in \mathrm{Li}(X)$. Define an associative operation $\circ$ on $X \setminus \mathrm{Li}(X)$ by letting $x \circ y = t_{n+1}(x, y)$ where $n$ is chosen such that $t_n(x, y) \in \mathrm{Li}(X)$.

# Laver-like algebras

A self-distributive algebra is an algebra $(X, *)$ that satisfies the identity $x * (y * z) = (x * y) * (x * z)$.

Suppose $(X, *)$ is self-distributive. An element $x \in X$ is said to be a left-identity if $x * y = y$ for all $y \in X$. Let $\mathrm{Li}(X)$ denote the set of all left-identities in $X$. We say that a subset $L \subseteq X$ is a left-ideal if $y \in L$ implies $x * y \in L$.

A self-distributive algebra $(X, *)$ is Laver-like if

1. $\mathrm{Li}(X)$ is a left-ideal in $X$, and
2. whenever $x_n \in X$ for $n \in \omega$, there is some $N \in \omega$ with $x_0 * \cdots * x_N \in \mathrm{Li}(X)$ (Parentheses are grouped on the left. i.e. $x * y * z = (x * y) * z$).

If $(X, *)$ is a Laver-like algebra, then define the Fibonacci terms $t_n$ for $n \geq 1$ by letting $t_1(x, y) = y, t_2(x, y) = x$, and $t_{n+2}(x, y) = t_{n+1}(x, y) * t_n(x, y)$. Then for all $x, y$ there is some $n$ where $t_n(x, y) \in \mathrm{Li}(X)$. Define an associative operation $\circ$ on $X \setminus \mathrm{Li}(X)$ by letting $x \circ y = t_{n+1}(x, y)$ where $n$ is chosen such that $t_n(x, y) \in \mathrm{Li}(X)$.

# Large cardinals

# Large cardinals

- Rank-into-rank, $j : V_\lambda \to V_\lambda$-Laver-like algebras $\mathcal{E}_\lambda$.
- $n$-huge-Laver-like algebras.
- Extendible-Laver-like algebras.
- Supercompact
- Woodin
- Measurable
- Ramsey
- Erdos
- Indescribable
- Weakly compact
- Mahlo
- Inaccessible

# Algebras of elementary embeddings

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$.
$(\mathcal{E}_\lambda, *)$ is self-distributive.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$.
$(\mathcal{E}_\lambda, *)$ is self-distributive.

If $\gamma$ is a limit ordinal with $\gamma < \lambda$, then define a congruence $\equiv^\gamma$ on $(\mathcal{E}_\lambda, *)$ by letting $j \equiv^\gamma k$ iff $j(x) \cap V_\gamma = k(x) \cap V_\gamma$ for all $x \in V_\gamma$.
Then $(\mathcal{E}_\lambda / \equiv^\gamma, *)$ is a Laver-like algebra.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$. $(\mathcal{E}_\lambda, *)$ is self-distributive.

If $\gamma$ is a limit ordinal with $\gamma < \lambda$, then define a congruence $\equiv^\gamma$ on $(\mathcal{E}_\lambda, *)$ by letting $j \equiv^\gamma k$ iff $j(x) \cap V_\gamma = k(x) \cap V_\gamma$ for all $x \in V_\gamma$. Then $(\mathcal{E}_\lambda / \equiv^\gamma, *)$ is a Laver-like algebra.

(ZFC) If $n$ is a natural number, then there is a unique algebra $A_n = (\{1, \ldots, 2^n\}, *)$ such that

1. $x * (y * z) = (x * y) * (x * z)$, and
2. $x * 1 = x + 1 \mod 2^n$ for all $x, y, z$

which we shall call a classical Laver table.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$. $(\mathcal{E}_\lambda, *)$ is self-distributive.

If $\gamma$ is a limit ordinal with $\gamma < \lambda$, then define a congruence $\equiv^\gamma$ on $(\mathcal{E}_\lambda, *)$ by letting $j \equiv^\gamma k$ iff $j(x) \cap V_\gamma = k(x) \cap V_\gamma$ for all $x \in V_\gamma$. Then $(\mathcal{E}_\lambda / \equiv^\gamma, *)$ is a Laver-like algebra.

(ZFC) If $n$ is a natural number, then there is a unique algebra $A_n = (\{1, \ldots, 2^n\}, *)$ such that

1. $x * (y * z) = (x * y) * (x * z)$, and
2. $x * 1 = x + 1 \mod 2^n$ for all $x, y, z$

which we shall call a classical Laver table.

Classical Laver tables are Laver-like and every Laver-like algebra generated by a single element is isomorphic to some $A_n$.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$. $(\mathcal{E}_\lambda, *)$ is self-distributive.

If $\gamma$ is a limit ordinal with $\gamma < \lambda$, then define a congruence $\equiv^\gamma$ on $(\mathcal{E}_\lambda, *)$ by letting $j \equiv^\gamma k$ iff $j(x) \cap V_\gamma = k(x) \cap V_\gamma$ for all $x \in V_\gamma$. Then $(\mathcal{E}_\lambda / \equiv^\gamma, *)$ is a Laver-like algebra.

(ZFC) If $n$ is a natural number, then there is a unique algebra $A_n = (\{1, \ldots, 2^n\}, *)$ such that

1. $x * (y * z) = (x * y) * (x * z)$, and
2. $x * 1 = x + 1 \mod 2^n$ for all $x, y, z$

which we shall call a classical Laver table.

Classical Laver tables are Laver-like and every Laver-like algebra generated by a single element is isomorphic to some $A_n$.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$. $(\mathcal{E}_\lambda, *)$ is self-distributive.

If $\gamma$ is a limit ordinal with $\gamma < \lambda$, then define a congruence $\equiv^\gamma$ on $(\mathcal{E}_\lambda, *)$ by letting $j \equiv^\gamma k$ iff $j(x) \cap V_\gamma = k(x) \cap V_\gamma$ for all $x \in V_\gamma$. Then $(\mathcal{E}_\lambda / \equiv^\gamma, *)$ is a Laver-like algebra.

(ZFC) If $n$ is a natural number, then there is a unique algebra $A_n = (\{1, \ldots, 2^n\}, *)$ such that

1. $x * (y * z) = (x * y) * (x * z)$, and
2. $x * 1 = x + 1 \mod 2^n$ for all $x, y, z$

which we shall call a classical Laver table.

Classical Laver tables are Laver-like and every Laver-like algebra generated by a single element is isomorphic to some $A_n$.

# Algebras of elementary embeddings

The existence of a non-trivial elementary embedding $j : V_\lambda \to V_\lambda$ is among the strongest of all large cardinal axioms.

Let $\mathcal{E}_\lambda$ be the set of all elementary embeddings $j : V_\lambda \to V_\lambda$. Then define an operation $*$ on $\mathcal{E}_\lambda$ by letting $j * k = \bigcup_{\alpha<\lambda} j(k|V_\alpha)$. $(\mathcal{E}_\lambda, *)$ is self-distributive.

If $\gamma$ is a limit ordinal with $\gamma < \lambda$, then define a congruence $\equiv^\gamma$ on $(\mathcal{E}_\lambda, *)$ by letting $j \equiv^\gamma k$ iff $j(x) \cap V_\gamma = k(x) \cap V_\gamma$ for all $x \in V_\gamma$. Then $(\mathcal{E}_\lambda / \equiv^\gamma, *)$ is a Laver-like algebra.

(ZFC) If $n$ is a natural number, then there is a unique algebra $A_n = (\{1, \ldots, 2^n\}, *)$ such that

1. $x * (y * z) = (x * y) * (x * z)$, and
2. $x * 1 = x + 1 \mod 2^n$ for all $x, y, z$

which we shall call a classical Laver table.

Classical Laver tables are Laver-like and every Laver-like algebra generated by a single element is isomorphic to some $A_n$.

# $n+1$-ary self-distributivity

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

If $(X, t)$ is an $n+1$-ary self-distributive algebra, then define the hull $\Gamma(X, t) = (X^n, *)$ where $*$ is the binary operation defined by $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n))$.

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

If $(X, t)$ is an $n+1$-ary self-distributive algebra, then define the hull $\Gamma(X, t) = (X^n, *)$ where $*$ is the binary operation defined by $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n))$. Then $\Gamma(X, t)$ is a self-distributive algebra.

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

If $(X, t)$ is an $n+1$-ary self-distributive algebra, then define the hull $\Gamma(X, t) = (X^n, *)$ where $*$ is the binary operation defined by $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n))$. Then $\Gamma(X, t)$ is a self-distributive algebra. We say that an $n+1$-ary self-distributive algebra $(X, t)$ is Laver-like if its hull $\Gamma(X, t)$ is Laver-like.

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

If $(X, t)$ is an $n+1$-ary self-distributive algebra, then define the hull $\Gamma(X, t) = (X^n, *)$ where $*$ is the binary operation defined by $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n))$. Then $\Gamma(X, t)$ is a self-distributive algebra. We say that an $n+1$-ary self-distributive algebra $(X, t)$ is Laver-like if its hull $\Gamma(X, t)$ is Laver-like.

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

If $(X, t)$ is an $n+1$-ary self-distributive algebra, then define the hull $\Gamma(X, t) = (X^n, *)$ where $*$ is the binary operation defined by $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n))$. Then $\Gamma(X, t)$ is a self-distributive algebra. We say that an $n+1$-ary self-distributive algebra $(X, t)$ is Laver-like if its hull $\Gamma(X, t)$ is Laver-like.

# $n+1$-ary self-distributivity

Suppose that $t$ is an $n+1$-ary operation on a set $X$. Then $t$ is said to be self-distributive if it satisfies the identity

$$t(x_1, \ldots, x_n, t(y_1, \ldots, y_n, y))$$

$$= t(t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n), t(x_1, \ldots, x_n, y)).$$

If $t : X^{n+1} \to X$, then for $a_1, \ldots, a_n \in X$, define $L_{t,a_1,\ldots,a_n} : X \to X$ by letting $L_{t,a_1,\ldots,a_n}(x) = t(a_1, \ldots, a_n, x)$. Then $t$ is self-distributive iff each $L_{t,a_1,\ldots,a_n}$ is an endomorphism of $(X, t)$.

If $(X, t)$ is an $n+1$-ary self-distributive algebra, then define the hull $\Gamma(X, t) = (X^n, *)$ where $*$ is the binary operation defined by $(x_1, \ldots, x_n) * (y_1, \ldots, y_n) = (t(x_1, \ldots, x_n, y_1), \ldots, t(x_1, \ldots, x_n, y_n))$. Then $\Gamma(X, t)$ is a self-distributive algebra. We say that an $n+1$-ary self-distributive algebra $(X, t)$ is Laver-like if its hull $\Gamma(X, t)$ is Laver-like.

# Functional endomorphic Laver tables-Part 1

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\wr : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\wr : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.
5. If $\mathfrak{l}(1\mathbf{x}) \in X$, then there is some $x \in X$ where $t^\bullet(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x}), x) = \mathfrak{l}(\mathbf{x})$

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.
5. If $\mathfrak{l}(1\mathbf{x}) \in X$, then there is some $x \in X$ where $t^\bullet(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x}), x) = \mathfrak{l}(\mathbf{x})$
6. If $\mathfrak{l}(1\mathbf{x}) \in X$, then $(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x})) \notin \mathbf{Li}(\Gamma(X, t^\bullet))$

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.
5. If $\mathfrak{l}(1\mathbf{x}) \in X$, then there is some $x \in X$ where $t^\bullet(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x}), x) = \mathfrak{l}(\mathbf{x})$
6. If $\mathfrak{l}(1\mathbf{x}) \in X$, then $(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x})) \notin \mathbf{Li}(\Gamma(X, t^\bullet))$

**Intuition**

The elements in $\Diamond(X, t^\bullet)$ are factorization trees of elements in the algebra $(X, t^\bullet)$.

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.
5. If $\mathfrak{l}(1\mathbf{x}) \in X$, then there is some $x \in X$ where $t^\bullet(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x}), x) = \mathfrak{l}(\mathbf{x})$
6. If $\mathfrak{l}(1\mathbf{x}) \in X$, then $(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x})) \notin \mathbf{Li}(\Gamma(X, t^\bullet))$

**Intuition**

The elements in $\Diamond(X, t^\bullet)$ are factorization trees of elements in the algebra $(X, t^\bullet)$.

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.
5. If $\mathfrak{l}(1\mathbf{x}) \in X$, then there is some $x \in X$ where $t^\bullet(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x}), x) = \mathfrak{l}(\mathbf{x})$
6. If $\mathfrak{l}(1\mathbf{x}) \in X$, then $(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x})) \notin \mathbf{Li}(\Gamma(X, t^\bullet))$

**Intuition**

The elements in $\Diamond(X, t^\bullet)$ are factorization trees of elements in the algebra $(X, t^\bullet)$.

# Functional endomorphic Laver tables-Part 1

Suppose that $(X, t^\bullet)$ is an $n+1$-ary Laver-like algebra. Then let $\Diamond(X, t^\bullet)$ be the algebra whose underlying set consists of all functions $\mathfrak{l} : \{1, \ldots, n\}^* \to X \cup \{\#\}$ that satisfies the following

1. $\mathfrak{l}(\varepsilon) \in X$
2. $\mathfrak{l}(\mathbf{x}) \in X$ for only finitely many $\mathbf{x} \in \{1, \ldots, n\}^*$
3. If $\mathfrak{l}(\mathbf{x}) = \#$ then $\mathfrak{l}(i\mathbf{x}) = \#$
4. If $\mathfrak{l}(\mathbf{x}) \in X$ then either $\mathfrak{l}(i\mathbf{x}) = \#$ for $1 \leq i \leq n$ or $\mathfrak{l}(i\mathbf{x}) \in X$ for $1 \leq i \leq n$.
5. If $\mathfrak{l}(1\mathbf{x}) \in X$, then there is some $x \in X$ where $t^\bullet(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x}), x) = \mathfrak{l}(\mathbf{x})$
6. If $\mathfrak{l}(1\mathbf{x}) \in X$, then $(\mathfrak{l}(1\mathbf{x}), \ldots, \mathfrak{l}(n\mathbf{x})) \notin \mathbf{Li}(\Gamma(X, t^\bullet))$

**Intuition**

The elements in $\Diamond(X, t^\bullet)$ are factorization trees of elements in the algebra $(X, t^\bullet)$.

# Functional endomorphic Laver tables-Part 2

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^{\bullet})$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^{\bullet}(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^{\bullet})$ can be endowed with a unique operation $t^{\sharp}$ such that

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and
3. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, t_x(\mathfrak{u}_1, \ldots, \mathfrak{u}_n)) =$
$t^\sharp(t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_1), \ldots, t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_n), t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$.

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and
3. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, t_x(\mathfrak{u}_1, \ldots, \mathfrak{u}_n)) =$
   $t^\sharp(t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_1), \ldots, t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_n), t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$.

Then $(\Diamond(X, t^\bullet), t^\sharp)$ is an $n+1$-ary Laver-like algebra called a functional endomorphic Laver table.

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and
3. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, t_x(\mathfrak{u}_1, \ldots, \mathfrak{u}_n)) =$
   $t^\sharp(t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_1), \ldots, t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_n), t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$.

Then $(\Diamond(X, t^\bullet), t^\sharp)$ is an $n+1$-ary Laver-like algebra called a functional endomorphic Laver table.

Furthermore, if there are efficient algorithms for computing $\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}$, then one can also compute $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l})(\mathbf{x})$ efficiently.

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and
3. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, t_x(\mathfrak{u}_1, \ldots, \mathfrak{u}_n)) =$
   $t^\sharp(t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_1), \ldots, t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_n), t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$.

Then $(\Diamond(X, t^\bullet), t^\sharp)$ is an $n+1$-ary Laver-like algebra called a functional endomorphic Laver table.

Furthermore, if there are efficient algorithms for computing $\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}$, then one can also compute $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l})(\mathbf{x})$ efficiently.

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and
3. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, t_x(\mathfrak{u}_1, \ldots, \mathfrak{u}_n)) =$
   $t^\sharp(t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_1), \ldots, t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_n), t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$.

Then $(\Diamond(X, t^\bullet), t^\sharp)$ is an $n+1$-ary Laver-like algebra called a functional endomorphic Laver table.

Furthermore, if there are efficient algorithms for computing $\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}$, then one can also compute $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l})(\mathbf{x})$ efficiently.

# Functional endomorphic Laver tables-Part 2

If $\mathfrak{l}_1, \ldots, \mathfrak{l}_n \in \Diamond(X, t^\bullet)$ and $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \notin \mathrm{Li}(\Gamma(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)))$ , then define $t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n) = \mathfrak{l}$ precisely when $\mathfrak{l}(\varepsilon) = t^\bullet(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon), x)$ and $\mathfrak{l}(\mathbf{x}i) = \mathfrak{l}_i(\mathbf{x})$.

The set $\Diamond(X, t^\bullet)$ can be endowed with a unique operation $t^\sharp$ such that

1. if $(\mathfrak{l}_1(\varepsilon), \ldots, \mathfrak{l}_n(\varepsilon)) \in \mathrm{Li}(\Gamma(X, t^\bullet))$, then $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = \mathfrak{l}$,
2. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}) = t_{\mathfrak{l}(\varepsilon)}(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$ whenever $\mathfrak{l}(1) = \#$, and
3. $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, t_x(\mathfrak{u}_1, \ldots, \mathfrak{u}_n)) =$
   $t^\sharp(t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_1), \ldots, t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{u}_n), t_x(\mathfrak{l}_1, \ldots, \mathfrak{l}_n)$.

Then $(\Diamond(X, t^\bullet), t^\sharp)$ is an $n+1$-ary Laver-like algebra called a functional endomorphic Laver table.

Furthermore, if there are efficient algorithms for computing $\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l}$, then one can also compute $t^\sharp(\mathfrak{l}_1, \ldots, \mathfrak{l}_n, \mathfrak{l})(\mathbf{x})$ efficiently.

# The Ko-Lee key exchange

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.
4. Alice computes $K$ using the fact that $K = a \circ s$ and Alice knows $a, s$.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.
4. Alice computes $K$ using the fact that $K = a \circ s$ and Alice knows $a, s$.
5. Bob computes $K$ using the fact that $K = r \circ b$ and Bob knows $r, b$.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.
4. Alice computes $K$ using the fact that $K = a \circ s$ and Alice knows $a, s$.
5. Bob computes $K$ using the fact that $K = r \circ b$ and Bob knows $r, b$.

An eavesdropping party will only know $x, r, s$. No eavesdropping party should be able to compute $K$ with this information. Therefore $K$ is a shared secret between Alice and Bob established over a public channel.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.
4. Alice computes $K$ using the fact that $K = a \circ s$ and Alice knows $a, s$.
5. Bob computes $K$ using the fact that $K = r \circ b$ and Bob knows $r, b$.

An eavesdropping party will only know $x, r, s$. No eavesdropping party should be able to compute $K$ with this information. Therefore $K$ is a shared secret between Alice and Bob established over a public channel.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.
4. Alice computes $K$ using the fact that $K = a \circ s$ and Alice knows $a, s$.
5. Bob computes $K$ using the fact that $K = r \circ b$ and Bob knows $r, b$.

An eavesdropping party will only know $x, r, s$. No eavesdropping party should be able to compute $K$ with this information. Therefore $K$ is a shared secret between Alice and Bob established over a public channel.

# The Ko-Lee key exchange

In the following key exchange, Alice and Bob want to share a common secret by communicating over a public channel.

A semigroup $(X, \circ)$ and an element $x \in X$ are known to the public.

1. Alice selects some $a \in X$ and then sends $r = a \circ x$ to Bob.
2. Bob selects some $b \in X$ and the sends $s = x \circ b$ to Alice.
3. Let $K = a \circ x \circ b$.
4. Alice computes $K$ using the fact that $K = a \circ s$ and Alice knows $a, s$.
5. Bob computes $K$ using the fact that $K = r \circ b$ and Bob knows $r, b$.

An eavesdropping party will only know $x, r, s$. No eavesdropping party should be able to compute $K$ with this information. Therefore $K$ is a shared secret between Alice and Bob established over a public channel.

# Functional endomorphic Laver table based cryptography

# Functional endomorphic Laver table based cryptography

**Ko-Lee key exchange**

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange. This key exchange by Kalka and Teicher extends to $n$-ary self-distributive algebras as well. The functional endomorphic Laver tables may be used as a platform for this key exchange.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange. This key exchange by Kalka and Teicher extends to $n$-ary self-distributive algebras as well. The functional endomorphic Laver tables may be used as a platform for this key exchange.

## Authentication

In 2006, Dehornoy has shown that self-distributive algebras may be used as platforms for authentication schemes.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange. This key exchange by Kalka and Teicher extends to $n$-ary self-distributive algebras as well. The functional endomorphic Laver tables may be used as a platform for this key exchange.

## Authentication

In 2006, Dehornoy has shown that self-distributive algebras may be used as platforms for authentication schemes. In particular, the functional endomorphic Laver tables may be used as platforms for such authentication schemes.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange. This key exchange by Kalka and Teicher extends to $n$-ary self-distributive algebras as well. The functional endomorphic Laver tables may be used as a platform for this key exchange.

## Authentication

In 2006, Dehornoy has shown that self-distributive algebras may be used as platforms for authentication schemes. In particular, the functional endomorphic Laver tables may be used as platforms for such authentication schemes.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange. This key exchange by Kalka and Teicher extends to $n$-ary self-distributive algebras as well. The functional endomorphic Laver tables may be used as a platform for this key exchange.

## Authentication

In 2006, Dehornoy has shown that self-distributive algebras may be used as platforms for authentication schemes. In particular, the functional endomorphic Laver tables may be used as platforms for such authentication schemes.

# Functional endomorphic Laver table based cryptography

## Ko-Lee key exchange

If $X$ is a functionally endomorphic Laver table, then $(\Gamma(X) \setminus \mathrm{Li}((\Gamma(X)), \circ)$ may be used as a platform for the Ko-Lee key exchange.

## Kalka-Teicher key exchange

In year 1999, Anshel, Anshel, and Goldfeld have constructed a key exchange which could use any non-abelian group as a platform. In 2013, Kalka and Teicher have constructed a self-distributive version of the Anshel-Anshel-Goldfeld key exchange. This key exchange by Kalka and Teicher extends to $n$-ary self-distributive algebras as well. The functional endomorphic Laver tables may be used as a platform for this key exchange.

## Authentication

In 2006, Dehornoy has shown that self-distributive algebras may be used as platforms for authentication schemes. In particular, the functional endomorphic Laver tables may be used as platforms for such authentication schemes.

# Functional endomorphic Laver table based cryptography

# Functional endomorphic Laver table based cryptography

## Interactivity

The functional endomorphic Laver table based key exchanges at this point require Alice and Bob to communicate a few bytes of information back and forth with each other several times.

# Functional endomorphic Laver table based cryptography

## Interactivity

The functional endomorphic Laver table based key exchanges at this point require Alice and Bob to communicate a few bytes of information back and forth with each other several times.

## Classical security

From the existence of a rank-into-rank cardinal, we know that the classical Laver tables exhibit endless combinatorial complexity. The functional endomorphic Laver tables exhibit much more complex behavior. Therefore, it seems unlikely that one can mathematical prove that the functional endomorphic Laver table based cryptosystems are broken. A heuristic algorithm is more likely to break these cryptosystems.

# Functional endomorphic Laver table based cryptography

## Interactivity

The functional endomorphic Laver table based key exchanges at this point require Alice and Bob to communicate a few bytes of information back and forth with each other several times.

## Classical security

From the existence of a rank-into-rank cardinal, we know that the classical Laver tables exhibit endless combinatorial complexity. The functional endomorphic Laver tables exhibit much more complex behavior. Therefore, it seems unlikely that one can mathematical prove that the functional endomorphic Laver table based cryptosystems are broken. A heuristic algorithm is more likely to break these cryptosystems.

## Quantum security

The functional endomorphic Laver table based key exchanges appear to be secure against adversaries with quantum computers if they are secure against adversaries with access to classical computers only.

# Functional endomorphic Laver table based cryptography

## Interactivity

The functional endomorphic Laver table based key exchanges at this point require Alice and Bob to communicate a few bytes of information back and forth with each other several times.

## Classical security

From the existence of a rank-into-rank cardinal, we know that the classical Laver tables exhibit endless combinatorial complexity. The functional endomorphic Laver tables exhibit much more complex behavior. Therefore, it seems unlikely that one can mathematical prove that the functional endomorphic Laver table based cryptosystems are broken. A heuristic algorithm is more likely to break these cryptosystems.

## Quantum security

The functional endomorphic Laver table based key exchanges appear to be secure against adversaries with quantum computers if they are secure against adversaries with access to classical computers only.

# Functional endomorphic Laver table based cryptography

## Interactivity

The functional endomorphic Laver table based key exchanges at this point require Alice and Bob to communicate a few bytes of information back and forth with each other several times.

## Classical security

From the existence of a rank-into-rank cardinal, we know that the classical Laver tables exhibit endless combinatorial complexity. The functional endomorphic Laver tables exhibit much more complex behavior. Therefore, it seems unlikely that one can mathematical prove that the functional endomorphic Laver table based cryptosystems are broken. A heuristic algorithm is more likely to break these cryptosystems.

## Quantum security

The functional endomorphic Laver table based key exchanges appear to be secure against adversaries with quantum computers if they are secure against adversaries with access to classical computers only.

# Functional endomorphic Laver table based cryptography

## Interactivity

The functional endomorphic Laver table based key exchanges at this point require Alice and Bob to communicate a few bytes of information back and forth with each other several times.

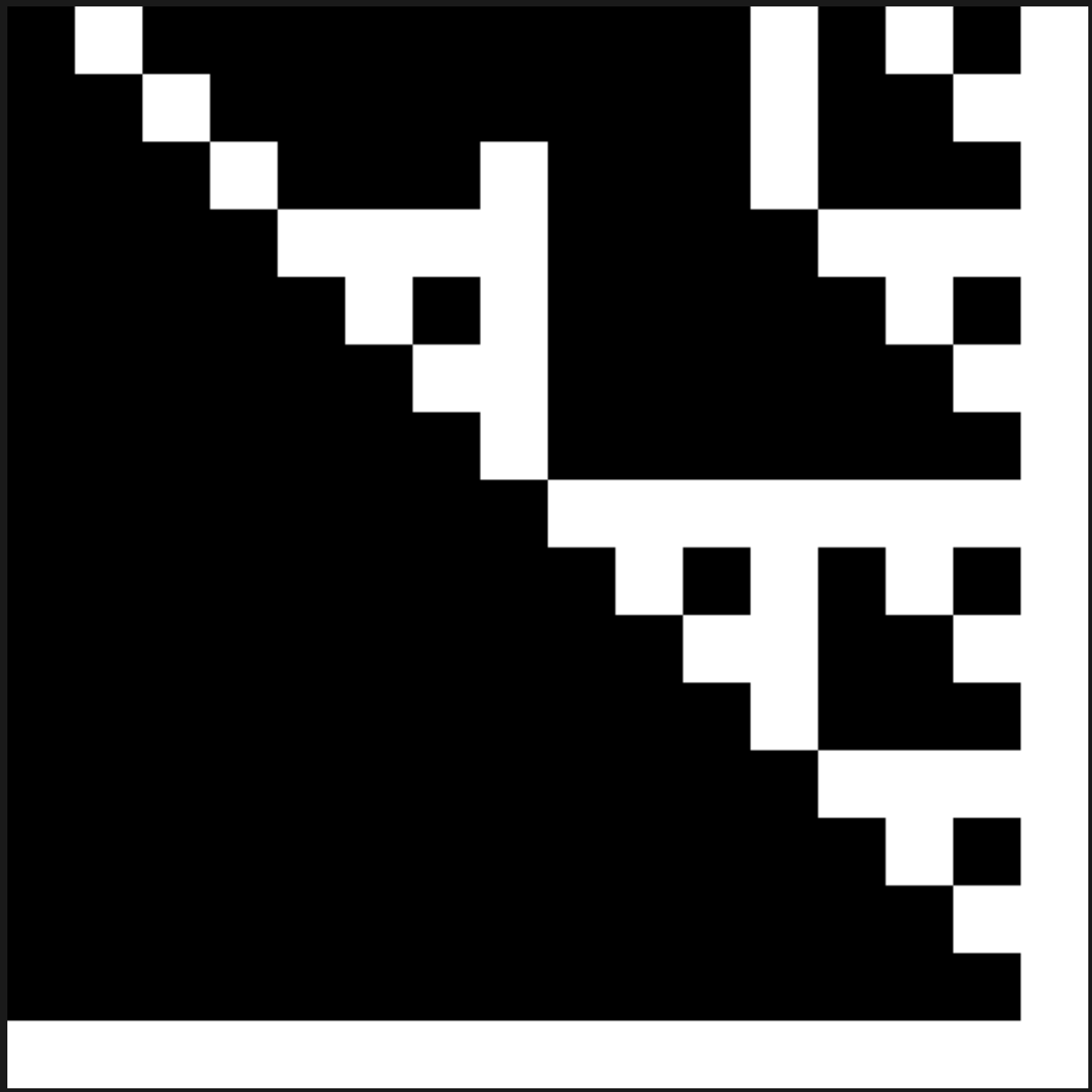
## Classical security

From the existence of a rank-into-rank cardinal, we know that the classical Laver tables exhibit endless combinatorial complexity. The functional endomorphic Laver tables exhibit much more complex behavior. Therefore, it seems unlikely that one can mathematical prove that the functional endomorphic Laver table based cryptosystems are broken. A heuristic algorithm is more likely to break these cryptosystems.

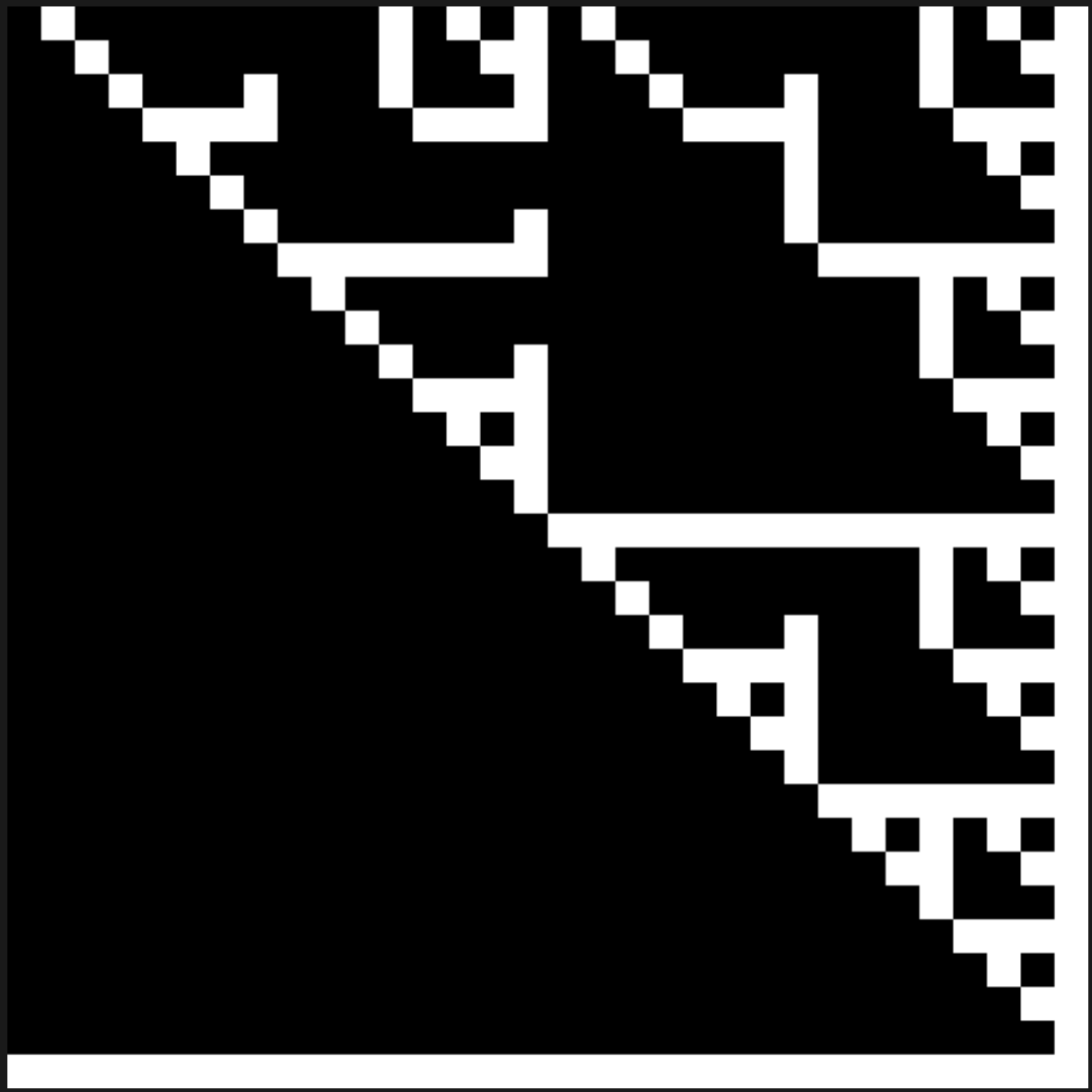
## Quantum security

The functional endomorphic Laver table based key exchanges appear to be secure against adversaries with quantum computers if they are secure against adversaries with access to classical computers only.

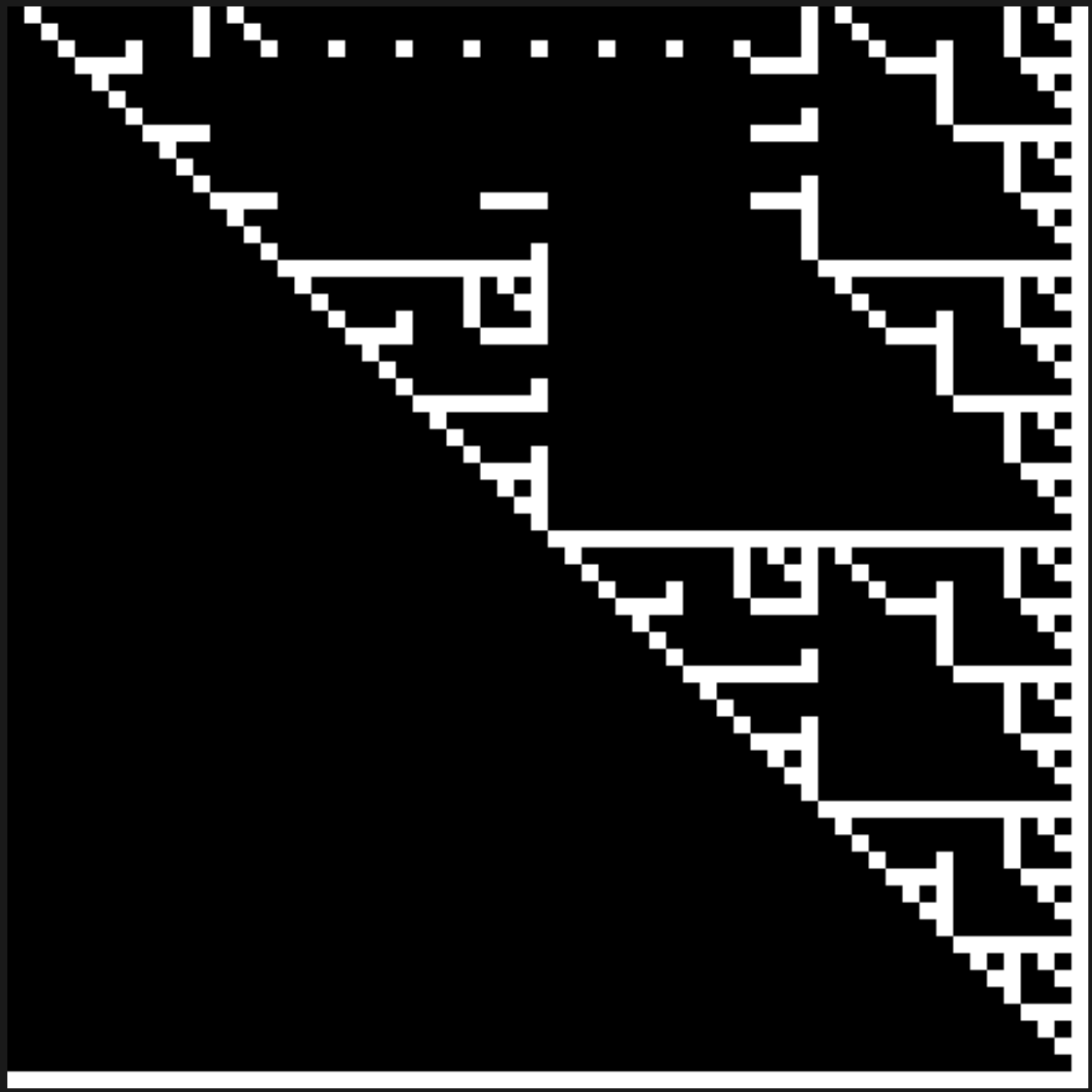
# Pictures: $A_4$



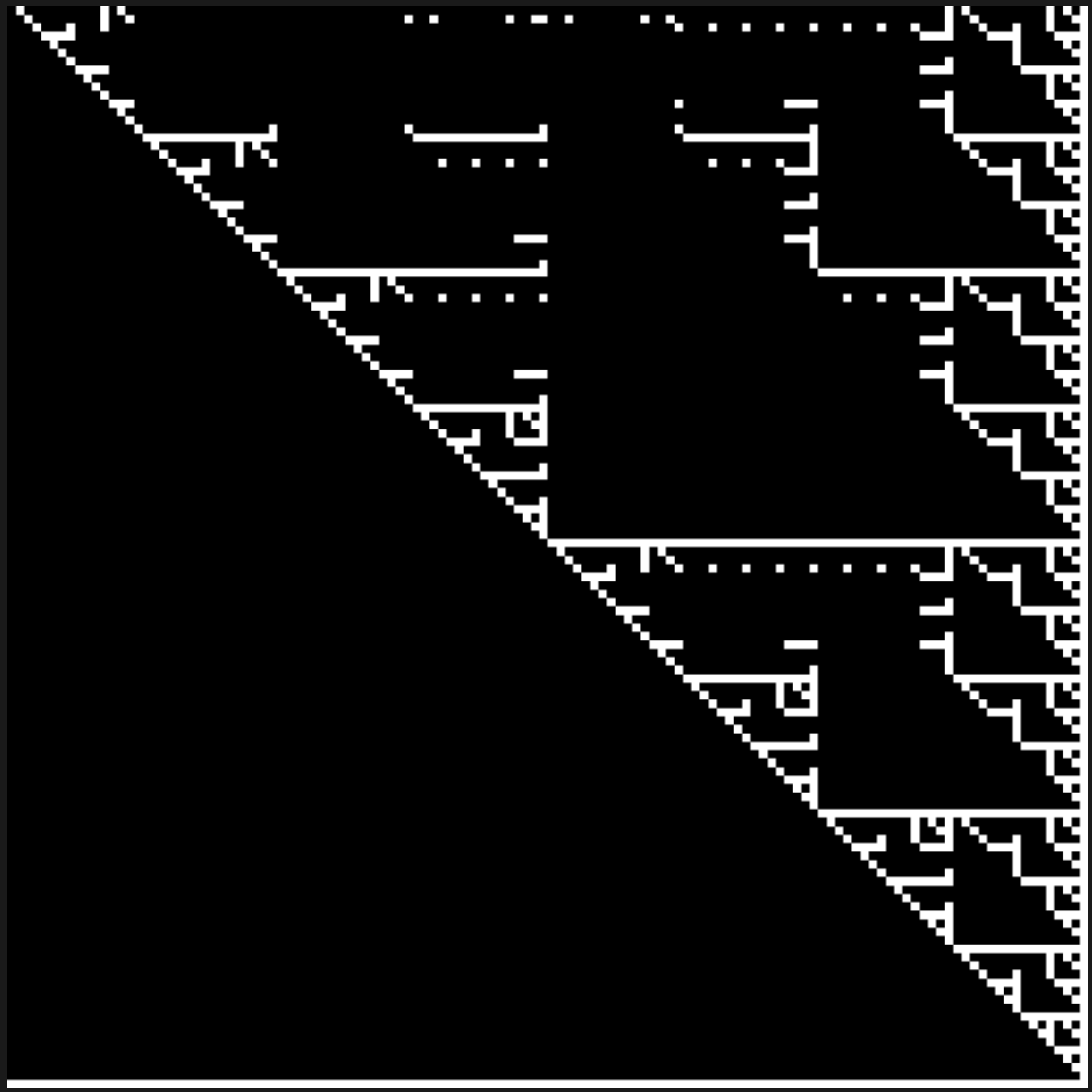
# Pictures: $A_5$



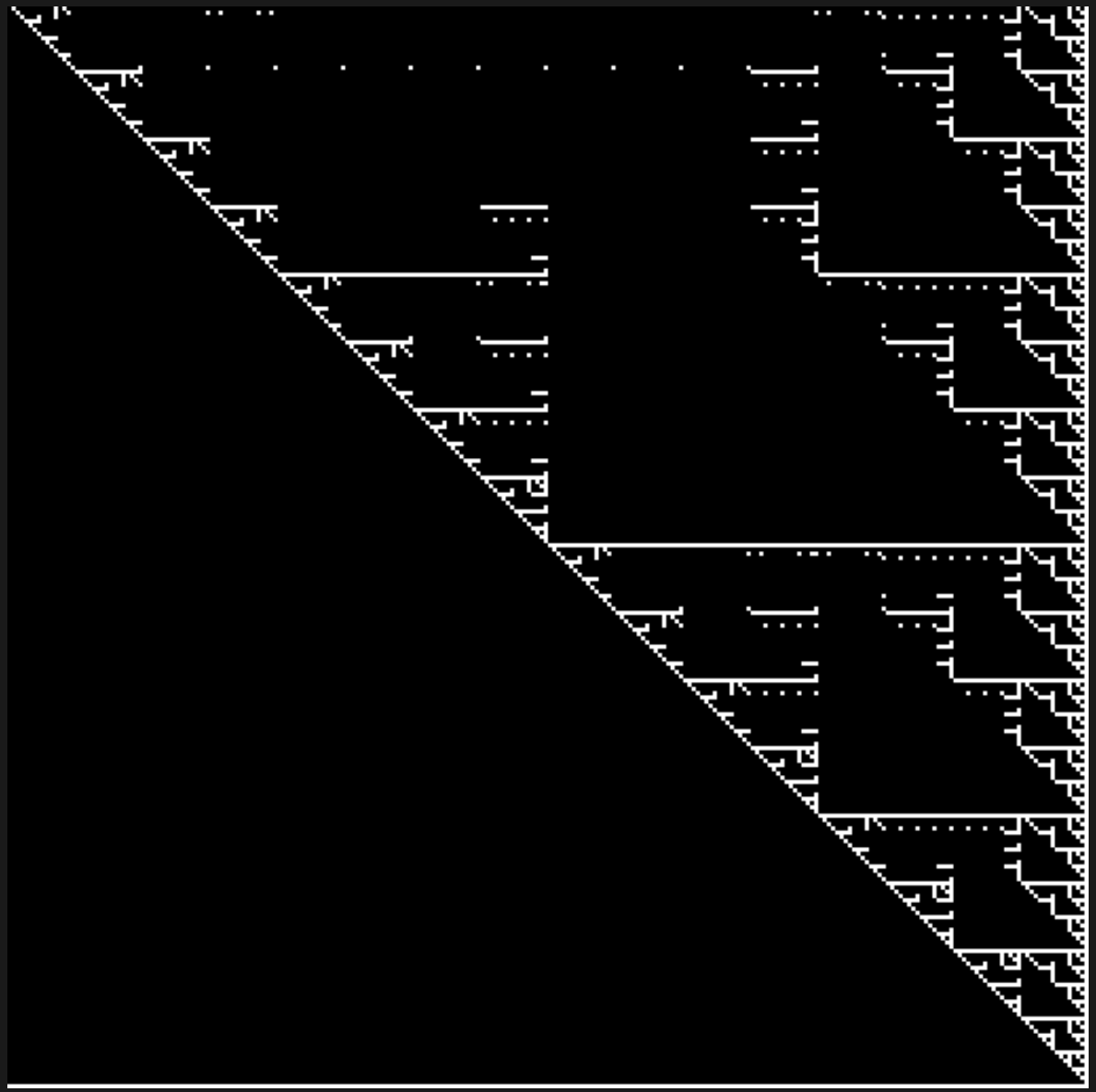
# Pictures: $A_6$



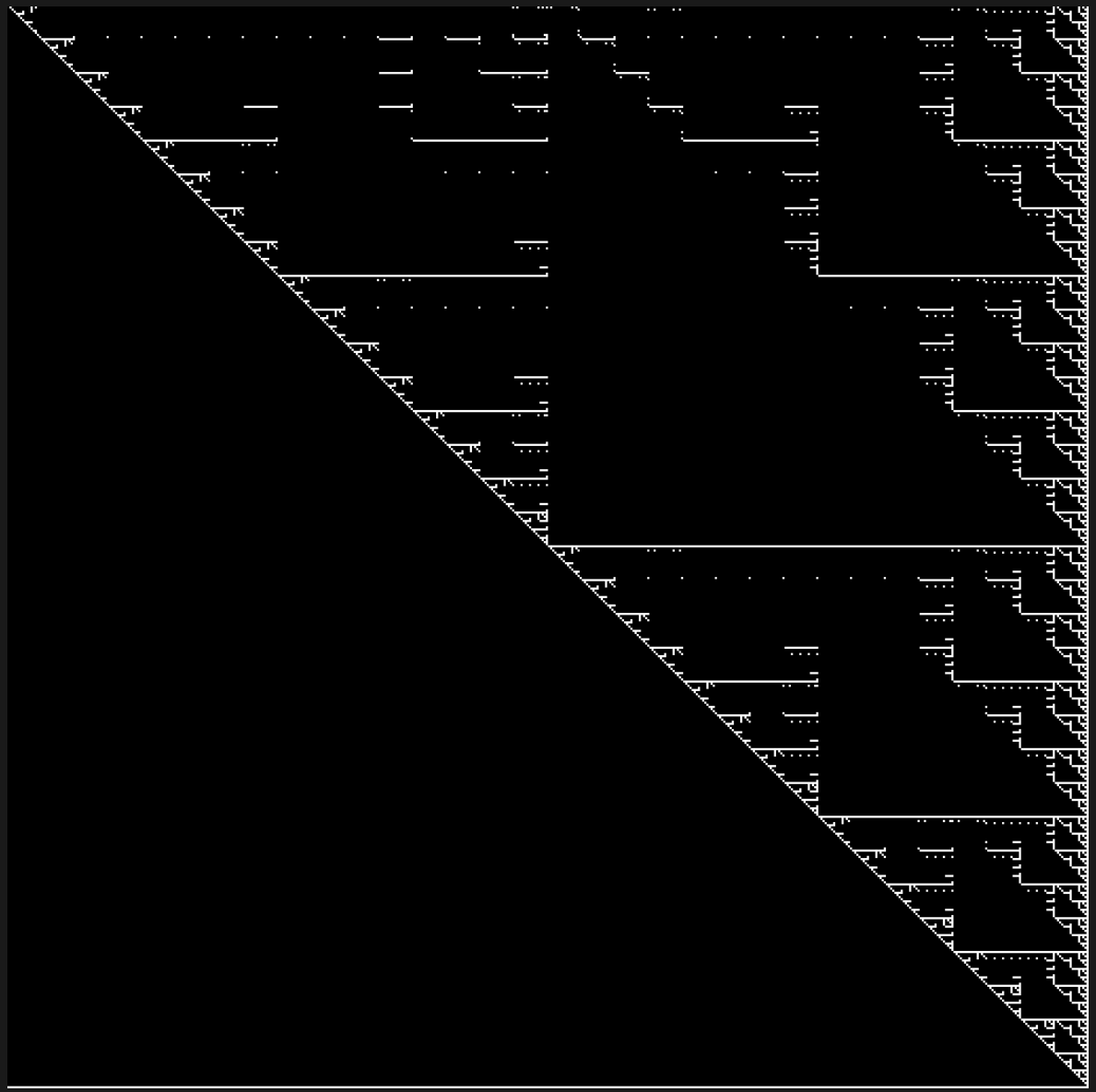
# Pictures: $A_7$



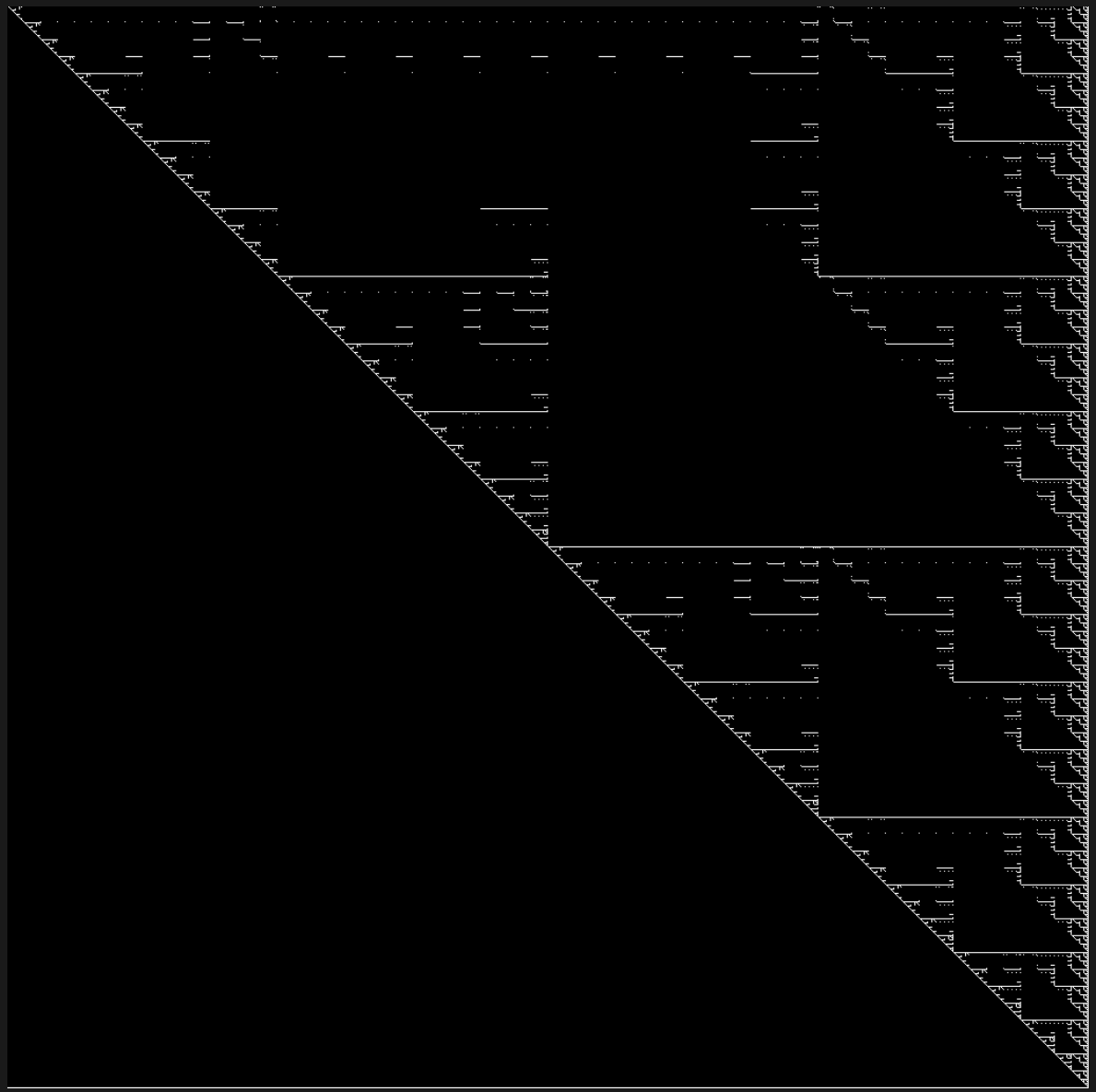
# Pictures: $A_8$



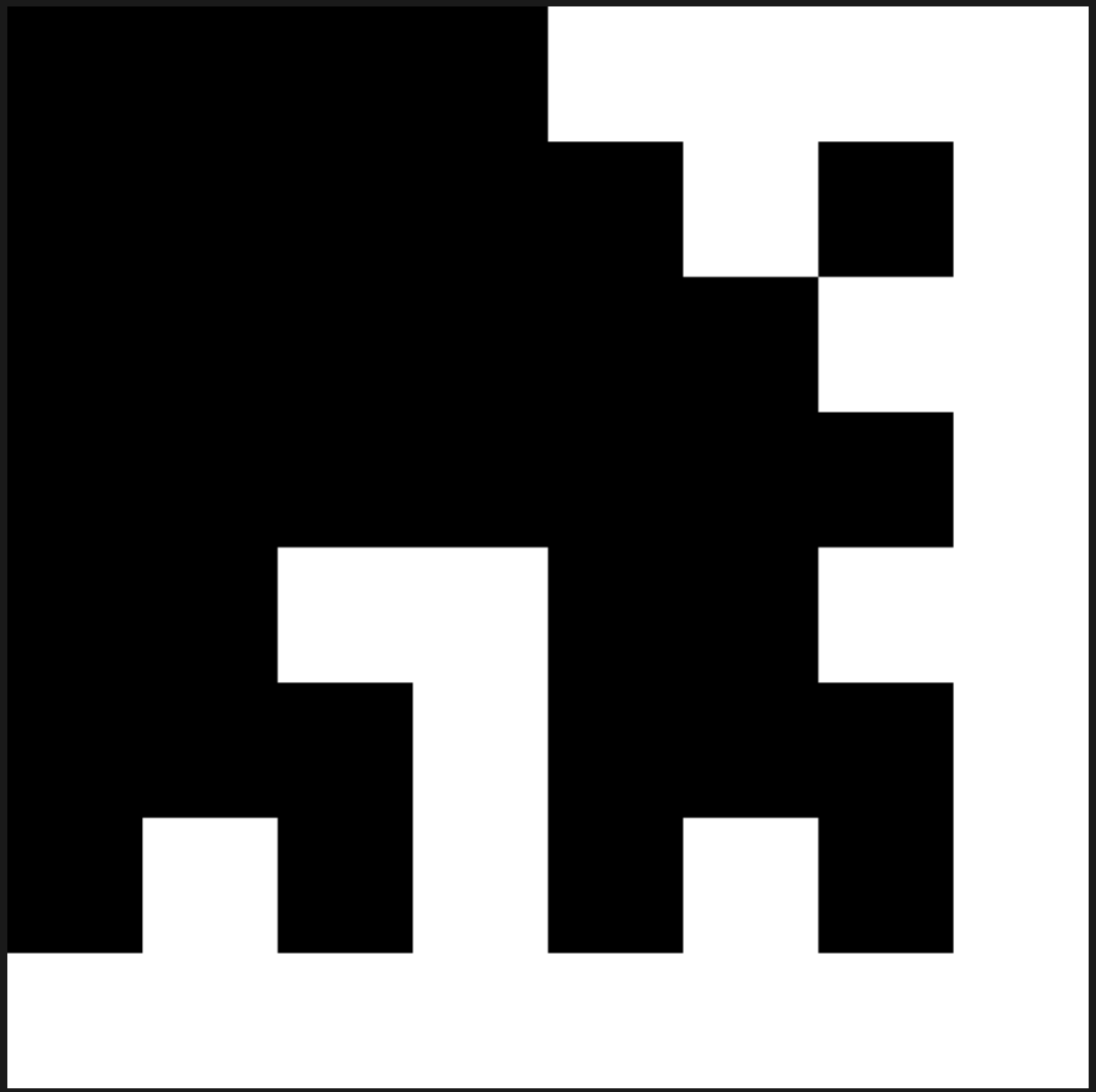
# Pictures: $A_9$



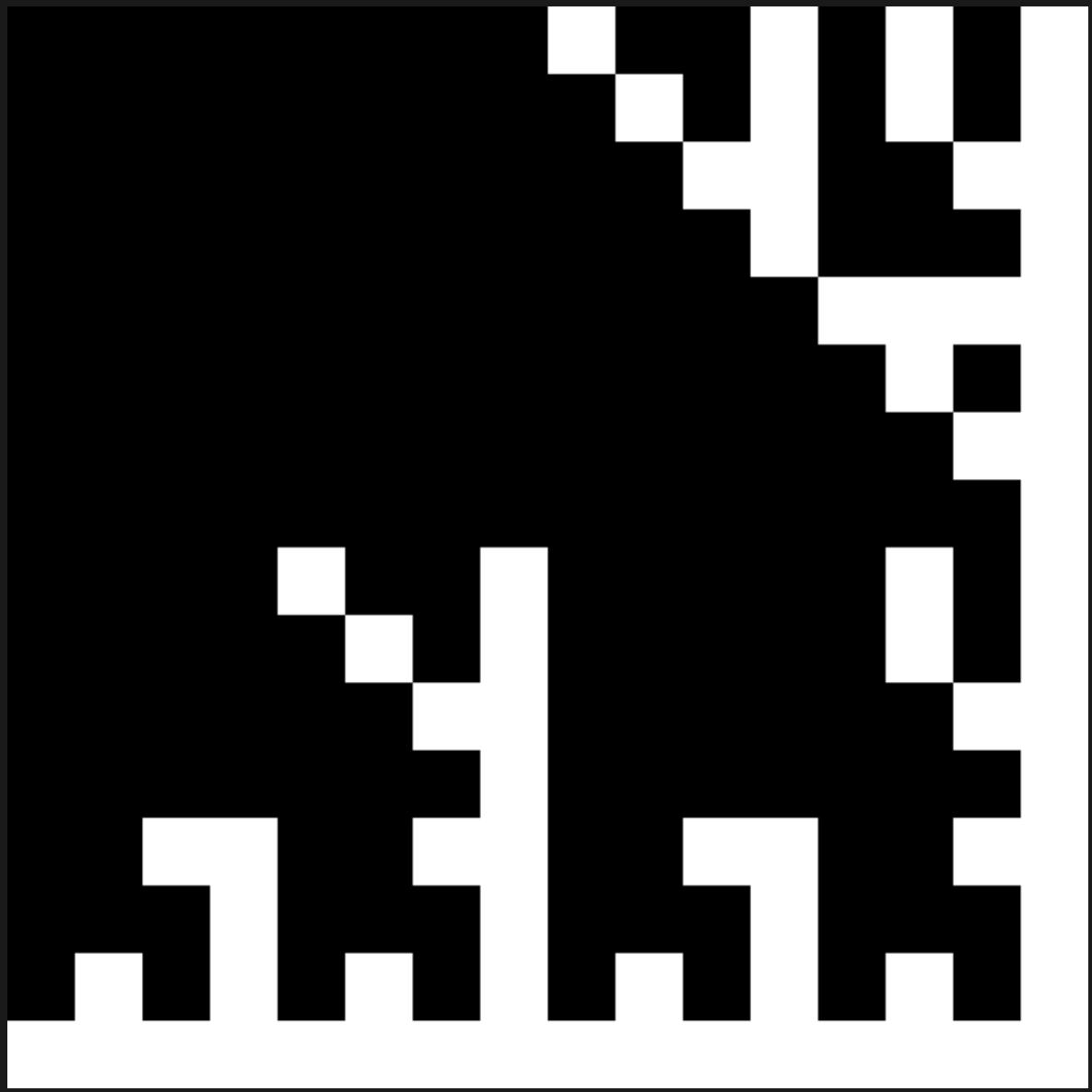
# Pictures: $A_{10}$



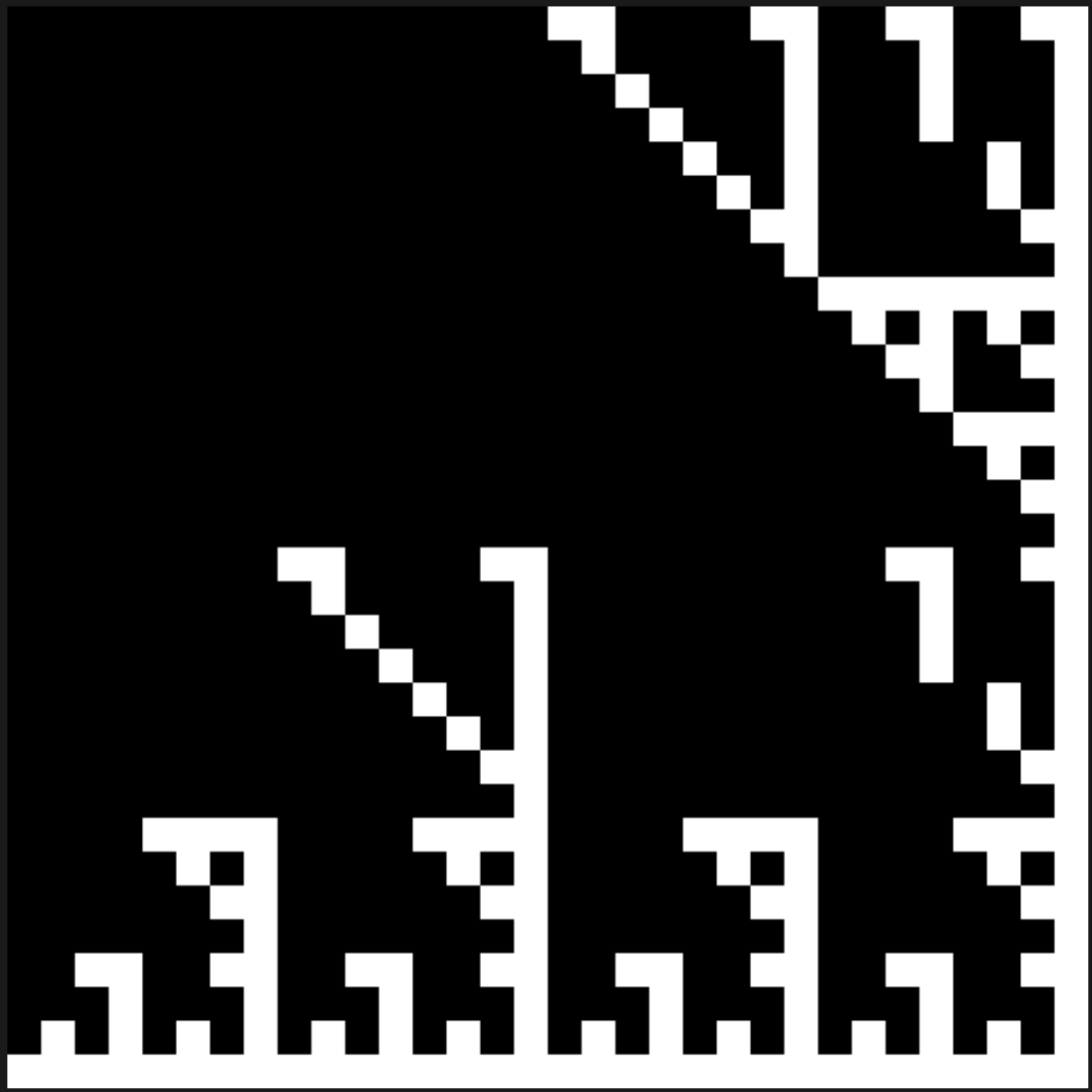
# Pictures: $A_3$



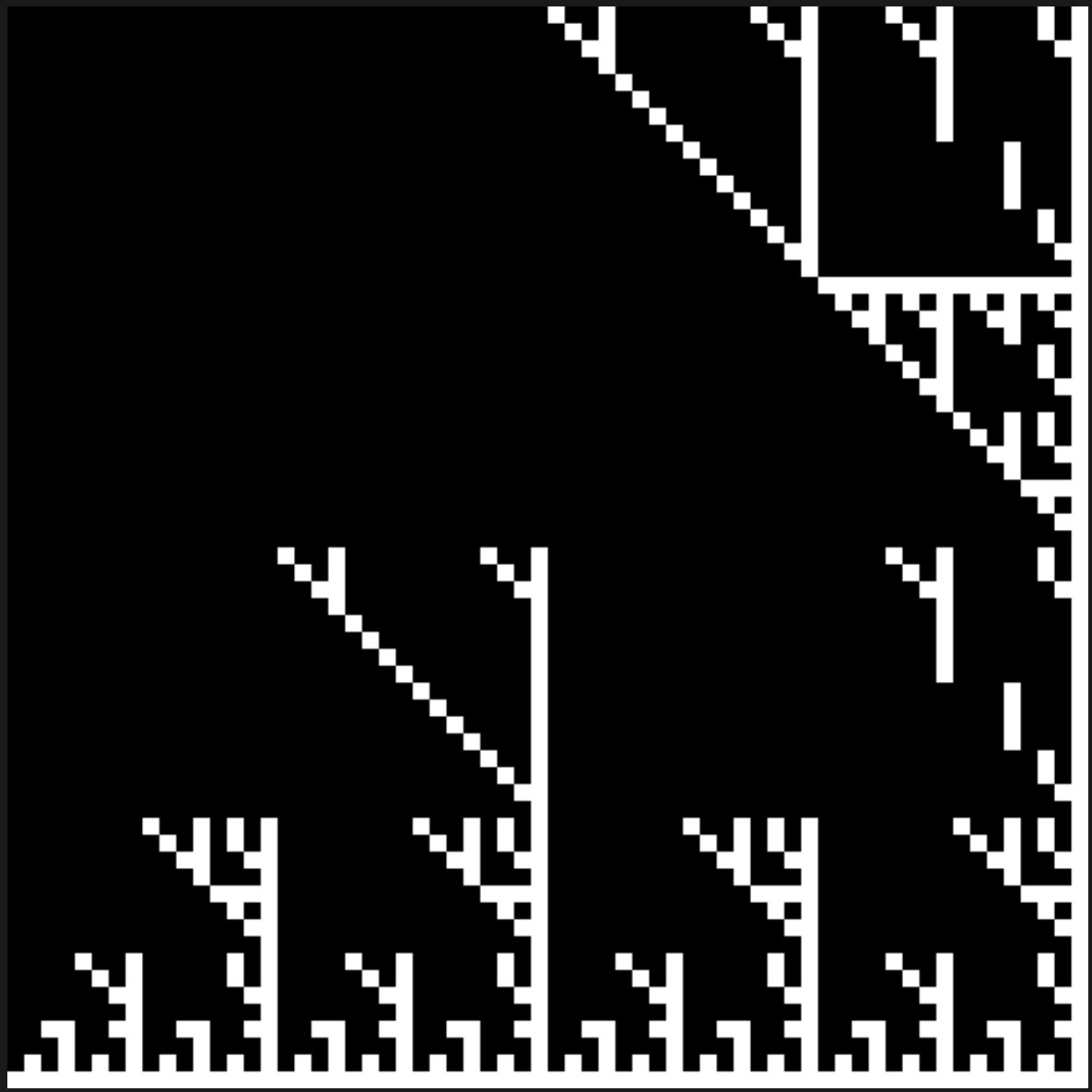
# Pictures: $A_4$



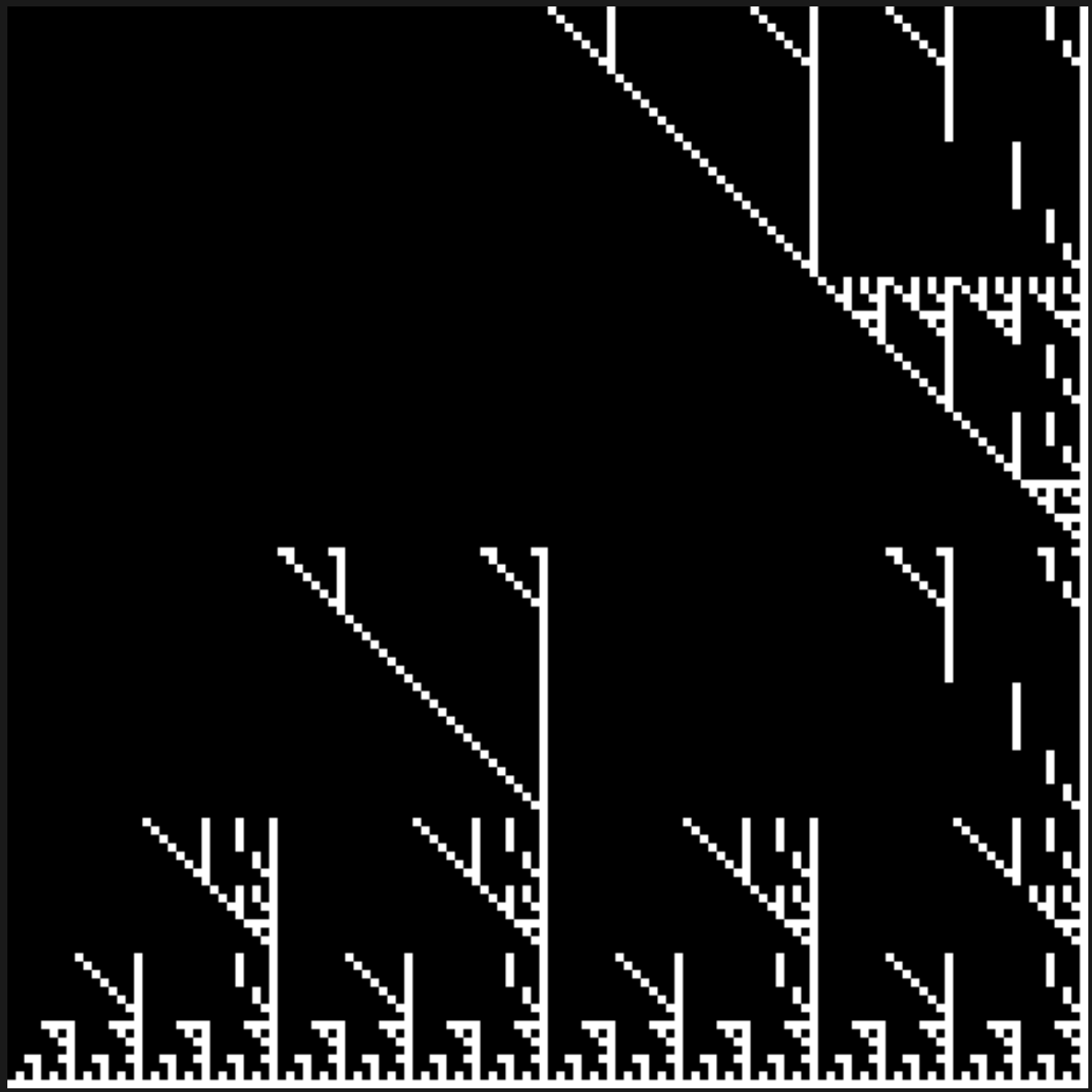
# Pictures: $A_5$



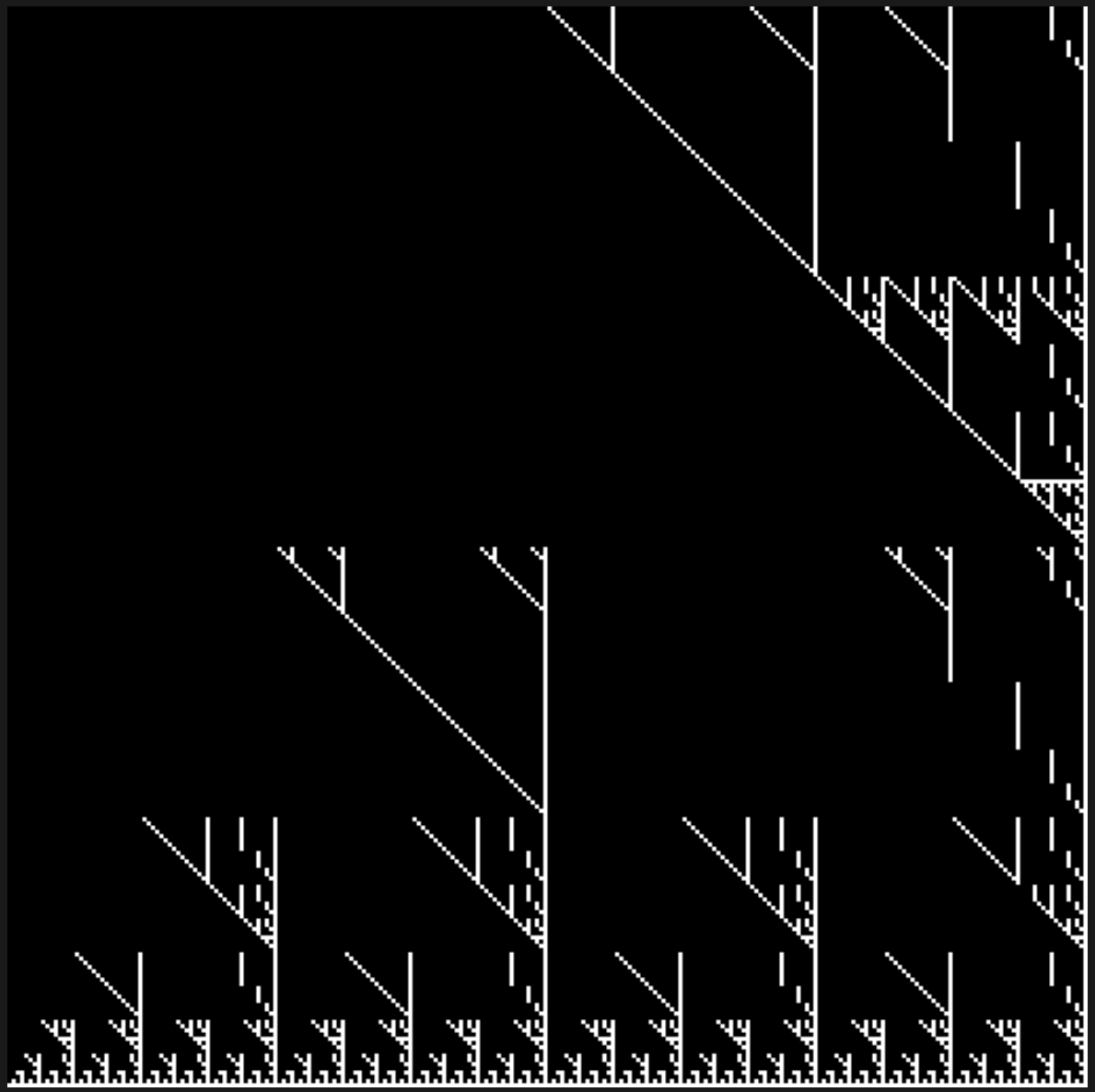
# Pictures: $A_6$



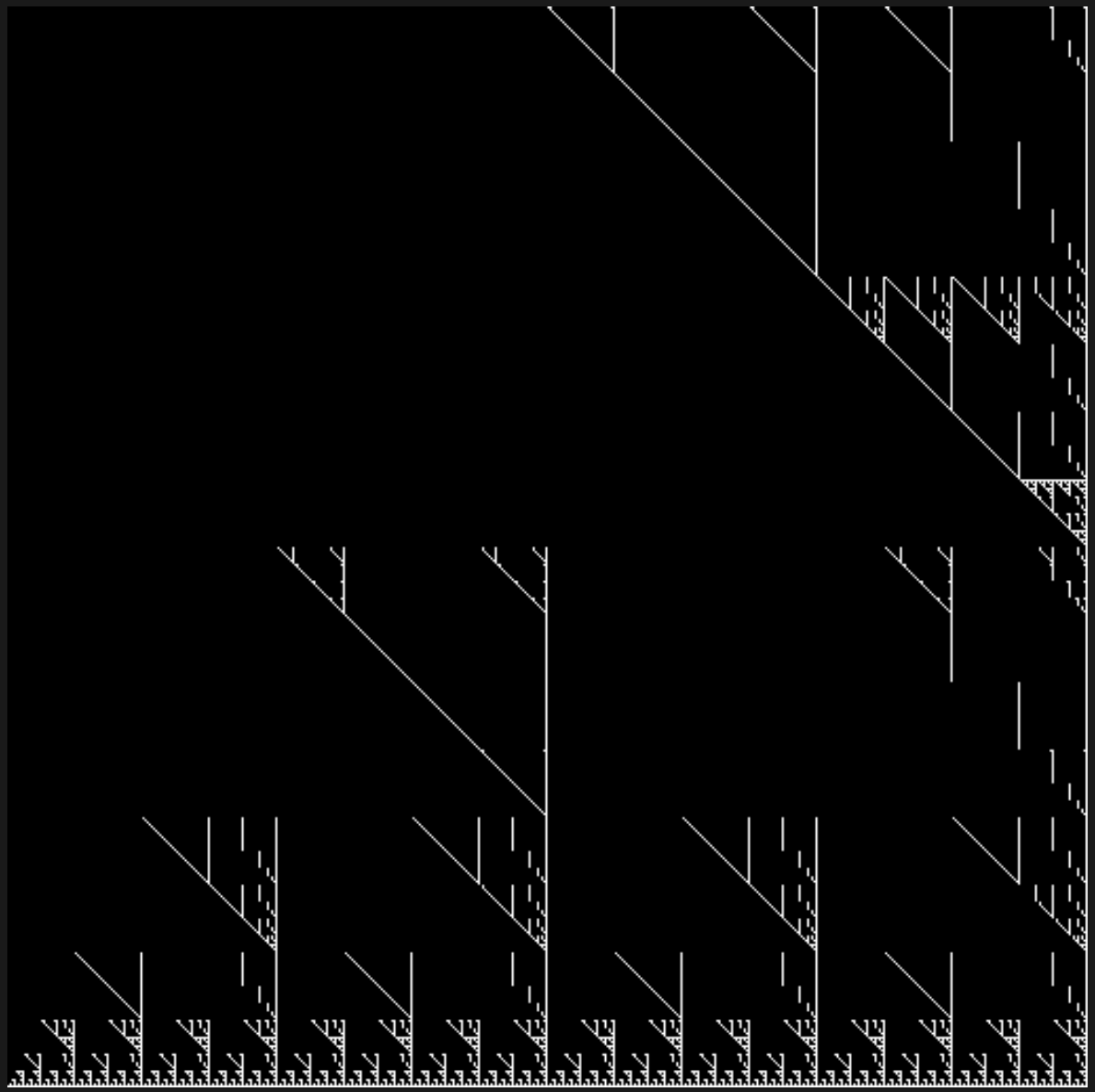
# Pictures: $A_7$



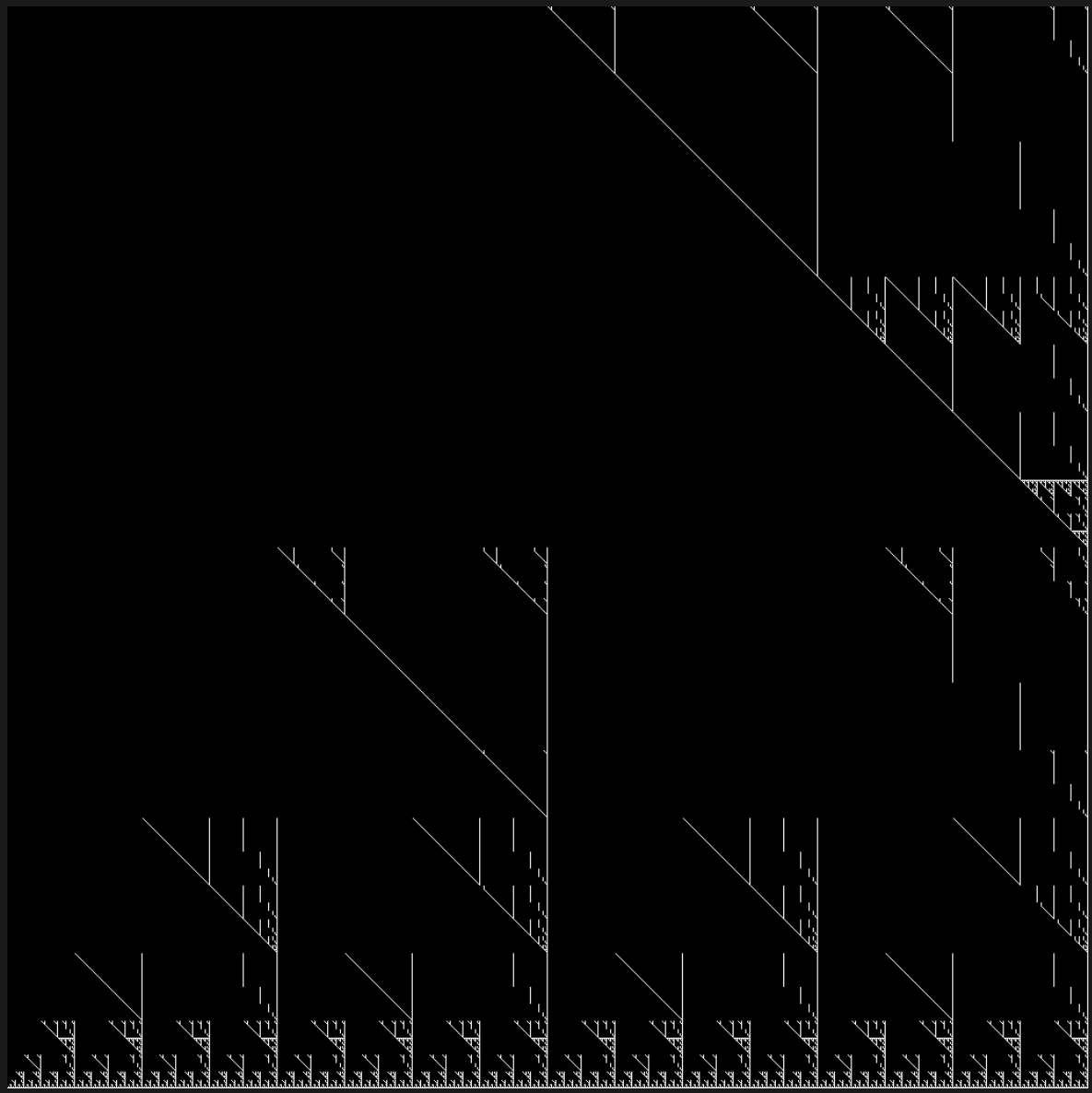
# Pictures: $A_8$



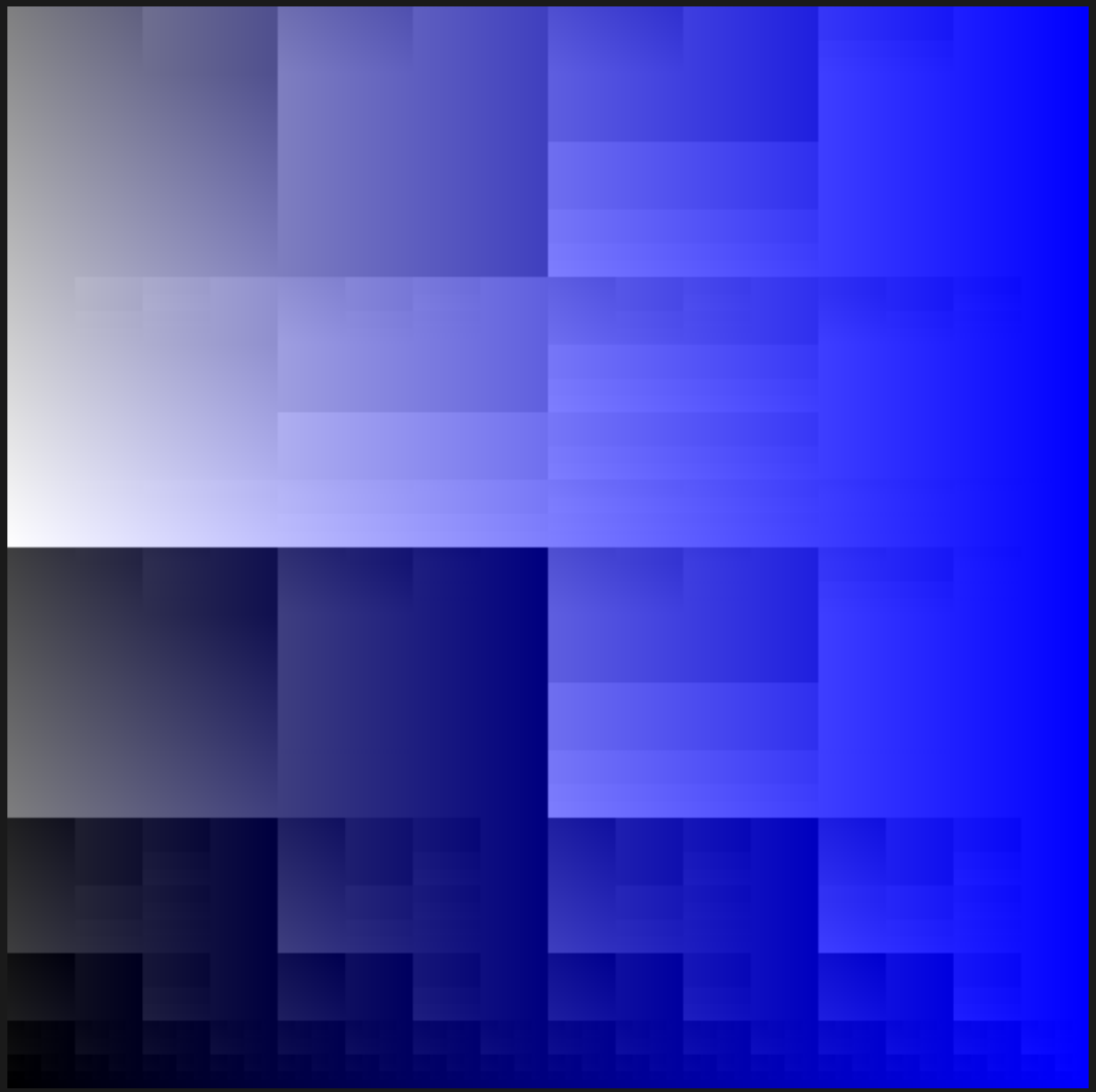
# Pictures: $A_9$



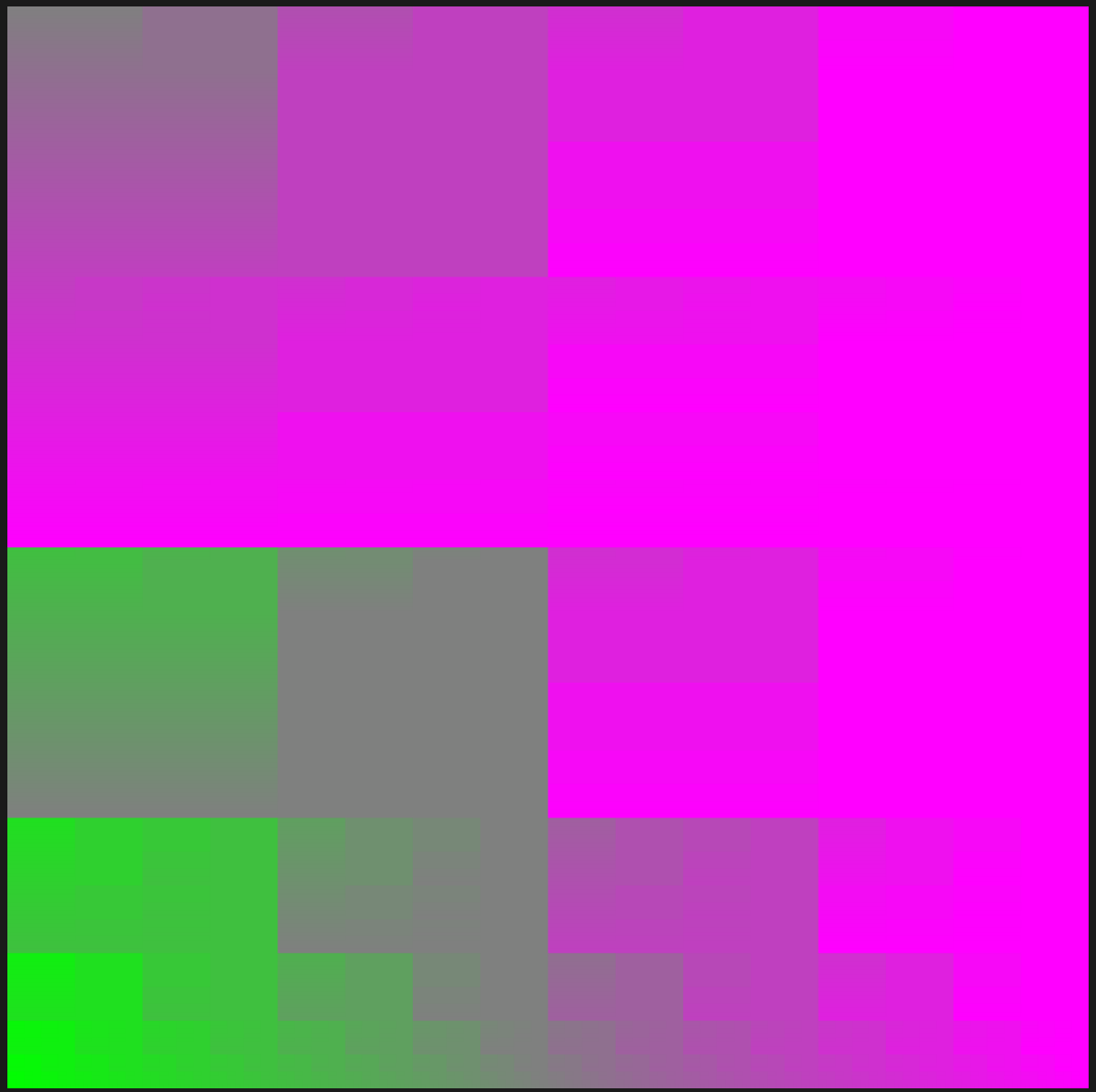
# Pictures: $A_{10}$



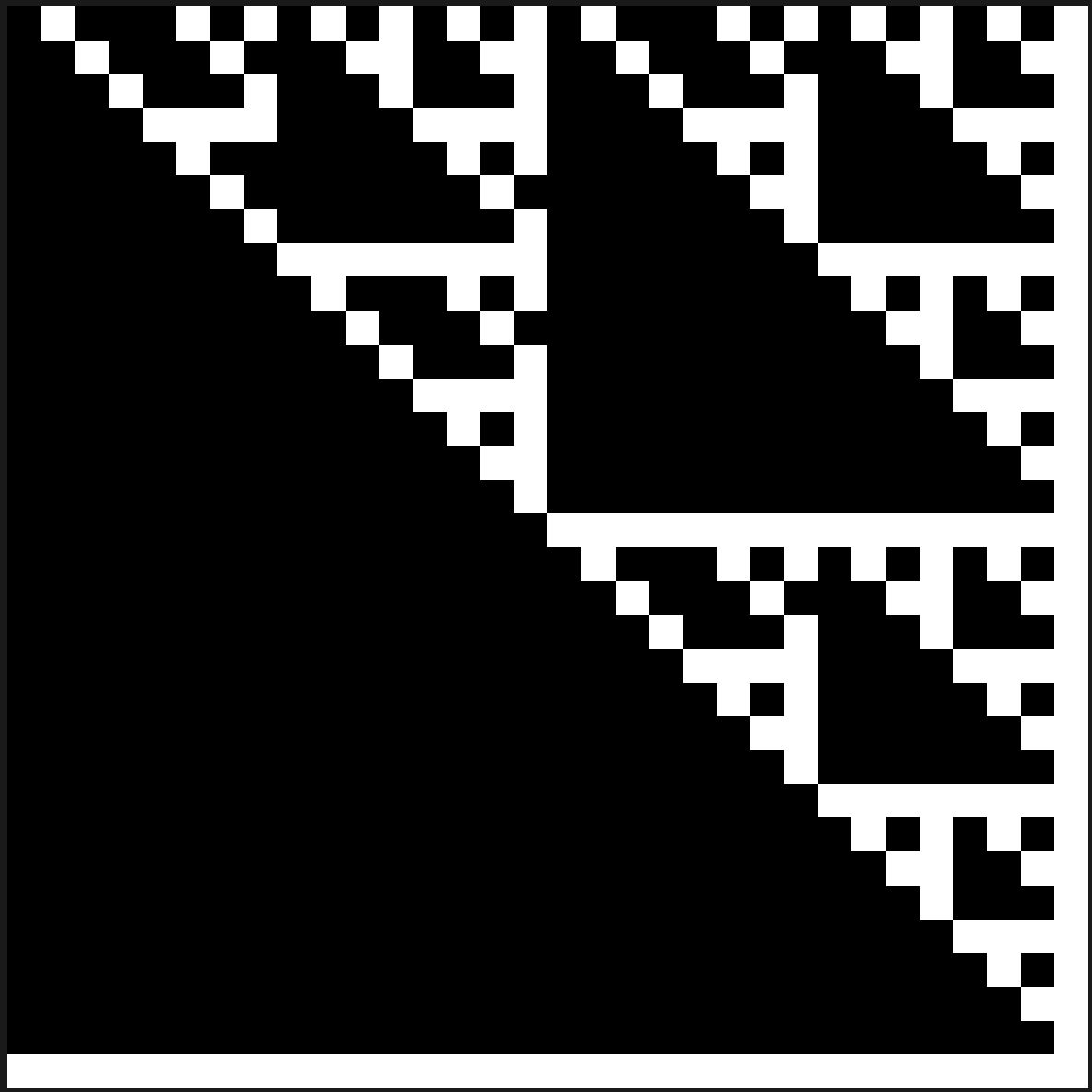
# Pictures:Classical Laver table heat map



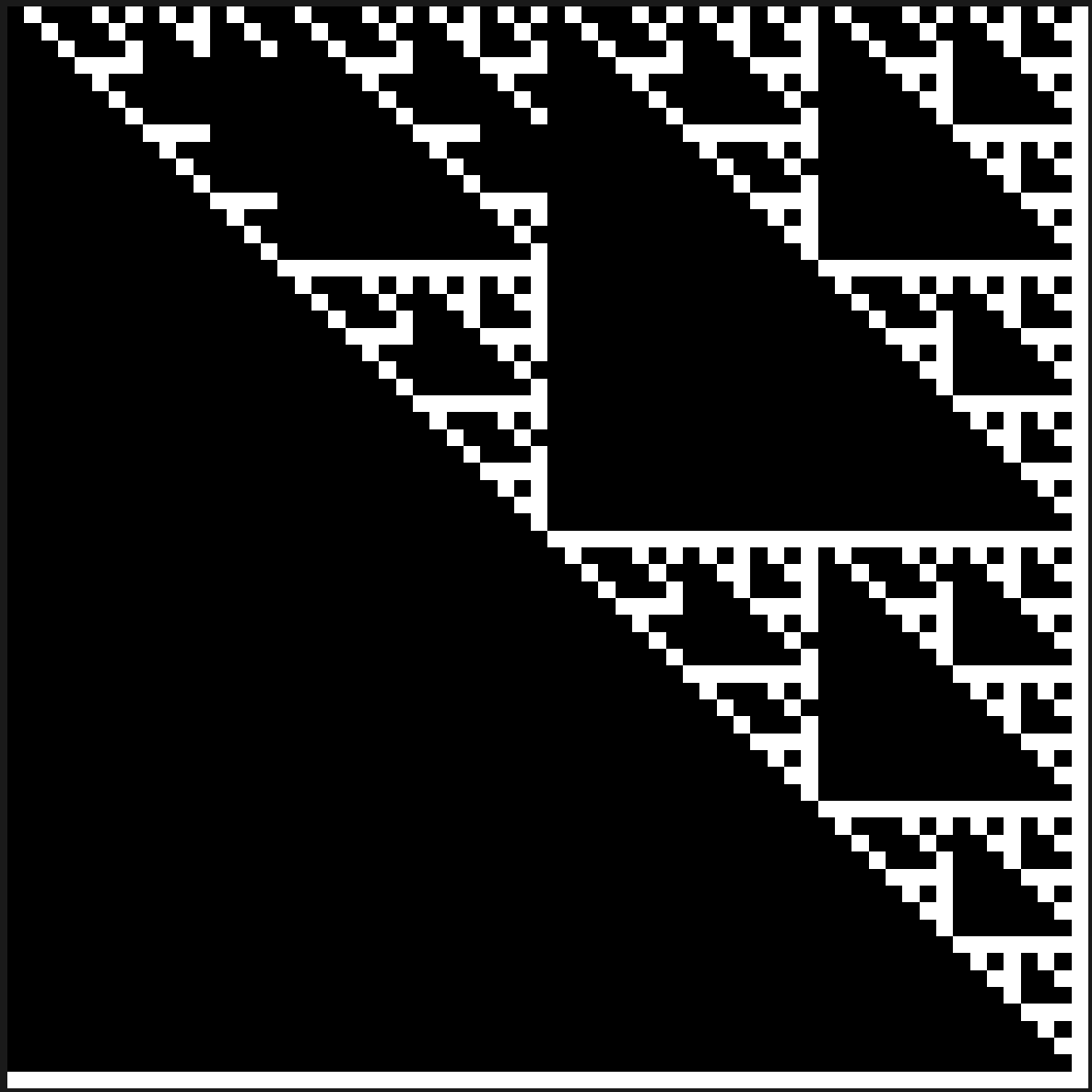
# Pictures:Classical Laver table heat map



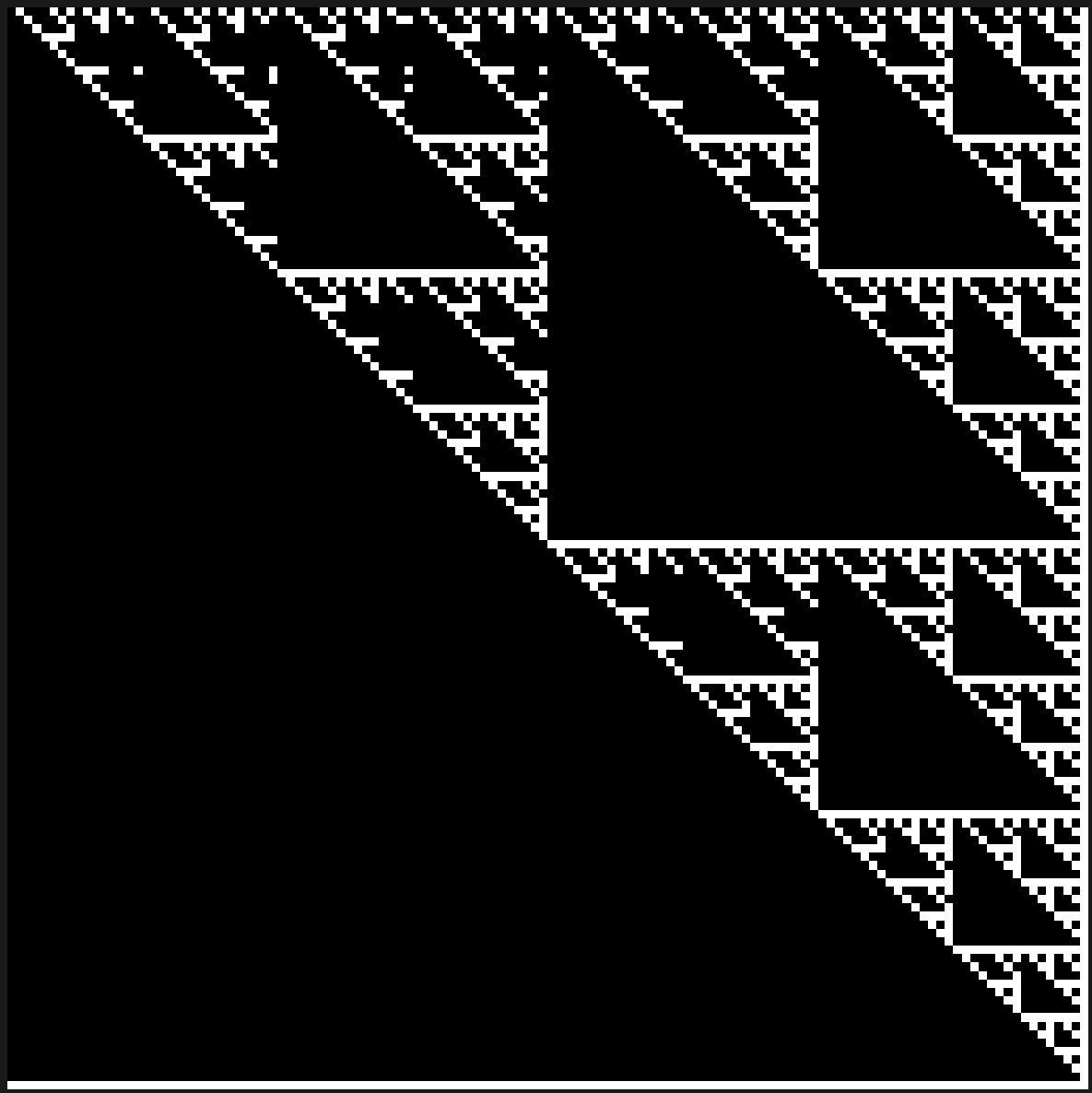
# Pictures: $FM_5^-$



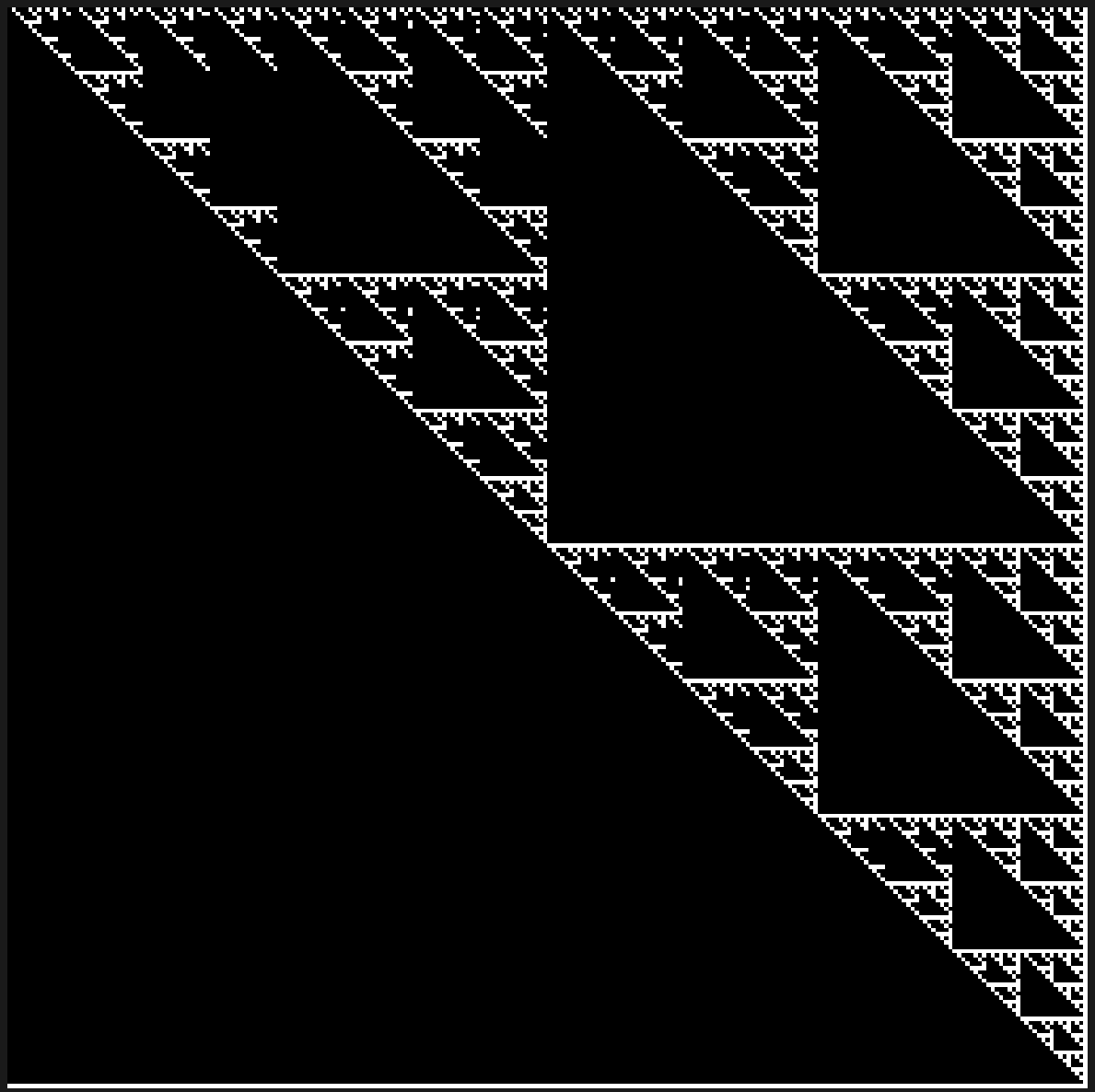
# Pictures: $FM_6^-$



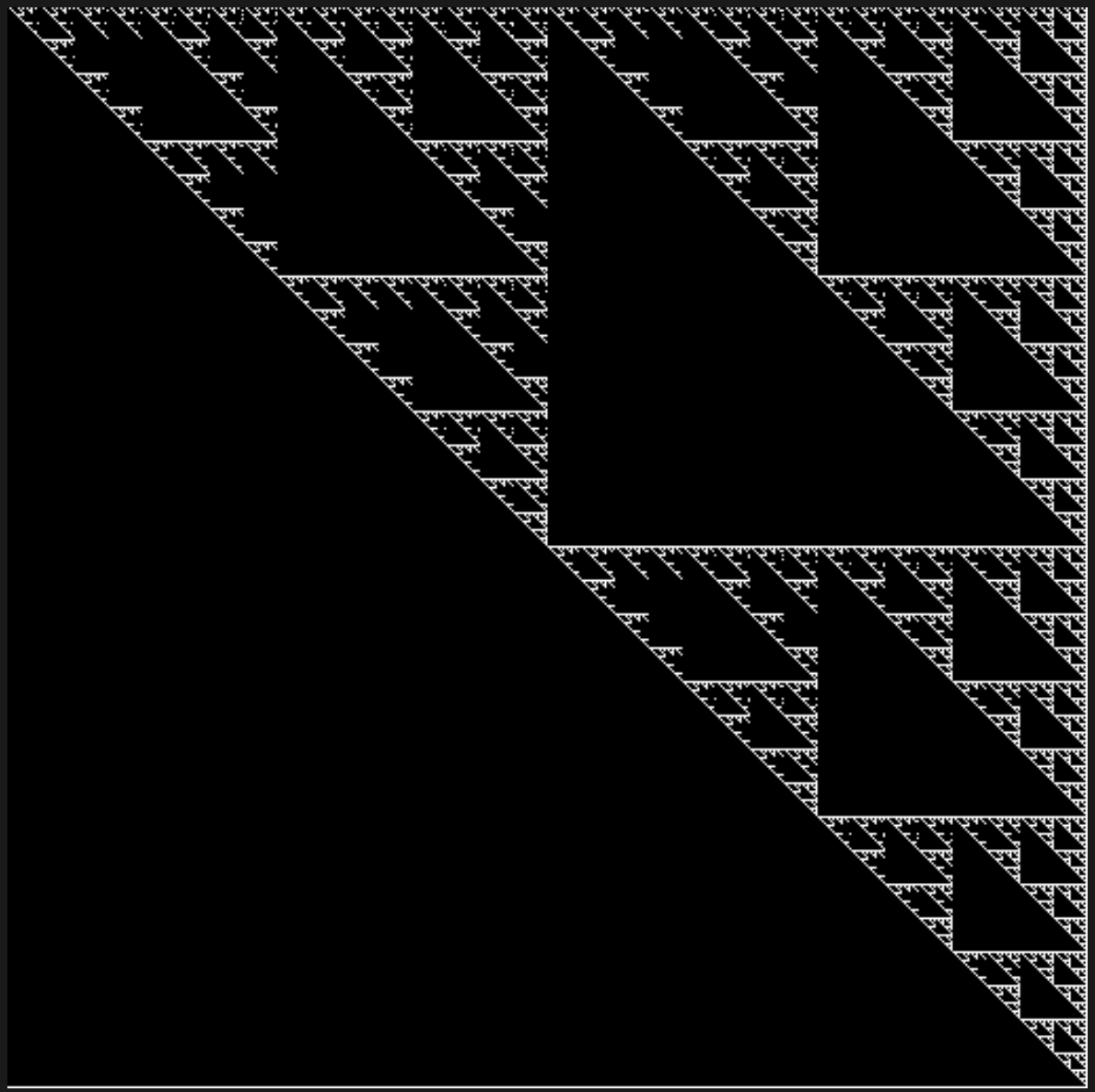
# Pictures: $FM_7^-$



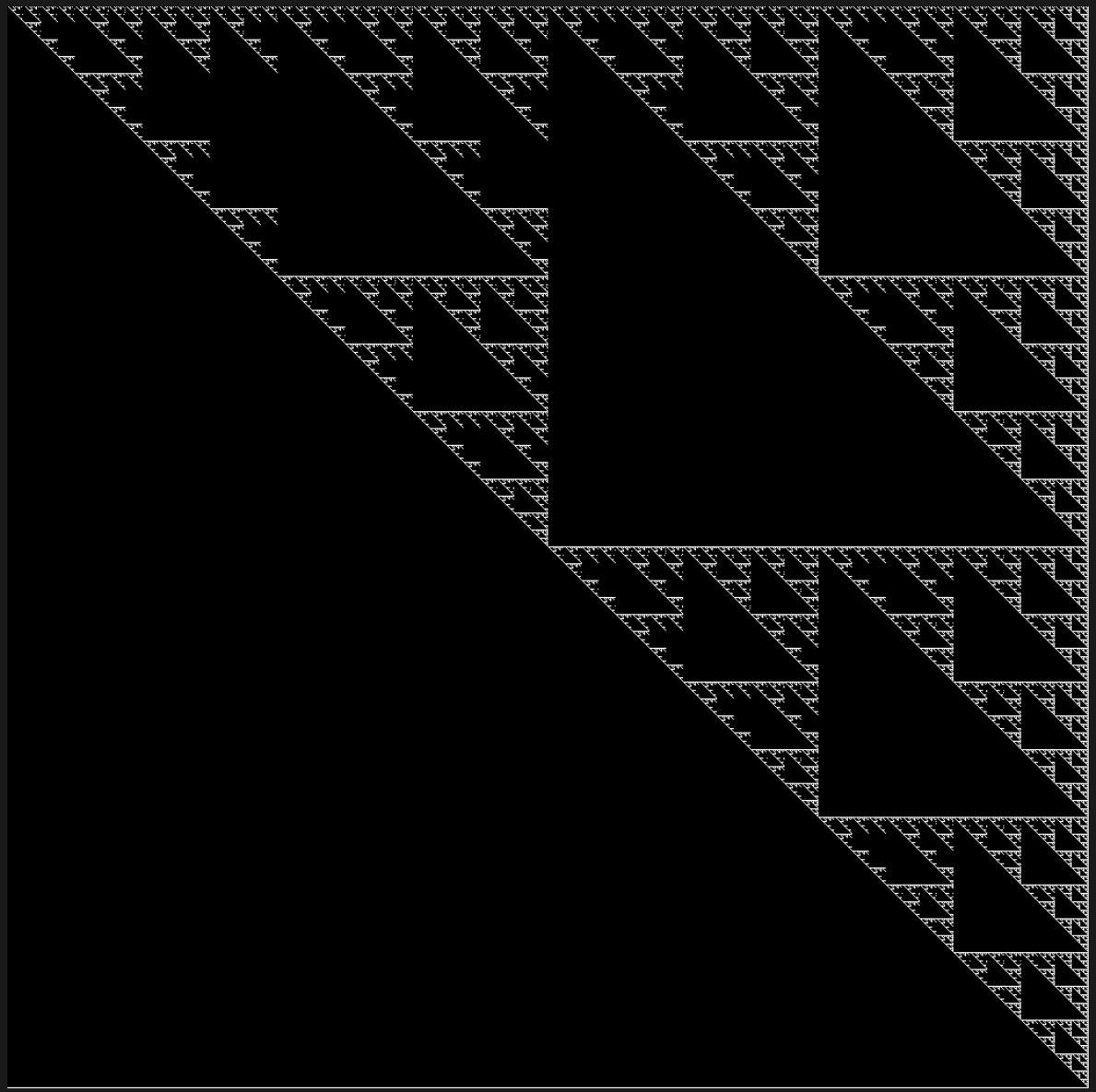
# Pictures: $FM_8^-$



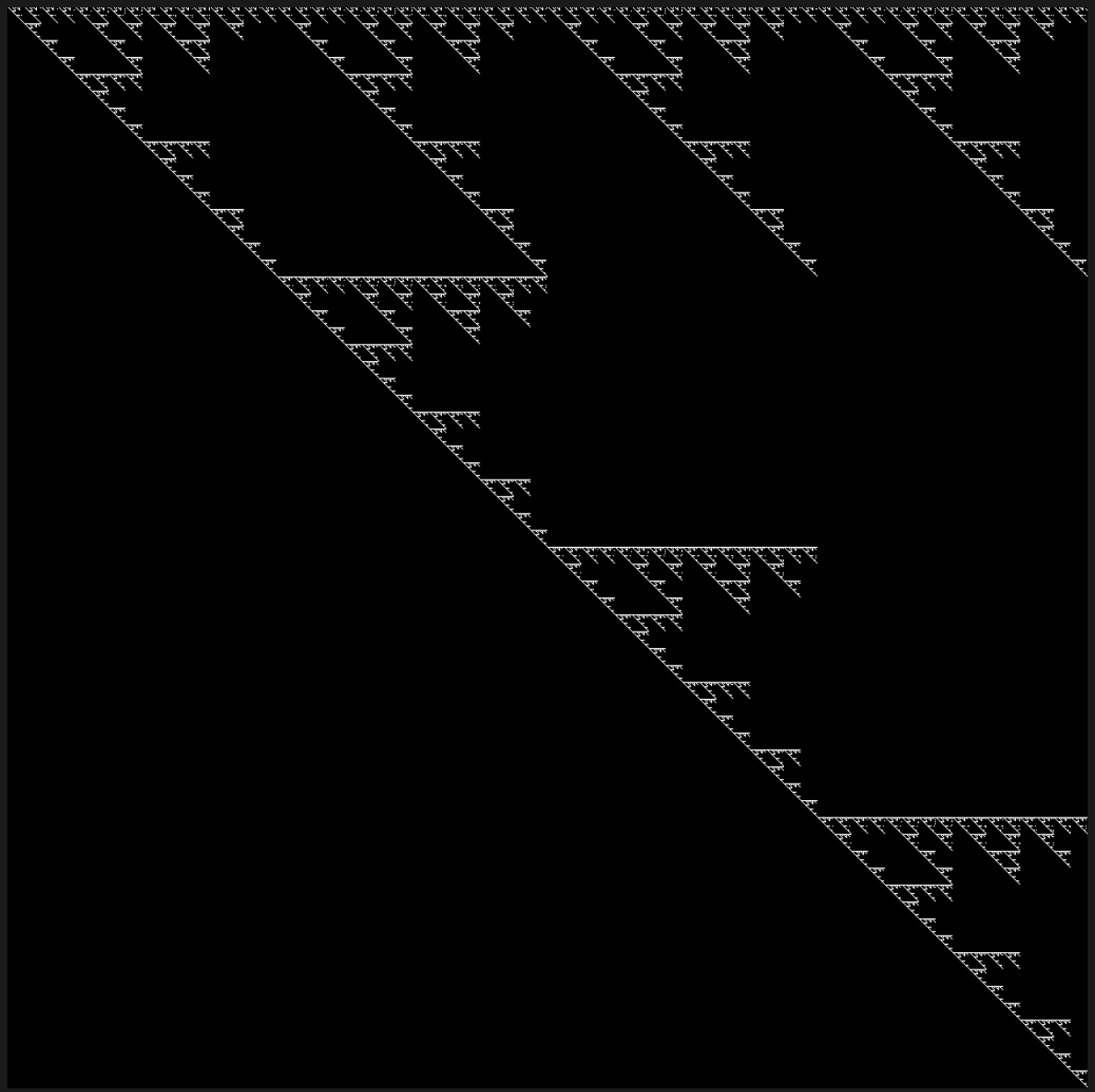
# Pictures: $FM_9^-$



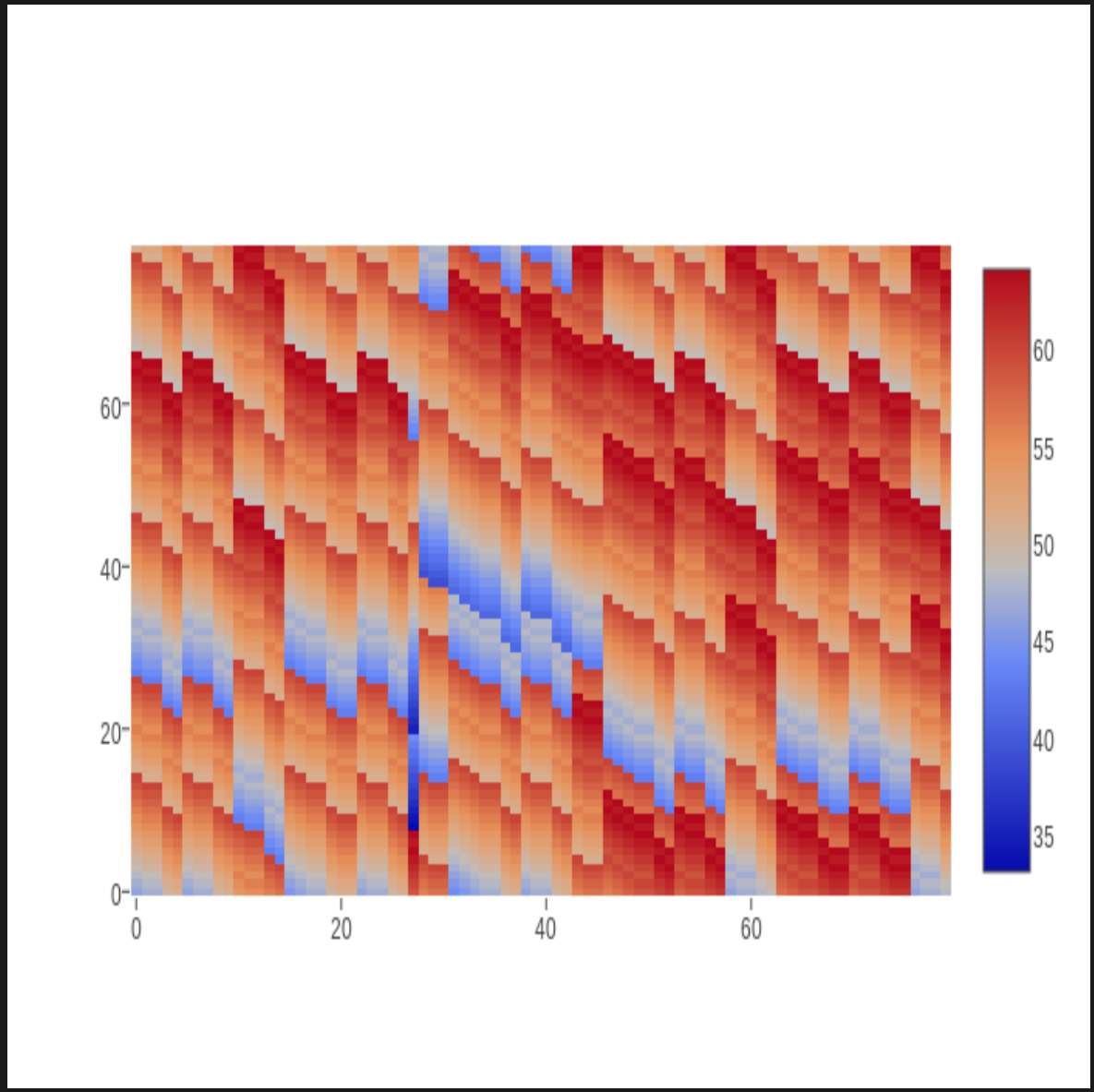
# Pictures: $FM_{10}^{-}$



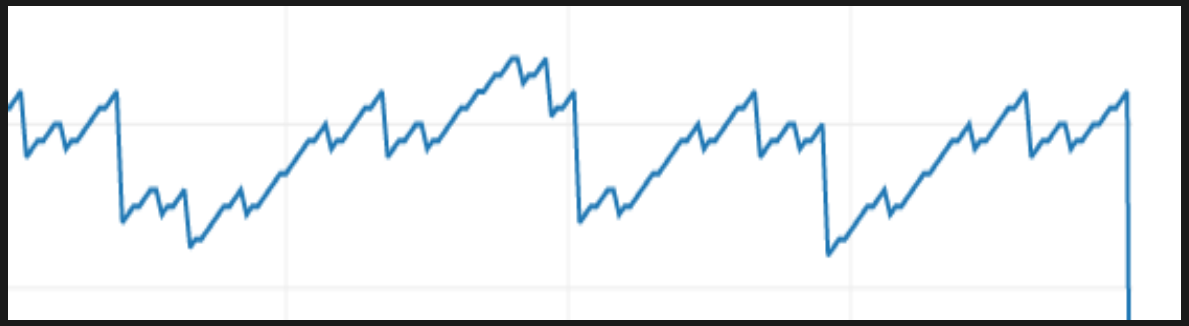
# Pictures:Multigenic Laver table snapshot



# Pictures:Endomorphic Laver table snapshot



# Pictures:Endomorphic Laver table snapshot



# The end

All work shall appear in my upcoming paper Generalizations of Laver tables (140 pages, abridged version available online).

JavaScript computer applications can be found at boolesrings.org/jvanname.