About a Mathematical Model of the Eye Glyphs

Chris Mzz.

Last updated on May 3, 2023

Contents

Introduction

If you're reading this, the *eyes* need no introduction. I won't waste your time explaining what they are, but if you did somehow end up downloading this document and have no idea what it's for, you should probably read about this somewhere else.

The biggest source of eyes info I can point you towards would be Gonzo's The Emerald Tablet, containing as much info as possible about the topic.
If you want the main info, you can read this page from the wiki [4], or this document [3].

As I don't need to elaborate on the context of the puzzle itself, I'll use this section to talk about me, and why I chose to write a document about this.
I'm Chris, a third year in Maths University (Aix-Marseille Université, France, I know I'm doxxing myself but trust me, my personal info's basically everywhere anyway), and although that doesn't give me any authority on mathematics as a whole, I haven't seen a lot of variety in the math-based methods to model this puzzle, so *that's what this document will mainly try to do*.

For clarification, I'll model the problem in different ways that all focus on different fields of mathematics, so that *anyone* who has some high-level education in maths can try and have a crack at making up a new method to try and solve the puzzle (not that anyone really needs help with that, the community's been killing it with new ideas [6]).

I'll obviously try to explain how and why some of the concepts I'll mention are useful in the context of solving the puzzle, but no promises on trying to actually use them. And, I'm sorry, but I won't be tackling cryptography as a whole as there's already a **lot** of documents covering that already [2].

For convenience, I'll denote the center, upwards, right, downwards, and left eyes as C, U, R, D and L respectively.
The set containing all eye positions will be :

$$\mathcal{E} := \{C, U, R, D, L\}$$

1 The algebraic $\mathbb{Z}_5$ approach

The most obvious way of viewing the problem, that has been used before, is representing the eye positions as numbers mod 5.

Let's add some context to that.

1.1 (not) Group Theory

In group theory, a *group* can be mostly thought of as a combination of a set, and an operation, generally addition, denoted by $+$.
This can be for example $(\mathbb{Z}, +)$, the integers.

A *ring* is the combination of a group and another operation, generally multiplication denoted by $\times$ or $\cdot$ (rings aren't like fields though, so you don't have to worry about inverses being defined).

Consider the ring $(\mathbb{Z}_5, +, \cdot)$.
An element of the ring is, by definition, an element of $\mathbb{Z}_5$, on which we can perform addition $(+)$ and multiplication $(\cdot)$.

Forgive the seemingly unnecessary terms, but we need them to avoid confusion later.

The community who worked on this approach and developed the main ideas surrounding it decided the following attribution [3] :

$$C = 0, \quad U = 1, \quad R = 2, \quad D = 3, \quad L = 4$$

This, alone, does not satisfy a group structure!

The main grudge I have with this vision is that it leads members of the community to come up with ways to "add" the numbers (and maybe take the remainder mod 5 since all the numbers are already mod 5).
But **two rights don't make a left**, and therefore it is incorrect to state that $2 + 2 = 4$ in this system.

This model does have its benefits however, as we'll see shortly after this next section.

1.2 Possible Extensions

This is the part where I wanted to mention vector spaces, but can't due to a lack of group structure in our current system.

This is in my opinion, the part of the model that is most lacking, so I'll try and propose some ideas but honestly, anything goes so long as it follows a certain set of rules.

We want to choose an operation that I'll write as $*$ for now, such that :

- There is a neutral element :
$$\exists p_0 \in \mathcal{E}, \quad \forall p \in \mathcal{E}, \quad p * p_0 = p$$
Such an element will be noted 0.
- $*$ is commutative :
$$\forall (p_1, p_2) \in \mathcal{E}^2, \quad p_1 * p_2 = p_2 * p_1$$
- $*$ is associative :
$$\forall (p_1, p_2, p_3) \in \mathcal{E}^3, \quad p_1 * (p_2 * p_3) = (p_1 * p_2) * p_3$$
- Every element has an inverse by $*$:
$$\forall p_1 \in \mathcal{E}, \exists p_2 \in \mathcal{E} \quad p_1 * p_2 = 0$$

This assumes $*$ is commutative, but if you want to try using an non-commutative operation, that's fine too, although the rest of this document might not fit just right with such a choice.

For this to work, we necessarily need to pick a 0 element, which the community has more or less agreed should be C.

From there, we need an operation $*$ that will allow us to build an isomorphism from our current system to $(\mathbb{Z}_5, +)$.
Such an operation is the cyclic relationship defined by :

$$U * U = R, \quad U * R = D, \quad U * D = L, \quad U * L = C$$

which allows us to write once and for all $(\mathcal{E}, *) \simeq (\mathbb{Z}_5, +)$, with :

$$C = 0, \quad U = 1, \quad R = 2, \quad D = 3, \quad L = 4$$

This might feel unnecessary to you, but other isomorphisms are possible with different attributions, and you could draw parallels with other groups entirely, so don't hesitate to think of other sets with 5 elements (五行, for example).

1.3 Possible Vector Space, Operations

A lot of evidence points towards regrouping an eye message as trigrams [3] [1].

Such trigrams contain 3 eyes, each staring in a given direction.

Let $\mathcal{E}^3 = \mathcal{E} \times \mathcal{E} \times \mathcal{E}$ be the Kronecker product on which we can define a more generalised version of the $*$ operation :

$$\forall (t_1, t_2) = \left(\begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}, \begin{pmatrix} p'_1 \\ p'_2 \\ p'_3 \end{pmatrix} \right) \in \mathcal{E}^3 \times \mathcal{E}^3, \quad t_1 * t_2 = \begin{pmatrix} p_1 * p'_1 \\ p_2 * p'_2 \\ p_3 * p'_3 \end{pmatrix}$$

Obviously, in a similar fashion we have $(\mathcal{E}^3, *) \simeq (\mathbb{Z}_5^3, +)$, so we'll be referring to $\mathbb{Z}_5^3$ now.

We can now extend our system to vector spaces, given *yet another* operation, say $\otimes$, from elements of a field $(S, \circ, \otimes)$, such that :

- $\otimes$ is distributive in regards to $+$:

$$\forall (t_1, t_2) \in \mathbb{Z}_5^3 \times \mathbb{Z}_5^3, \forall \sigma \in S, \quad \sigma \otimes (t_1 + t_2) = \sigma \otimes t_1 + \sigma \otimes t_2$$

- $\otimes$ is distributive in regards to $\circ$:

$$\forall t \in \mathbb{Z}_5^3, \forall (\sigma_1, \sigma_2) \in S^2, \qquad (\sigma_1 \circ \sigma_2) \otimes t = \sigma_1 \otimes t + \sigma_2 \otimes t$$

This is quite harder to find as multiplication by real number is usually the selected operation for $\otimes$, and yet there is no obvious way to multiply trigrams by a real factor.

However, constructing a vector space-like object is possible with some other operations that work on bigger sets of data, namely *composition* of elements from the *permutation group* $(\mathfrak{S}_3)$. Usually, the symmetric group is used as an action over a vector space [5], which isn't what we'll be attempting in the next section.

1.3.1 Symmetric Group vector space-ish extension

I won't be showing proof that the operation is valid, as the proof is easy but requires a good understanding of permutations in $\mathfrak{S}_n$ and explaining the details of that is completely pointless in regards to the vector space itself.

In this case, we'll be looking at $(\mathfrak{S}_3, \circ)$, where $\circ$ will act as $\circ$ and $\otimes$ from the previous definition. Composition between permutations is common, and applying a permutation from $\mathfrak{S}_n$ to any n-sized array (in our case, a vector), is rather natural.

Here is an example of how you could apply operations between trigrams in this vector space :
Let $t = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}, t' = \begin{pmatrix} p'_1 \\ p'_2 \\ p'_3 \end{pmatrix} \in \mathbb{Z}_5^3$. Consider $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in \mathfrak{S}_3$.

$$t + t' = \begin{pmatrix} p_1 + p'_1 \\ p_2 + p'_2 \\ p_3 + p'_3 \end{pmatrix}$$

$$\sigma(t) = \begin{pmatrix} p_3 \\ p_1 \\ p_2 \end{pmatrix}$$

Just as a proof of concept, it's distributive :

$$\sigma(t)+\sigma(t')=\begin{pmatrix}p_3\\p_1\\p_2\end{pmatrix}+\begin{pmatrix}p'_3\\p'_1\\p'_2\end{pmatrix}=\begin{pmatrix}p_3+p'_3\\p_1+p'_1\\p_2+p'_2\end{pmatrix}=\sigma(t+t')$$

And each element in $\mathfrak{S}_3$ has an inverse in regards to $\circ$. We'll write τ_{ij} the transpositions between the i-th and j-th element to save space :

σ	σ^{-1}
id	id
τ_{12}	τ_{12}
τ_{13}	τ_{13}
τ_{23}	τ_{23}
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

Don't be mistaken though, this isn't a proper vector space since I don't know how one could use $\mathfrak{S}_3$ to form a ring structure, and therefore cheated this definition to fit the bill a bit better.

1.3.2 Operations on trigrams

The idea of looking at trigrams as vector-like objects of $\mathbb{Z}_5^3$ is still interesting.

To be honest, I don't know what to write in this section, but still need to include it to emphasize how important variety is in this kind of work.

Many have proposed that the cipher changes with position, or some exterior factor, so we can consider a message as a sequence of $\mathbb{Z}_5^3$ elements, say $(t_n)_{n\in\mathbb{N}}$, and then have something of the form :

$$\omega(1)=\sum_{n=0}^{+\infty}a_nt_n$$

be a converging series, where a_n is some sequence (*citation needed*).

If that seems like a cool path you want to try, have fun with it, change what you need in the terminology, you could have $\omega(1)$ only be finite for a finite message, tamper with $\omega(X)=\sum_{n=0}^{+\infty}a_nt_nX^n$, choose a_n to be a periodic function to look for patterns... anything goes, and if you're hesitating, don't hesitate to contact me.

2 Analysis

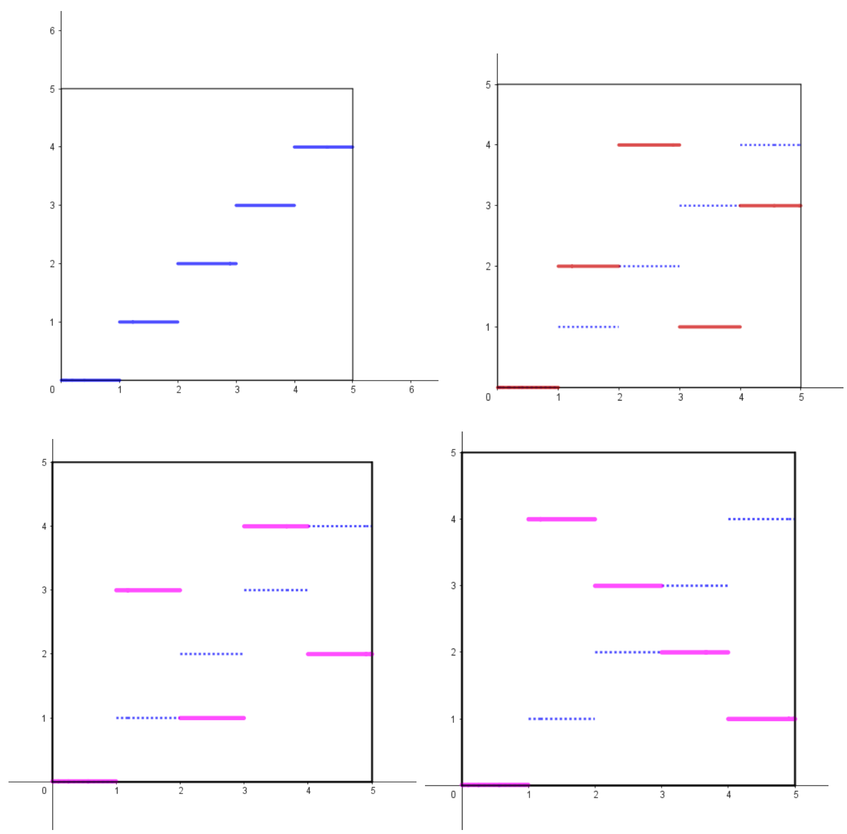
There are multiple ways of analysing the eyes by trying to identify their distribution with a function.
At first I was planning on separating this section so it could fit both real analysis and complex analysis, but real analysis on single variable functions boiled down to number theoretical functions, which, frankly, is boring.

Trivial discrete version
Here is the typical $[\![0,5]\!] \to [\![0,5]\!]$ function that would describe the eye distribution, using $\mathcal{E} \simeq [\![0,5]\!]$ similarly to our algebra section :

$$\forall n \in [\![0,5]\!], \quad f(n) = n$$

There is no really interesting thing to do at this point, so I won't dwell on it, but if you're thinking maybe you can multiply it, $Im\,(\lambda \times f([\![0,5]\!])) = [\![0,5]\!]$ for all λ such that $gcd(\lambda, 5) = 1$, also known as any number that isn't a multiple of 5.

See here for the patterns :



The blue lines are the identity function, and red or magenta just corresponds to different factors.

Top left is identity, top right is $2f$, bottom left is $3f$ and bottom right is $4f$.

2.1 The Complex Bijection

Real analysis doesn't work out too well if we stay in a single dimension, and moving up a dimension is tedious in contrast to just switching to the complex plane.
But is that possible ?

Well, actually, it's more than possible : it's *practical*.
Remember how the eyes attribution was taking $C = 0$ and then moving clockwise ?
It turns out, the complex plane's main character is perfect for rotations.

What I mean by this is that multiplying any complex number by i will effectively rotate it by $\frac{\pi}{2}$ radians on the plane relative to 0.
If you want to see the vector field associated with multiplication by i, head here, and type ix into the function definition (I have a new version where it displays it as z but I'm not going to update it just for that, sorry).
If you want proper norm colouring, you'll need to click on the **update** button, but it's not essential to understand my point.

Note : there's an error in my terminology in the "Instructions" section, due to a copy-paste mistake from my Pólya field applet, this is not a Pólya vector field.

Main takeaway :

> We can identify $\mathcal{E}$ with $\{0, i, 1, -i, -1\}$, by identifying $\mathbb{C} \simeq \mathbb{R}^2$ and noticing that these are precisely the directions the eyes are staring in.
>
> Multiplying by $-i$ rotates clockwise and therefore always yields the "next" element in the list (excluding the center position), but the best part is that now, *up+down=center* and *left+right=center* is justified by a way more natural set of equations :
>
> $$1 - 1 = 0 \quad i - i = 0$$

We could definitely extend $[\![0, 5]\!]$ to $[0, 5]$, but that would seem odd as the numbers between 0 and 5 serve more as indexes, and having numbers between that might require some very personal interpretation, as multiplication between the numbers themselves was very up in the air.

Let's change that.

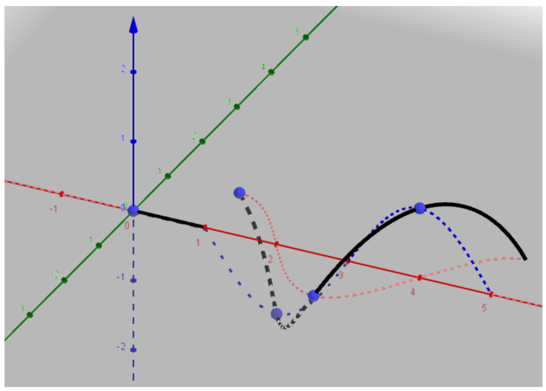
2.2 A Complex Extension

Let $f : [0, 5] \to S_E(0, 1)$ where $S_E(0, 1)$ is the union of the unit sphere in $\mathbb{C}$ and a single point at zero $S(0, 1) \cup 0$, defined by :

$$f(x) = \begin{cases} 0 & \text{if } 0 \le x < 1 \\ e^{\frac{i(2-x)\pi}{2}} & \text{if } 1 \le x \le 5 \end{cases}$$

The only problem with this model is that it isn't continuous in $x = 1$.
I'm not sure this can be, or even *should* be fixed, as it could currently be described as a piecewise smooth function on $[0, 5]$, where each smooth component is either constant or bijective with another space.

For those wondering what this function looks like, here it is.



Complex function extended to piecewise smoothness, with projections on the real space (red) and imaginary space (blue).

Along the X-Axis :	variable x running through $[0, 5]$.
Along the Y-Axis :	real part of $f(x)$.
Along the Z-Axis :	imaginary part of $f(x)$.

2.2.1 Working on trigram vectors of the form $t \in Im(f)^3$

The tricky part here, is that now we have a function that's defined on a real interval, and we want 3D vectors in which each component represents an eye.
As we previously established, a 360° rotatable eye is represented by any complex number of module 0 or 1, so we have :

$$t \in Im(f)^3 \Leftrightarrow \exists (p_1, p_2, p_3) \in S_E(0, 1), \qquad t = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

Now, many operations can be defined on trigrams as $Im(f)^3 \subsetneq \mathbb{C}^3$.
The kind of operation we want is more restricted, however, as we want the results to remain bounded in $S_E(0, 1)$.

For convenience, let's write $T := Im(f)^3 = S_E(0, 1)^3$.

Multiplication :

Let $(t,t') \in T^2, \quad t = \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}, \quad t' = \begin{pmatrix} p'_1 \\ p'_2 \\ p'_3 \end{pmatrix}.$

The most natural step to take with this method is multiplication applied on each component, which corresponds to rotation by a certain amount per component (or nullification) :

$$t \times t' := \begin{pmatrix} p_1 \times p'_1 \\ p_2 \times p'_2 \\ p_3 \times p'_3 \end{pmatrix}$$

Here is an applet that lets you play around with multiplication and exponentiation, displaying the set of images in the 2D graphs view, so you don't have to rotate around in the 3D view all the time.

What can this help with ?

Many community members such as Lymm seem to think a rotating cipher is in play rewording to not have to include context) :

"*The ciphertext alphabet [could] be thought of as a disk that rotates by some particular amount at each step. The amount it rotates could depend on the plaintext. The order of the symbols on the wheel may not be the numerical order of the trigram values.*"

I really like this idea, and I think the complex extension might help with computing solutions to this in a readable way.

Here are some ideas :

(i) There's something I haven't seen proposed a lot, given it isn't likely, but, maybe this rotating cipher translates back to eye trigrams.
Now suppose we have a trigram wheel that you'd have to compose with the entire message to get a more clear message (maybe solvable using frequency analysis).

(ii) Instead of having a trigram wheel, we could use an ordered set of $\mathfrak{S}_3$ permutations to apply to the trigrams and achieve a similar result to (i).

(iii) Defining a refined scalar product over T could lead to a new space on which translation is more likely. This has been proposed multiple times in different ways, but there are so many ways to do it that we'd need more in-game clues before needing to try it (if ever you find in-game information about how to combine three values into one in a *specific* way, please let everyone know).

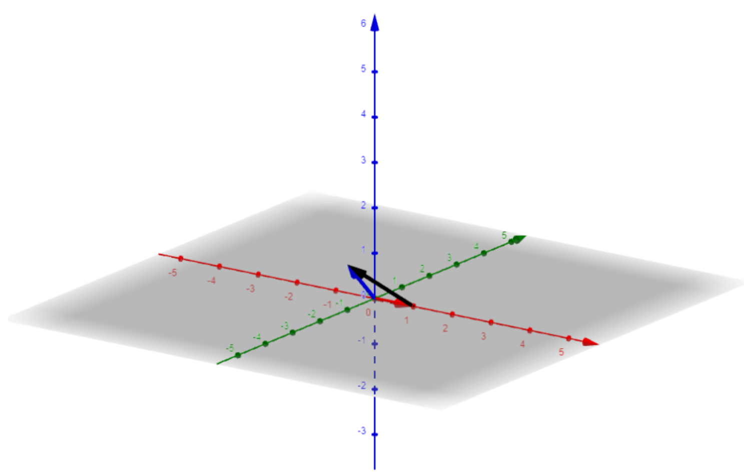
2.2.2 Representing trigrams in $T := Im(f)^3$, thanks to $T \subsetneq \mathbb{C}^3 \simeq \mathbb{R}^3 \times \mathbb{R}^3$

In this subsection, the piecewise-smoothness won't be of any use, but it's still good practice to prove that such a model does exist to further remove any future contradictions in the paper.

We would like to use this model to represent the trigrams in a vector space that we can visualise in hopes to extract meaningful information.
We'll want a visual representation of our vector space $T := Im(f)^3 = S_E(0,1)^3$ which is a subspace of $\mathbb{C}^3$. As each component of a vector is *complex*, the dimension of this space is actually 6, not 3, so we'll have trouble representing the trigrams in a 3D graph.

What I tried doing was breaking up a trigram into two separate *sub*-trigrams, one containing the real part and the other containing the imaginary part.
This action would form a bijection between $\mathbb{C}^3$ and $\mathbb{R}^3 \times \mathbb{R}^3$, then leaving us room to represent any trigram as **two** vectors in 3D space.
However, we'd need a way to separate one from the other, to know which is the *real* vector and which is the *imaginary* one.

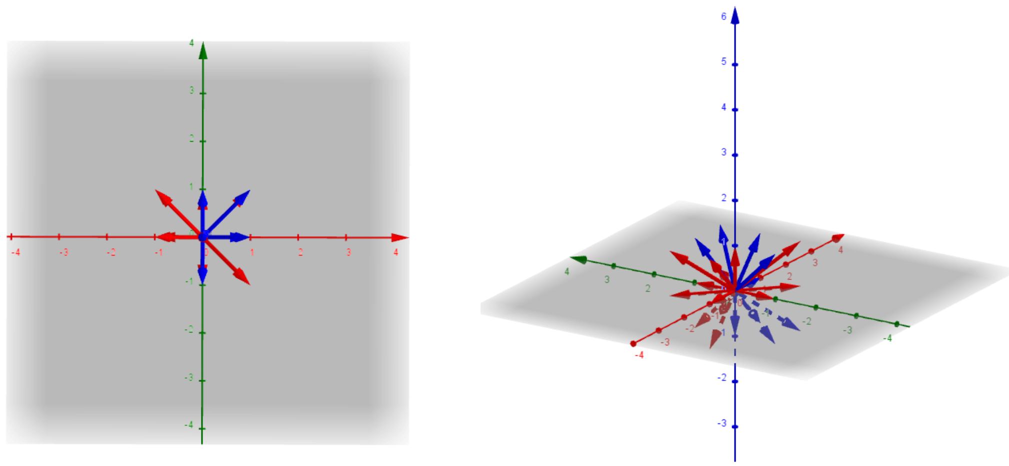
This lead me to arbitrarily colouring the real part in blue and imaginary in red.
Here is the graph it ended up giving, with a few tweaks to make it read any of the 9 messages but also any custom trigram.



Representation of a trigram in $\mathbb{R}^3 \times \mathbb{R}^3$

2.2.3 Results and points of interest

Thanks to this model, it's possible to view every trigram of every message at once, and notice that a couple vectors are entirely missing.
We know that only 83 of the possible 125 trigrams actually appear in the messages, but it was not known that by pairing left/right with up/down would also yield an incomplete set of vectors.



View of all trigrams of all messages along last vector component (left)
Side view of all trigrams of all messages (right)

An entire cardinal direction is missing, not being generated neither by real, nor by imaginary part.
This is an entirely separate remark from the 83 trigram fact, although it's of course a consequence of the fact that the trigrams don't represent the whole set.

What this tells us is that the set of *missing* trigrams (the missing 42) is specific enough that positions 1 and 2 of a trigram never hit both left or both down, leaving an gap in this representation.

Another single vector is missing : left/right/left or down/up/down vector.

This leaves a total of 4 missing vectors from the entire set of vectors (27 vectors) :

$$\begin{pmatrix}-1\\-1\\-1\end{pmatrix},\quad \begin{pmatrix}-1\\-1\\0\end{pmatrix},\quad \begin{pmatrix}-1\\-1\\1\end{pmatrix},\quad \begin{pmatrix}-1\\1\\-1\end{pmatrix}$$

Note that all vectors are overlapping, so the colours in the figures above are meaningless, there could for example be a red and blue vector overlapping in the same spot.

Final Notes

I have work to do so I don't have too much time to experiment, but the point of extending the model to a function like this one proposed here, is to allow for a wider range of operations.
The point of the whole document is to have a couple models that work, and extend them to a more general model each time, to make the math easier to work on, so it won't always be one-to-one.

This document will be updated, but I'm afraid I can't be 27/4 on this (yes I saw the typo but it's funny so I'll leave it).

Don't hesitate to contact me if you have something you think might be useful for the document, or something you think is inaccurate.
I'm also available if you need help on something, so yeah, you can DM me on Discord !

Sincerely,
Chris Mzz.#0523  (thanks for the art **Ry**!)

Exterior Sources, Further Reading

Couldn't find any easy to read paper on :

- Non-abelian vector spaces,
- Recursively defined sequences used in whole series.

References

[1] Noita eye data. https://docs.google.com/spreadsheets/d/195Rtc8kj4b74LtIyakqGP-iHhm36vyT5i8w7H5JjOV8/edit#gid=1929937409.

[2] codewarrior0. Noita eye glyphs: Analytical overview. https://docs.google.com/document/d/1QeagH8TklJsd8iribMtT5LIRL91laOUU_tFcVl7OOqA/edit#heading=h.kube2smqfujy.

[3] Multiple contributors. Noita eye glyph messages. https://docs.google.com/document/d/1s6gxrc1iLJ78iFfqC2d4qpB9_r_c5U5KwoHVYFFrjy0/edit.

[4] Multiple contributors. Noita eye glyph wiki. https://noita.wiki.gg/wiki/Eye_Messages.

[5] LUCAS REIS. On the dimension of permutation vector spaces. *Bulletin of the Australian Mathematical Society*, 100(2):256–267, 2019.

[6] Toboter. Noita eye glyphs "progress". https://docs.google.com/document/d/1XMNXktCoSabnFWZf9rJFoaKMzsA1bbv7x1Xh9tXkKYk/edit#heading=h.gq20wfhs4tmi.