Graphe associé au corps $F_5[x]/(1+3x+x^2+3x^3+x^4)$

Gaëtan Kuhn

Who am I ? A former student of the University of Geneva who finished his master's degree in mathematics in February 2020. For my master thesis, I studied the links between algebraic structures and graphs. My supervisor Anders Karlsson and I then co-authored a paper on a completely new type of graph associated with finite fields.

What do we see on this picture ? It is a graph, i.e. an object composed of vertices (points) and edges (links between two vertices). In this case, this graph has 625 vertices and 4996 edges. Graphs are combinatorial objects that can be useful in different areas of mathematics. What you see is one of its geometric realizations.

In which context does this graph appear ? As mentioned above, graphs can be used in different areas of mathematics. This one belongs to a family of graphs, used in general algebra to distinguish different models of a finite field. It represents one of the models of $GF(5^4)$: the quotient $F_5[x]/(1+3x+x^2+3x^3+x^4)$.

What's the point of distinguishing different models of finished fields ? Let's start by shedding some light on this notion of field. A finite field is a mathematical structure with p^n elements, equipped with two compatible operations (a sum and a product). The number p must be a prime number and n a positive integer. For each pair of (p, n), there is "only one finite field up to isomorphism". Behind this somewhat indigestible denomination lies the following idea : two fields with the same number of elements have equivalent operations. However, the choice of a model proves to be important when making (large) calculations, especially when these objects are implemented in algorithms. Some are more efficient and faster than others. This may seem to contradict what has been said in the previous paragraph, but this is not the case. To illustrate this, let us make an analogy. Let us consider addition and multiplication as we know them. Next, let's take the Arabic and Roman numbering systems as two "models" for representing our elements, the numbers. If I ask you to calculate the sum of forty-three with one hundred and thirty-two, you will agree that it is more convenient to do the calculation with the Arabic numerical model (43 + 132), rather than with the Roman model (XLIII + CXXXII). And let's not even talk about multiplication ! So the nature of the operation remains the same, but the models are different and for calculation, one is more convenient than the other.

I want more details ! A graph of this family is constructed as a superposition of two Cayley graphs (of the additive group and the multiplicative group), with the roots of the polynomial that builds our model as generators. These graphs have been designed so that an automorphism of field is an automorphism of graph.

The orange part corresponds to a Cayley graph of the group ${C_5}^n$. It is not surprising to have a very regular shape linked to 5. For the cyan part on the other hand, it is a little more chaotic ! There is nevertheless a tendency : for very large fields, an epicycloid [1] at $p \pm 1$ petals appears. This is a phenomenon that can be found in simpler graphs, associated with the usual multiplication tables (c.f. references from [2] to [4]).

1. Plane curve produced by tracing the path of a chosen point on the circumference of a circle which rolls without slipping around a fixed circle

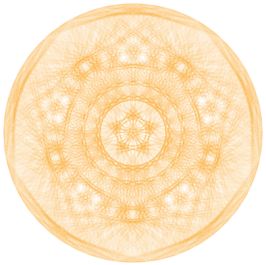

FIGURE 1 – Additive subgraph

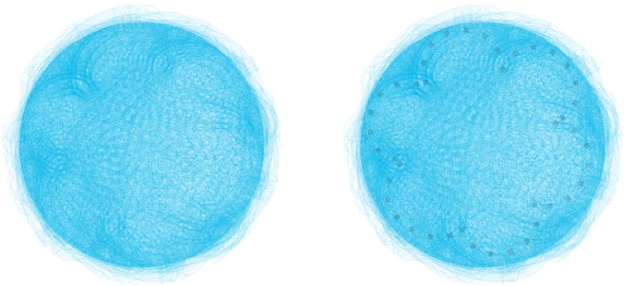

FIGURE 2 – Multiplicative subgraph

As far as the classical invariants of graphs are concerned, the graphs of this family are connected, with a diameter bounded by : $((2p-1)(2n+1)-3)$. Computer simulations tend to show us that this diameter might actually be much smaller, which would make this family of graphs all the more interesting ! Its mesh size is 2, the cycles in question are around $x^{p^k}(x^{p^k}-1)^{-1}$. It is a property that comes directly from the structure of the fields we are studying. Other properties regarding the roots of the polynomial, such as being a normal or primitive element, also materialize on the graph. A few eigenvalues have been found, but most of its spectrum remains unknown for the moment. If you wish to have more details, you can read the article [1].

Références

[1] Anders Karlsson and Gaëtan Kuhn *A natural graph of finite fields distinguishing between models*. Submitted, 2020.

[2] Simon Plouffe *La forme de b^n mod p*. Non publié, 2020.

[3] Simon Plouffe *The reflection of light rays in a cup of coffee*. Non publié, 2020.

[4] Heider Alward, *The Dancing Mandala : Multiplication Tables Plotted on a Unit Circle*, `https://www.youtube.com/watch?v=13be44CqrrI`

[5] Mathologer, *Times Tables,Mandelbrot and the Heart of Mathematics*, `https://www.youtube.com/watch?v=qhbuKbxJsk8`