Thompson's Group F

Yarik Vitovsky

June 15, 2025

Main Talking Points

- Thompson's Group Introduction
- Binary Tree Mirrored Image and General Expression
- $\overline{X}$ Encryption

Thompson's Group F

Basic Definition

Thompson's group F is defined as the group of piecewise linear maps:

$$F : [0,1] \to [0,1]$$

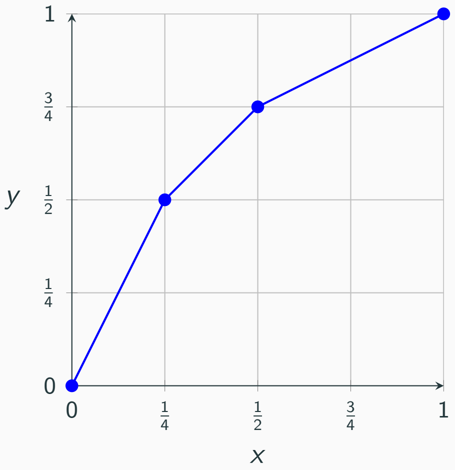
These maps are **homeomorphisms** (bijective and continuous functions with continuous inverses) that **preserve orientation**.

Definition of an Element

Each element in the group is defined by how it partitions the interval. The partition is made by dyadic rational breakpoints of the form:

$$\frac{m}{2^n}, \quad m \in \mathbb{Z}, \quad n \in \mathbb{N}$$

Example X_0



The element x_0 is defined by the following breakpoints:

$$\left[\left(\frac{1}{4}, \frac{1}{2}\right),\ \left(\frac{1}{2}, \frac{3}{4}\right)\right]$$

with the slopes of $f(t)$ in each interval:

$$f(t) = \begin{cases} 2t & \text{for } 0 \leq t \leq \frac{1}{4} \\ t + \frac{1}{4} & \text{for } \frac{1}{4} \leq t \leq \frac{1}{2} \\ \frac{t+1}{2} & \text{for } \frac{1}{2} \leq t \leq 1 \end{cases}$$

Generators in Thompson's Group F

Generators are the fundamental building blocks of the group. In Thompson's group F, all elements can be written as finite compositions of:

$$x_0, x_1, x_2, \ldots \quad \text{and their inverses}$$

Each generator x_i corresponds with:

- finite amount of unique breakpoints (all dyadic rationals)
- slopes that are powers of 2
- a well-defined inverse x_i^{-1} (also a homeomorphism)

Algebraic Form of F

These generators arise from a broader algebraic definition of Thompson's group F, known as its infinite presentation, which is given as:

$$\left\langle x_0, x_1, x_2, \ldots \,\middle|\, x_i^{-1} x_j x_i = x_{j+1}, \text{ for } i < j \right\rangle$$

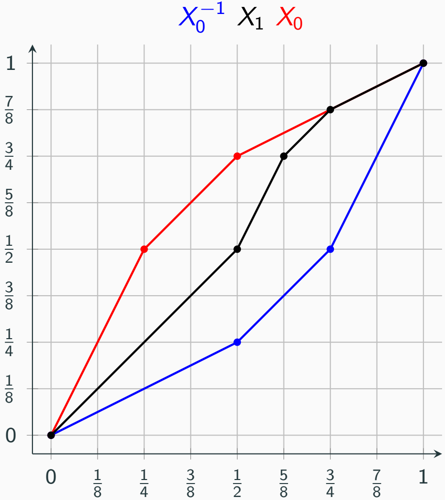
meaning that, due to its non-abelian structure and the function of composition, Thompson's group contains an infinite number of elements.

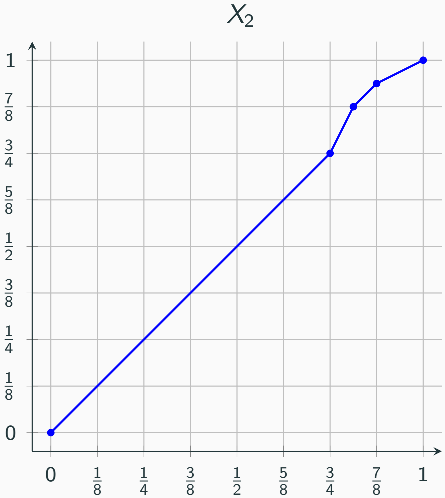
For every X_n, each breakpoint is generated by the formula:

$$\left[\left(1-\frac{1}{2^n}, 1-\frac{1}{2^{n+1}}\right), \left(1-\frac{3}{2^{n+2}}, 1-\frac{1}{2^{n+1}}\right), \left(1-\frac{1}{2^{n+1}}, 1-\frac{1}{2^n}\right)\right]$$

Generating X_2

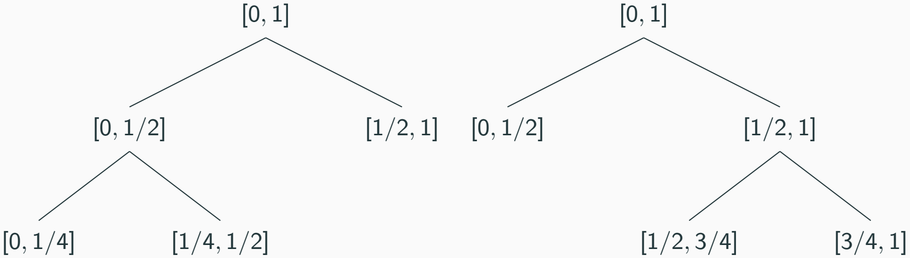
To generate the element X_2 we apply the conjugation: $X_0^{-1} X_1 X_0 = X_2$





Binary Trees

Since dividing the interval [0,1] defines a mapping function, it can be equivalently represented as a binary tree



This binary trees correspond to x_0 with the following breakpoints: $[(\frac{1}{4}, \frac{1}{2}),\ (\frac{1}{2}, \frac{3}{4})]$

Mirroring for Encryption

In our project, we studied mirrored binary trees as a part of the RSA public key protocol.

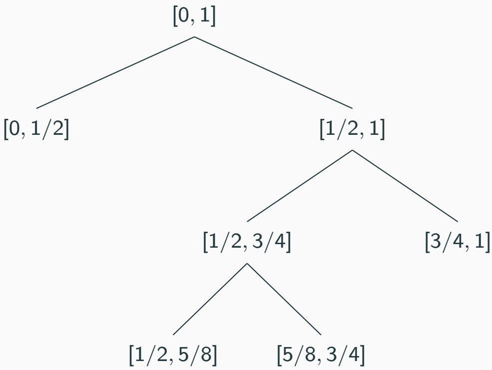
The key idea was to encrypt a message or generate a key using the mirroring operation. We took the tree representation of a known generator (e.g., X_1) and applied a structured mirroring process to produce a transformed version, $\overline{X_1}$.

This mirrored version preserves important algebraic properties while being structurally different, making it a strong candidate for use in encoding, decoding, or generating secure elements in group-based cryptographic systems.

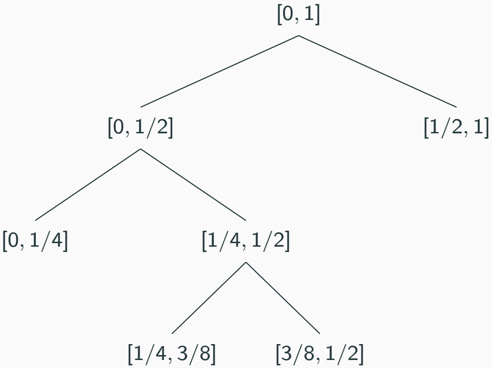
Mirroring Operation

X_1

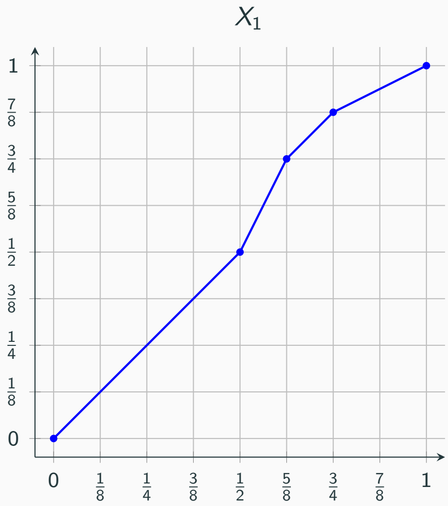
x tree

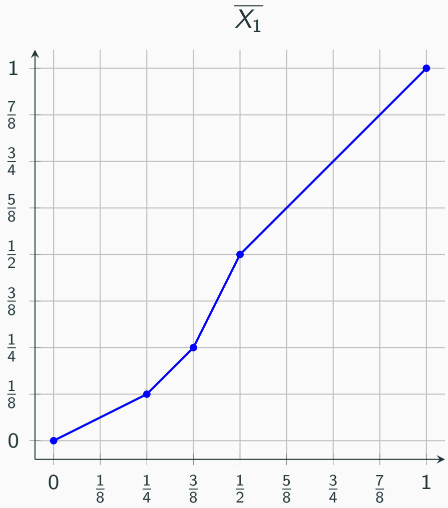


x tree mirrored

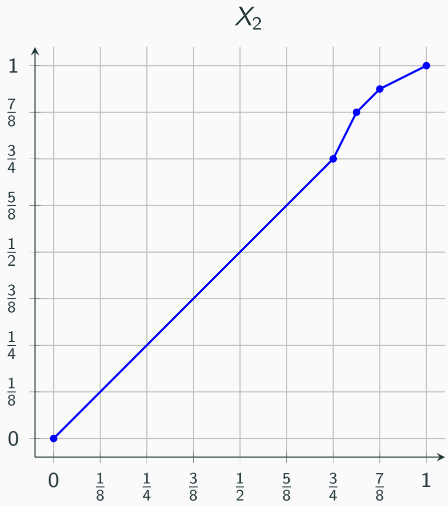


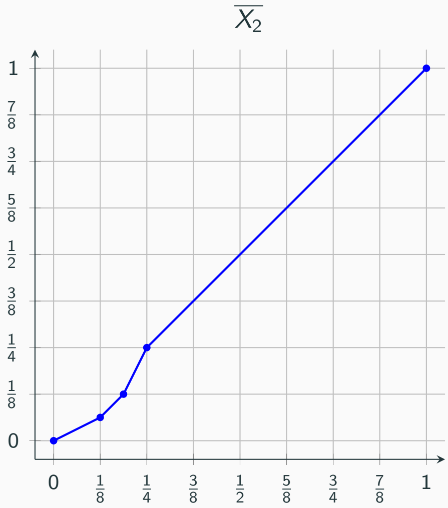
Mirrored Image Graph





The Pattern Continues





Interval Reflection in $\overline{X_n}$

Let the ordered sequence of subintervals that partition $[0,1]$ for X_n be:

$$\{(a_1, b_1),\ (a_2, b_2),\ \ldots,\ (a_k, b_k)\}$$

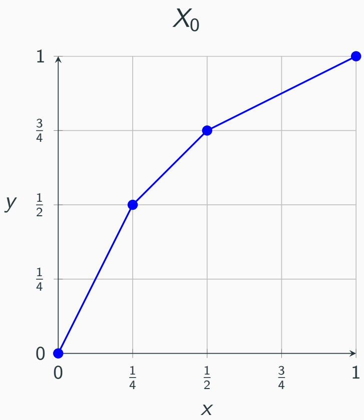
The mirrored function $\overline{X_n}$ reflects each part across the unit interval by the ordered sequence in reverse and by:

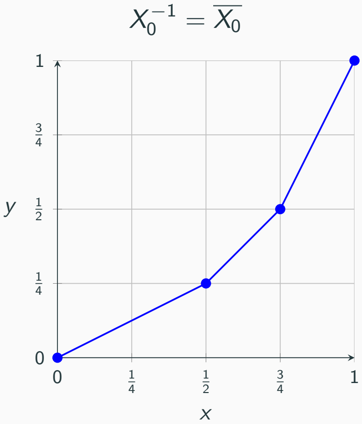
$$(a_i,\ b_i) \mapsto (1 - b_i,\ 1 - a_i)$$

The resulting sequence becomes:

$$\{(1 - b_k,\ 1 - a_k),\ \ldots,\ (1 - b_2,\ 1 - a_2),\ (1 - b_1,\ 1 - a_1)\}$$

Uniqueness of X_0





Among all generators, X_0 is unique in that its inverse coincides with its mirrored version:

New Objective

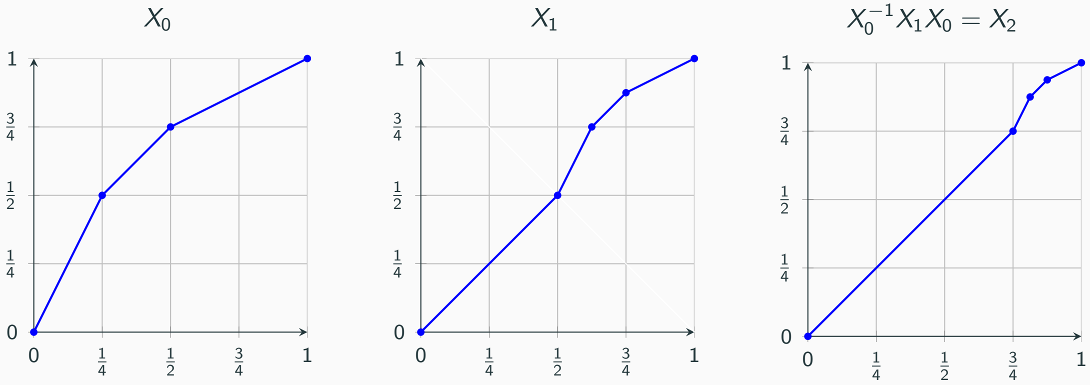
So far, we've explored:

- The definition and structure of Thompson's group F
- Different representations of group elements with some examples
- The process and patterns that arise when mirroring these elements

Our next goal:

To find a general algebraic expression for any mirrored element $\overline{X_n}$ using only the known generators and operations of F.

To achieve our goal, we first recognize the common pattern of generators in growing iterations.



First Expression

As we move to higher-index generators, we apply more layers of conjugation using X_0 and its inverse (excluding the original generators X_0 and X_1). This repeated conjugation causes the graph to gradually "shrink" towards 1.

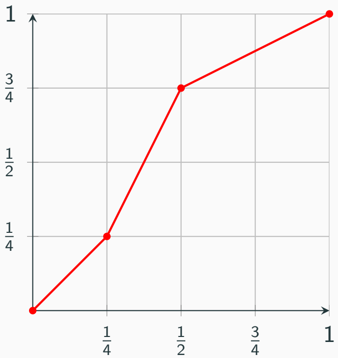
$$X_0^{-1}X_1X_0 = X_2 \quad \Rightarrow \quad X_0^{-2}X_1X_0^2 = X_3 \quad \Rightarrow \quad X_0^{-3}X_1X_0^3 = X_4$$

This naturally raises the question: What happens if we reverse the direction of the conjugation? That is:

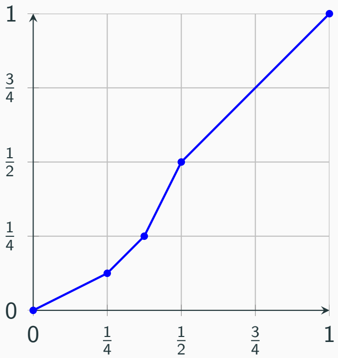
$$X_0X_1X_0^{-1} = ?$$

Current vs. Desired

Current ($X_0X_1X_0^{-1}$)

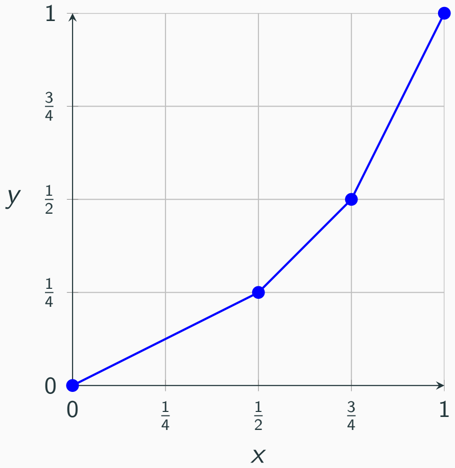


Desired ($\overline{X_1}$)



We're actually quite close - the first and last subintervals, (0,1/4) and (1/2,1), already match the mirrored structure. What's left is adjusting the slopes.

Graph of X_0^{-1}



We observe that X_0^{-1} adjusts the slopes exactly as needed.

Slope adjustment:

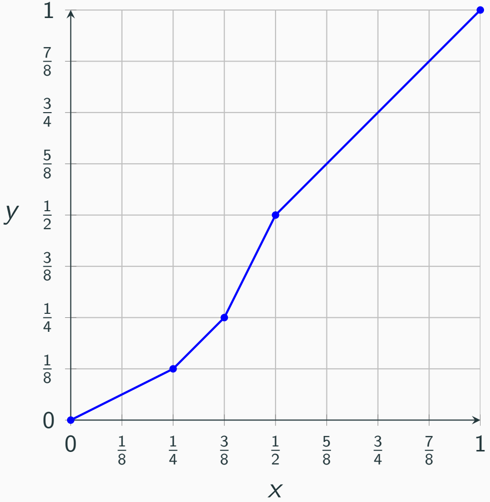
$$\text{Starting slope: } 1 \cdot \tfrac{1}{2} = \tfrac{1}{2}$$

$$\text{Ending slope: } \tfrac{1}{2} \cdot 2 = 1$$

This makes X_0^{-1} the final piece of the puzzle in constructing $\overline{X_1}$.

Result

Graph of $\overline{x_1}$



From our construction, we find:

$$X_0 X_1 X_0^{-2} = \overline{X_1}$$

This suggests the general formula:

$$\overline{X_n} = X_0^n X_1 X_0^{-(n+1)}$$

This expression generates the mirrored version $\overline{X_n}$ for any index n.

Proof By Induction

Goal: Show that

$$\overline{X_n} = X_0^n X_1 X_0^{-(n+1)} \quad \text{for all } n \in \mathbb{N}$$

using induction.

Base Case: $n = 1$

$$\overline{X_1} = X_0 X_1 X_0^{-2}$$

The base case holds.

Inductive Hypothesis: Assume

$$\overline{X_k} = X_0^k X_1 X_0^{-(k+1)} \quad \text{for some } k \in \mathbb{N}.$$

Inductive Step

To prove:

$$\overline{X_{k+1}} = X_0^{k+1} X_1 X_0^{-(k+2)}$$

Recall the recursive rule:

$$\overline{X_{k+1}} = X_0 \cdot \overline{X_k} \cdot X_0^{-1}$$

Substitute the inductive hypothesis:

$$= X_0 \cdot \left(X_0^k X_1 X_0^{-(k+1)} \right) \cdot X_0^{-1}$$

Group powers:

$$= X_0^{k+1} X_1 X_0^{-(k+2)}$$

The formula holds for $k+1$. Thus, by induction, it holds for all $n \in \mathbb{N}$.