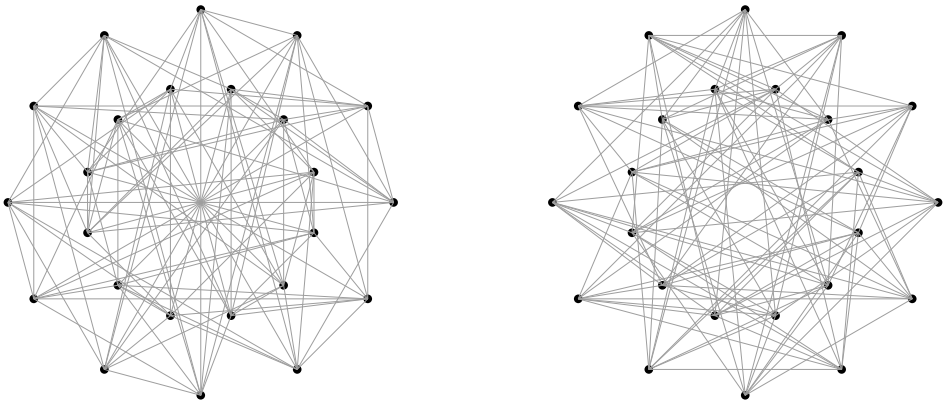
université
PARIS-SACLAY

GRAPHS
IN
THE QUANTUM WORLD

AMAURY FRESLON



Mathématiques
Orsay

FOREWORD

These are extended notes based on a lecture series given at Université Paris-Saclay during the welcome days of the Master's programme for the academic year 2026–2027. The aim of the programme was to give incoming Master's students a glimpse of some of the research topics pursued within the Department of Mathematics through a series of introductory lectures. The lectures covered by these notes focus on recent developments in the theory of quantum isomorphism of graphs and its connections with quantum information theory, operator algebras, and combinatorics.

Since the participants were Master's students, many of whom were just about to begin the programme, we kept the prerequisites to the level of a strong bachelor background. Consequently, we chose to focus on the interplay between combinatorics and Hilbert spaces – both familiar concepts to the students – and to avoid compact quantum groups altogether. This pedagogical choice largely determined the structure of the lectures.

The field presented in these notes is developing rapidly in many different directions, with substantial interaction between several mathematical communities. As a result, it is difficult to provide an exhaustive bibliography. We have done our best to cite sources that we believe will be useful to readers wishing to explore the subject further, but we have undoubtedly overlooked some relevant references, for which we apologise.

CONTENTS

FOREWORD

CONTENTS

LECTURE 1
THREE SHADES OF GRAPH ISOMORPHISM
1.1 A brief introduction . . . 1
1.2 The graph isomorphism game . . . 2
Classical setting . . . 3
Quantum setting . . . 4
1.3 Quantum permutations . . . 6
1.4 Counting homorphisms . . . 11
1.5 The Fundamental Theorem . . . 15

LECTURE 2
PERFECT ISN'T EASY
2.1 Graphs, games and the quantum . . . 19
2.1.1 From games to quantum . . . 19
2.1.2 The trace problem . . . 24
2.2 Constraints . . . 27
2.2.1 Classical isomorphism . . . 29
2.2.2 Quantum isomorphism . . . 30
2.2.3 Excursus : quantum independence . . . 32
A definition . . . 32
Connection to quantum isomorphism . . . 33
2.3 Examples . . . 36
2.3.1 The magic square . . . 36
2.3.2 More examples : the Arkhipov construction . . . 39

LECTURE 3
WHEN PLANAR MEETS QUANTUM
3.1 The strategy . . . 43
3.2 The basic operations . . . 47
3.2.1 Disjoint union . . . 47
3.2.2 Composition . . . 48
3.2.3 Reflection . . . 49
3.3 Gadget calculus . . . 49
3.3.1 The intertwining property . . . 50
3.3.2 Crafting gadgets . . . 50
3.4 Closing the cycle . . . 52
3.4.1 Yet another isomorphism . . . 52

3.4.2 The orbits trick 55

REFERENCES

LECTURE 1

THREE SHADES OF GRAPH ISOMORPHISM

1.1 A BRIEF INTRODUCTION

The main topic of this lecture series is *graph theory*, but saying that does not say much about the contents. Indeed, graph theory is a very broad field of mathematics and it is fascinating that such simple and elementary objects as (finite) graphs have deep connections to many different areas of mathematics. For instance, one often divides graph theory into several subjects depending on the techniques involved, giving rise to terms such as combinatorial graph theory, algebraic graph theory, geometric graph theory or spectral graph theory.

In these lectures, we want to introduce the reader to what we could call *quantum graph theory*, if that expression were not ambiguous : we are not studying « quantum graphs » (which constitute a field of their own, with close ties to what we will present hereafter) but classical graphs using tools inspired by quantum physics. Our main focus, however, is not on techniques or concepts borrowed from another area of mathematics, like in the examples given in the previous paragraph. Instead, we will focus on one concept, namely a weakening of the notion of graph isomorphism.

As we will see, these *quantum isomorphisms* appear in several guises, pertaining to different points of view. The connection between these points of view is what makes the theory rich and interesting, and our ultimate goal is to convey at least part of our fascination and excitement for this emerging topic.

The goal of this first lecture is to introduce the notion of quantum isomorphism of graphs, and motivate its study. One of the most remarkable aspects of that notion is that it brings together ideas from several areas of mathematics. Starting with quantum information theory, we will define something called *perfect quantum strategies*, which is our first avatar of quantum isomorphism. Then, we will turn to operator algebras through the notion of *quantum permutation matrices*, leading naturally to a generalization of graph isomorphism in the framework of *noncommutative geometry* and provides a bridge with the theory of compact quantum groups[1]. We will also introduce *homomorphism counts*, which are combinatorial invariants that allow us to compare graphs. Once all this is set, we will be able to state Theorem 1.5.1, which we have chosen to call the FUNDAMENTAL THEOREM because of its historical and conceptual importance in the subject. It simply says that all of the generalized notions of graph isomorphism that we introduced are equivalent, and it will be the cornerstone of these lectures.

Before embarking on this journey, let us give a few very elementary definitions, mainly to fix the terminology and notations.

DEFINITION 1.1.1. A *graph* consists of a finite set V of *vertices* and a set E of unordered pairs of vertices called *edges*. Moreover, in this text, we always assume that there are no *loops*, i.e. that for any $v \in V$, $(v,v) \notin E$.

If we denote a graph by G, then we might write $V(G)$ and $E(G)$ for its vertex set and edge set

1. Both because of limited time and limited background of the audience, we have chosen to avoid completely the theory of compact quantum groups in these lectures. The interested reader might consult [Fre23] for more on this.

respectively, in order to distinguish them from those of other graphs. The most important notion for us will be that of a graph isomorphism, which starts with the definition of a homomorphism.

DEFINITION 1.1.2. A *homomorphism* from a graph G to a graph H is a map

$$\phi : V(G) \to V(H)$$

such that $(\phi(v), \phi(v')) \in E(H)$ whenever $(v, v') \in E(G)$. Such a homomorphism is an *isomorphism* if it is bijective and if ϕ^{-1} is also a graph homomorphism. Then, G and H are said to be *isomorphic*.

We will write $\phi : G \to H$ to express the fact that ϕ is a graph homomorphism from G to H. The set of all graph homomorphisms from G to H will be denoted by $\mathrm{Hom}(G, H)$.

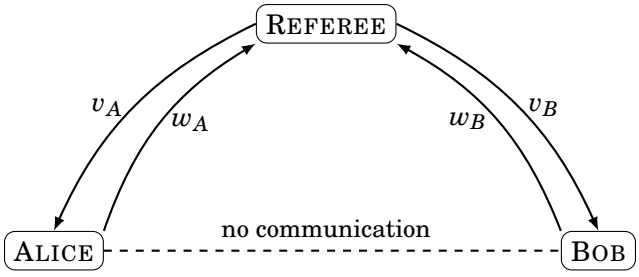
1.2 THE GRAPH ISOMORPHISM GAME

We start with quantum information theory. Very roughly speaking, *information theory* tries to describe the general properties of a communication system, and especially its effectiveness in several senses, based on an abstract framework relying only on the laws of classical physics. The first general mathematical framework for information theory was developed by C. SHANNON in the 1940's. With the advent of quantum mechanics, and especially the progressive understanding of the phenomenon of *entanglement*, it became a natural question for physicists and mathematicians alike to try to extend the theory so as to encompass the possibilities offered by quantum phenomena. This led to the development of quantum information theory as a field at the intersection of mathematics, physics and computer science. One of the basic tools in this field is called a *game*, and we will now study one. This is a simplified version of the so-called *graph isomorphism game* introduced in [AMR+19].

As is often the case in quantum information theory, the game is played by two players named ALICE (denoted by A) and BOB (denoted by B). They cooperate to win against the REFEREE (denoted by R) leading the game. The rules are given by two graphs G and H with vertex sets having the same cardinality, which are known to A and B. At each round of the game, R sends a vertex $v_A \in V(G)$ to A and a vertex $v_B \in V(G)$ to B. Each of them answers with a vertex $w_A \in V(H)$, $w_B \in V(H)$ of the other graph and they win the round if the following conditions are satisfied :

- If $v_A = v_B$, then $w_A = w_B$;
- If $(v_A, v_B) \in E(G)$, then $(w_A, w_B) \in E(H)$;
- If $v_A \neq v_B$ and $(v_A, v_B) \notin E(G)$, then $w_A \neq w_B$ and $(w_A, w_B) \notin E(H)$.

The crucial point in the story is that once the game starts, A and B **cannot communicate in any way**. The situation can be summarized by the following picture.



The natural question is then :

Question 1.2.1. Under which conditions on the graphs G and H can the players devise a strategy that always wins ?

Answering Question 1.2.1 first requires making precise sense of a *strategy*, both in the classical and quantum settings.

Classical setting

Classically, a strategy for the graph isomorphism game means that each player decides in advance which vertex they will answer depending on the input. This is quite naturally formalised through two functions

$$f_A, f_B : V(G) \to V(H)$$

such that Alice answers $f_A(v)$ when given input v and Bob answers $f_B(v')$ when given input v'.

However, in order to improve their chances of winning, the players may introduce some randomness in their strategy. We will then have functions

$$p_A, p_B : V(G) \times V(H) \to [0,1]$$

such that for any $v \in V(G)$,

$$\sum_{w \in V(H)} p_A(v,w) = 1 = \sum_{w \in V(H)} p_B(v,w).$$

This has a simple probabilistic interpretation. For $v \in V(G)$, let $X_A(v)$ (respectively $X_B(v)$) be a random variable with values in $V(H)$ and such that

$$\mathbb{P}(X_A(v) = w) = p_A(v,w) \quad \& \quad \mathbb{P}(X_B(v') = w') = p_B(v',w').$$

Upon receiving their inputs v and v', Alice and Bob both perform a random experiment corresponding to the random variables $X_A(v)$ and $X_B(v')$ respectively. The outcome of their experiments is then the answers they give.

Of course, our first definition of a strategy is a particular case of that second one, given by

$$p_A(v,w) = \delta_{f_A(v),w} \quad \& \quad p_B(v',w') = \delta_{f_B(v'),w'}.$$

This is equivalent to requiring all the random variables $X_A(v)$ and $X_B(v')$ to be deterministic, hence we will call these *deterministic strategies*.

Even though probabilistic strategies may seem more favourable, they are useless as long as one seeks a *perfect strategy*, that is to say one that wins at all times. Moreover, one can easily identify deterministic strategies which are perfect. For the convenience of the proof, we will write $(v,v') \sim (w,w')$ if answering w to v and w' to v' wins the game.

THEOREM 1.2.2 Given two graphs G and H, there exists a perfect classical strategy for the graph isomorphism game if and only if G and H are isomorphic.

Proof. We first prove that if there is a perfect probabilistic strategy, then there is a deterministic one. Let p_A and p_B describe such a strategy. Given $v,v' \in V(G)$, let $w,w' \in V(H)$ be such that

$$p_A(v,w) \neq 0 \neq p_B(v',w').$$

Since there is a positive probability that ALICE and BOB will answer w and w' respectively, and since the strategy is perfect, $(v,v') \sim (w,w')$. As a consequence, setting

$$p'_A(v,w) = 1 \text{ and } p'_A(v,z) = 0 \text{ for all } z \neq w,$$

and similarly for p_B, yields another perfect probabilistic strategy. Repeating that operation, we eventually obtain a perfect deterministic strategy since the probability distributions p_A and p_B become deterministic.

Now, given such a perfect deterministic strategy, which is described by two functions f_A and f_B, first observe that by definition, $f_A(v) = f_B(v)$ for all $v \in V(G)$ so that $f_A = f_B$. Moreover, if $v \neq v'$, then

$$f_A(v) \neq f_B(v') = f_A(v')$$

so that f_A is injective, and therefore bijective since G and H have the same finite number of vertices. Lastly, because $(v,v') \sim (f_A(v), f_A(v'))$, v and v' are adjacent in G if and only if $f_A(v)$ and $f_A(v')$ are adjacent in H, hence f_A is a graph isomorphism. ∎

Quantum setting

We now turn to the quantum world. The reader may not be familiar with the mathematical formalism of quantum mechanics or with the basics of quantum information theory, and giving a detailed introduction to these topics is certainly beyond our scope (we refer the reader, for instance, to [Wil13] for this). We will nevertheless try to motivate the definition of a quantum strategy by some quantum mechanical considerations.

The fundamental idea is that ALICE and BOB will set up before the game starts a quantum mechanical system, and then each carry part of it with them so that they can manipulate it. The quantum phenomenon known as *entanglement* will then enable them to produce correlations with the other one's subsystem by manipulating theirs without any communication. The postulates of quantum mechanics assert that the states of a quantum system can be described by the vectors of a Hilbert space. Let therefore $\mathscr{H}$ be a Hilbert space fixed once and for all and let $\psi \in \mathscr{H}$ represent the state of the system before the game starts. As it turns out, multiplying ψ by an arbitrary complex number does not change its physical content, so that we can (and will) assume that $\|\psi\| = 1$.

Another postulate of quantum mechanics is that any measurable physical quantity of the system is given by a self-adjoint operator A on $\mathscr{H}$, and that the possible outcomes of a measurement of A are the eigenvalues of A. Let us assume for the moment that $\mathscr{H}$ is finite-dimensional and write

$$\mathrm{Sp}(A) = \{\lambda_1, \cdots, \lambda_n\}.$$

If Π_i denotes the orthogonal projection onto the eigenspace corresponding to λ_i, then these operators tell us « how likely » the outcome λ_i is if the observable A is measured in the state ψ. This can be made concrete by considering the quantities

$$p_i = \langle \Pi_i(\psi), \psi \rangle. \tag{1.1}$$

Lemma 1.2.3. *The numbers $(p_i)_{1 \leqslant i \leqslant n}$ form a probability distribution : they are non-negative numbers and sum to* 1.

Proof. First, because orthogonal projections are self-adjoint,

$$\begin{aligned} \langle \Pi_i(\psi), \psi \rangle &= \langle \Pi_i^2(\psi), \psi \rangle \\ &= \langle \Pi_i^* \Pi_i(\psi), \psi \rangle \\ &= \langle \Pi_i(\psi), \Pi_i(\psi) \rangle \\ &= \|\Pi_i(\psi)\|^2 \\ &\geqslant 0. \end{aligned}$$

Second, A being self-adjoint, it is diagonalizable, hence $\mathscr{H}$ is the orthogonal direct sum of its eigenspaces, which exactly means that

$$\sum_{i=1}^{n} \Pi_i = \mathrm{Id}_{\mathscr{H}},$$

hence

$$\begin{aligned} \sum_{i=1}^{n} p_i &= \left\langle \sum_{i=1}^{n} \Pi_i(\psi), \psi \right\rangle \\ &= \langle \psi, \psi \rangle \\ &= \|\psi\|^2 \\ &= 1. \end{aligned}$$

■

Since these numbers sum to 1, they form a probability distribution on the set of possible outcomes of the measurement. From a mathematical perspective, one can then forget about A and simply consider a family of orthogonal projections $(\Pi_i)_{i\in I}$ such that

$$\sum_{i=1}^{n} \Pi_i = \mathrm{Id}_{\mathscr{H}}.$$

Such a family describes a quantum measurement with possible outcomes $I = \{1, \cdots, n\}$, the probability of having outcome $i \in I$ being given by Equation (1.1).

Even though this is a correct and reasonable setting for quantum measurement, it turns out that we need to extend it slightly. Such an extension enables, for instance to consider, *statistical ensembles* of quantum states instead of single ones, and is in a sense the most general notion of « acting on a quantum mechanical system ». Recall that an operator T on a Hilbert space $\mathscr{H}$ is said to be *positive* if $\langle T\xi, \xi\rangle \geqslant 0$ for all $\xi \in \mathscr{H}$.

DEFINITION 1.2.4. A *Positive Operator-Valued Measure* (in short POVM) is a finite[2] family of positive operators $\mathscr{E} = (E_i)_{i\in I}$ acting on a Hilbert space $\mathscr{H}$ such that

$$\boxed{\sum_{i\in I} E_i = \mathrm{Id}_{\mathscr{H}}.}$$

Note that given a state ψ, the previous probabilistic interpretation still makes sense. We will therefore consider that if we want to measure the « observable » $\mathscr{E}$ in the state ψ, then we get outcome i with probability

$$p_i = \langle E_i(\psi), \psi\rangle \geqslant 0.$$

Let us go back to the strategy of ALICE and BOB. Assume that they have prepared the state ψ and both have at their disposal, for each $v \in V(G)$, a POVM denoted respectively by

$$\mathscr{E}_v^A = (E_{vw})_{w\in V(H)} \quad \& \quad \mathscr{E}_v^B = (F_{vw})_{w\in V(H)}.$$

Upon receiving inputs v and v' respectively, each one wants to apply its corresponding POVM to ψ and send as an answer the outcome of the measurement. But here appears a crucial issue : in quantum mechanics, making a measurement changes the system ! This is problematic because we do not know how to produce the POVM giving the result of the joint measurements of the two players : since ALICE and BOB cannot communicate, they cannot agree on who measures first, ruining the mere possibility of building a strategy.

To overcome this problem, the players will need to choose their POVMs wisely. The simplest solution, which is the one usually taken, is that we require all the operators to pairwise commute, in the sense that

$$E_{vw}F_{v'w'} = F_{v'w'}E_{vw}$$

for all $v, v' \in V(G)$ and all $w, w' \in V(H)$. Then, setting $D_{vv'ww'} = E_{vw}F_{v'w'}$ defines a family of operators satisfying all the properties of Definition 1.2.4. So here we go !

DEFINITION 1.2.5. A *perfect quantum strategy* for the graph isomorphism game consits of a Hilbert space $\mathscr{H}$ together with

- For each $v \in V(G)$, two POVMs

  $$\boxed{\mathscr{E}_v^A = \{E_{vw} \mid w \in V(H)\} \quad \& \quad \mathscr{E}_v^B = \{F_{vw} \mid w \in V(H)\}}$$

  such that $E_{vw}F_{v'w'} = F_{v'w'}E_{vw}$ for all $v, v' \in V(G)$ and $w, w' \in V(H)$.

- A vector $\psi \in \mathscr{H}$ such that

  $$\big\langle (E_{vw}F_{v'w'})\psi, \psi\big\rangle = 0$$

  if $(v, v') \nsim (w, w')$;

2. We restrict here the definition to finitely many operators for simplicity, and because this is all we need in the sequel. In general, one should consider a family of operators indexed by measureable subsets of a measure space, with natural conditions making it a « measure » with operator values.

Remark 1.2.6. In quantum information theory, there are several notions of quantum strategies, corresponding to various assumptions on the POVMs. Ours is called the *commuting operator model*, and since this is the only one we will use, we will simply call it a quantum strategy.

As one might expect, quantum strategies include classical ones. Indeed, if we have a classical probabilistic strategy given by two functions p_A and p_B, let $\mathscr{H} = \mathbf{C}$ and set

$$E_{vw}(1) = p_A(v,w).1 \quad \& \quad F_{v'w'}(1) = p_B(v',w').1.$$

For a fixed v, this defines two POVMs which commute. Moreover, the correlations associated with the vector

$$\psi = 1$$

satisfy

$$\langle E_{vw}F_{v'w'}(\psi),\psi\rangle = p_A(v,w)p_B(v',w') = \langle F_{v'w'}E_{vw}(\psi),\psi\rangle.$$

Because by THEOREM 1.2.2 the existence of a perfect classical strategy for the graph isomorphism game is the same as the graphs being isomorphic, the authors of [AMR+19] introduced the terminology *quantum isomorphic* for graphs admitting a perfect quantum strategy for the graph isomorphism game. We will, however, use that terminology for another notion below, even though we will see in THEOREM 1.5.1 that they are equivalent.

1.3 QUANTUM PERMUTATIONS

We will now take a completely different route to define a notion of quantum isomorphism between two graphs. This starts on a set-theoretic level : an isomorphism is in particular a bijection between the vertex sets of the graphs. So what would be a « quantum » version of a bijection between two finite sets? Non-commutative geometry provides the heuristic for this, by shifting the focus from points in a space to functions on that space. More explicitly, in classical physics one considers physical quantities described by functions on a space (topological, or a manifold) describing the states of the system. In quantum physics, such observable quantities get the extra feature that they should not necessarily commute with one another. This is of course impossible for scalar-valued functions, but easy to realize using *operator-valued functions*. This gives us our heuristic : find operator-valued functions which, when further assumed to all commute, boil down to usual functions on the classical space.

We will implement this idea for permutations, which is not very difficult because we are dealing with finite spaces. Let us consider, for $1 \leqslant i,j \leqslant N$, the following functions $c_{ij} : \mathfrak{S}_N \to \mathbf{C}$,

$$c_{ij}(\sigma) = \delta_{i\sigma(j)}.$$

These are easily seen to generate all scalar-valued functions on $\mathfrak{S}_N$: for a given $\sigma \in \mathfrak{S}_N$, we have

$$\delta_\sigma = \prod_{i=1}^{N} c_{\sigma(i)i}.$$

Moreover, they form a nice generating set because they all satisfy $c_{ij}^2 = c_{ij}$. The natural thing is therefore to replace each c_{ij} by a projection in a fixed Hilbert space $\mathscr{H}$. Moreover, because c_{ij} is real-valued, we will require the projections to be self-adjoint, hence orthogonal.

To go further, let us recast our functions slightly differently. Given a permutation $\sigma \in \mathfrak{S}_N$, we can associate to it a matrix P_σ whose (i,j)-th coefficient is exactly $c_{ij}(\sigma)$. The fact that σ is bijective implies that on each row and each column of P_σ, there is exactly one non-zero coefficient. Converting this into a property of the projections is a bit tricky, since the non-zero coefficient changes when the permutation changes. It is better to restate the property in terms of functions. And indeed, this is equivalent to the following equalities for all $1 \leqslant k,\ell \leqslant N$:

$$\sum_{i=1}^{N} c_{ik} = \mathbf{1} = \sum_{j=1}^{N} c_{\ell j},$$

where **1** denotes the constant function equal to 1. Any function on $\mathfrak{S}_N$ acts on the other ones by multiplication, and **1** is the identity for that action. Therefore, we will replace it by the identity of the Hilber space $\mathscr{H}$, leading us to the definition that we were looking for.

DEFINITION 1.3.1. Let $\mathscr{H}$ be a Hilbert space. A *quantum permutation (matrix)* in $\mathscr{H}$ is a matrix $P = (p_{ij})_{1\leqslant i,j\leqslant N}$ with entries in $B(\mathscr{H})$ such that :

- p_{ij} is an orthogonal projection for all $1 \leqslant i, j \leqslant N$,
- $\sum_{k=1}^{N} p_{kj} = \mathrm{Id}_{\mathscr{H}} = \sum_{k=1}^{N} p_{ik}$ for all $1 \leqslant i, j \leqslant N$.

The theory of quantum permutations is vast and mostly unexplored to this day. The survey [Web23] gives a comprehensive overview of its origins and connections to non-commutative geometry and quantum group theory, as well as many open problems. Feel free to try your hand at some of these ! Before adding graphs in the story, let us perform a sanity check. The guiding philosophy of non-commutative geometry is that we define objects involving operators, which should reduce to their usual classical counterpart when all the operators are forced to commute. Hence the question : what is a quantum permutation in which all entries commute ? The permutation matrices P_σ are of course examples. But if $N = 2$ and p is any projection in $B(\mathscr{H})$ for some Hilbert space $\mathscr{H}$, then the matrix

$$\begin{pmatrix} p & 1-p \\ 1-p & p \end{pmatrix}$$

is a quantum permutation matrix. Note however that it can be decomposed along permutations : if τ denotes the transposition in $\mathfrak{S}_2$, then

$$P = \mathrm{Id}_{\mathscr{H}} \otimes p + \tau \otimes (1-p).$$

Now, such a decomposition is the best we can do.

Proposition 1.3.2. *Let $P \in M_N(B(\mathscr{H}))$ be a quantum permutation matrix such that all the entries pairwise commute. Then, there exists projections $(p_\sigma)_{\sigma\in\mathfrak{S}_N}$ in $B(\mathscr{H})$ such that*

$$\sum_{\sigma\in\mathfrak{S}_N} p_\sigma = \mathrm{Id}_{\mathscr{H}}$$

and

$$\boxed{P = \sum_{\sigma\in\mathfrak{S}_N} P_\sigma \otimes p_\sigma.}$$

Proof. For $\sigma \in \mathfrak{S}_N$, let us set

$$p_\sigma = \prod_{i=1}^{N} p_{i\sigma(i)}.$$

Observe that

$$\begin{aligned} \mathrm{Id}_{\mathscr{H}} &= \prod_{i=1}^{N} \mathrm{Id}_{\mathscr{H}} \\ &= \prod_{i=1}^{N} \left(\sum_{j=1}^{N} p_{ij} \right) \\ &= \sum_{j_1,\cdots,j_N=1}^{N} p_{1j_1} \cdots p_{Nj_N}. \end{aligned}$$

Any term in the sum vanishes if $j_k = j_{k'}$ for some $k \neq k'$. In other words, the only non-zero terms are those where $j_k = \sigma(k)$ for some permutation $\sigma \in \mathfrak{S}_N$, hence

$$\begin{aligned} \mathrm{Id}_{\mathscr{H}} &= \sum_{\sigma\in\mathfrak{S}_N}^{N} p_{1\sigma(1)} \cdots p_{N\sigma(N)} \\ &= \sum_{\sigma\in\mathfrak{S}_N}^{N} p_\sigma. \end{aligned}$$

As a consequence, for any $1 \leqslant i, j \leqslant N$,

$$p_{ij} = p_{ij}\left(\sum_{\sigma\in\mathfrak{S}_N}^{N} p_\sigma\right)$$

But in p_σ appears the projection $p_{i\sigma(i)}$ whose product with p_{ij} vanishes unless $j = \sigma(i)$. Therefore,

$$p_{ij} = \sum_{\sigma\in\mathfrak{S}_N} \delta_{j\sigma(i)} p_\sigma$$

and this is precisely the (i,j)-th entry of the operator-valued matrix in the statement. ■

Now that we have a notion of quantum permutation, we can go further to quantum graph isomorphism. To do this, let us fix two graphs G and H. Assuming that $V(H)$ and $V(G)$ have cardinality N, we can see any isomorphism as a bijection $\sigma \in \mathfrak{S}_N$. To express the fact that it respects edges, we will use the matrix picture. Indeed, any graph can be encoded in its *adjacency matrix*. This is the matrix A_G indexed by $V(G) \times V(G)$, where

$$(A_G)_{vv'} = \begin{cases} 1 & \text{if } (v,v') \in E(G) \\ 0 & \text{otherwise} \end{cases}$$

Note that because the graph is undirected, this is a symmetric matrix. We now claim that σ being a graph isomorphism has a simple expression in terms of the adjacency matrices.

Lemma 1.3.3. *With the previous notations, σ is a graph isomorphism if and only if*

$$\boxed{P_\sigma A_G = A_H P_\sigma}$$

Proof. Choose orderings $V(G) = \{v_1, \cdots, v_N\}$ and $V(H) = \{w_1, \cdots, w_N\}$ to write the adjacency matrices. Then, the (i,j)-th coefficient of $P_\sigma A_G$ is

$$\sum_{k=1}^{N} (P_\sigma)_{ik} (A_G)_{v_k v_j} = (A_G)_{v_{\sigma^{-1}(i)} v_j}$$

while the corresponding coefficient of $A_H P_\sigma$ is

$$\sum_{k=1}^{N} (A_H)_{v_i v_k} (P_\sigma)_{kj} = (A_H)_{v_i v_{\sigma(j)}}.$$

These two numbers are equal if and only if $(A_G)_{v_{\sigma^{-1}(i)} v_j} = (A_H)_{v_i v_{\sigma(j)}}$. Therefore, the two matrices are equal if and only if for all $1 \leqslant i, j \leqslant N$,

$$(A_G)_{v_i v_j} = (A_H)_{v_{\sigma(i)} v_{\sigma(j)}},$$

i.e. if $(v_{\sigma(i)}, v_{\sigma(j)})$ is an edge if and only if (v_i, v_j) is. ■

The condition above also makes sense with a quantum permutation matrix, leading to the definition we are after. Let us nevertheless first clarify a subtle point. We have assumed here that $V(G)$ and $V(H)$ have the same cardinality, but the notion of a quantum permutation can make sense for rectangular matrices. And in principle, why should the mysteries of quantum physics not allow for different sizes? As it turns out, the existence of a quantum permutation forces equality of the sizes of the vertex sets.

Lemma 1.3.4. *Let G and H be two graphs and let $P = (p_{wv})_{w\in V(H), v\in V(G)}$ be a quantum permutation matrix. Then, $|V(G)| = |V(H)|$.*

Proof. This follows from a simple double-counting argument :

$$\begin{aligned}|V(H)|\,\mathrm{Id}_{\mathscr{H}} &= \sum_{w\in V(H)} \mathrm{Id}_{\mathscr{H}} \\ &= \sum_{w\in V(H)}\sum_{v\in V(G)} p_{wv} \\ &= \sum_{v\in V(G)}\sum_{w\in V(H)} p_{wv} \\ &= \sum_{v\in V(G)} \mathrm{Id}_{\mathscr{H}} \\ &= |V(G)|\,\mathrm{Id}_{\mathscr{H}}\end{aligned}$$

and the result follows. ∎

Let us now give the (too) long-awaited definition.

DEFINITION 1.3.5. A *quantum isomorphism* between two graphs G and H on N vertices is a quantum permutation matrix P such that

$$\boxed{PA_G = A_H P}$$

If such a quantum isomorphism exists, then the graphs are said to be *quantum isomorphic*. If $G = H$, then P is called a *quantum automorphism*.

Remark 1.3.6. Of course, any isomorphism f in the usual sense between G and H gives rise to a quantum isomorphism by setting $\mathscr{H} = \mathbf{C}$ and $p_{wv} = \delta_{f(v)w}$.

The condition $PA_G = A_H P$ is a concise way of stating $|V(G)| \times |V(H)|$ equations, but it can be useful to spell them out for concrete computations. Let us set $v \sim v'$ if the two vertices v and v' are *adjacent* in a graph, i.e. connected by an edge. Then, a quantum permutation P is a quantum isomorphism from G to H if and only if for any $v \in V(G)$ and $w \in V(H)$,

$$\sum_{v'\sim v} p_{wv'} = \sum_{w'\sim w} p_{w'v}.$$

As we will see in THEOREM 1.5.1, the notion of quantum isomorphism that we just introduced is equivalent to the one coming from the graph isomorphism game. Therefore, depending on the problem – and on personal tastes – one can shift from one picture to the other to get the best out of each. As an illustration, we will give below a few properties of quantum isomorphism. We start with a useful criterion to check whether a quantum permutation is a quantum graph isomorphism.

Proposition 1.3.7. *Let G and H be graphs and let $P = (p_{w,v})_{w\in V(H),v\in V(G)}$ be a quantum permutation. Then, P is a quantum isomorphism if and only if for all $(v,v') \in E(G)$ and $(w,w') \notin E(H)$, or $(v,v') \notin E(G)$ and $(w,w') \in E(H)$,*

$$p_{wv}p_{w'v'} = 0.$$

Proof. Assume first that p is a quantum isomorphism, let $(v,v') \in E(G)$ and $(w,w') \notin E(H)$ (the other case is treated in the same way, *mutatis mutandis*). We have

$$\begin{aligned}p_{wv}\left(\sum_{v''\sim v'} p_{wv''}\right)p_{w'v'} &= p_{wv}\left(\sum_{w''\sim w} p_{w''v'}\right)p_{w'v'} \\ &= p_{wv}\left(\sum_{w''\sim w} p_{w''v'}p_{w'v'}\right).\end{aligned}$$

Because $w' \nsim w$, every vertex $w'' \sim w$ satisfies $w'' \neq w'$. Hence, since projections lying in the same column are orthogonal, $p_{w''v'}p_{w'v'} = 0$ for every summand so that the right-hand side vanishes when $w' \nsim w$. But since $v' \sim v$, we have

$$\begin{aligned}p_{wv}p_{w'v'} &= \left(\sum_{v''\sim v'} p_{wv}p_{wv''}\right)p_{w'v'} \\ &= p_{wv}\left(\sum_{v''\sim v'} p_{wv''}\right)p_{w'v'}\end{aligned}$$

hence the result.

Assuming now that the condition in the statement holds, fix $v \in V(G)$ and $w \in V(H)$. Then,

$$\begin{aligned}\sum_{v' \sim v} p_{wv'} &= \left(\sum_{v' \sim v} p_{wv'}\right)\left(\sum_{w' \in V(H)} p_{w'v}\right)\\ &= \sum_{v' \sim v} \sum_{w' \in V(H)} p_{wv'} p_{w'v}\\ &= \sum_{v' \sim v} \sum_{w' \sim w} p_{wv'} p_{w'v}\\ &= \sum_{w' \sim w} \sum_{v' \sim v} p_{wv'} p_{w'v}\\ &= \left(\sum v' \in V(G) p_{wv'}\right)\left(\sum_{w' \sim w} p_{w'v}\right)\\ &= \sum_{w' \sim w} p_{w'v},\end{aligned}$$

so that P is indeed a quantum isomorphism. ■

This criterion often simplifies proofs by avoiding the computation of big matrix products. As an example, we will show that, as the name suggests, quantum isomorphism is a well-defined equivalence relation on graphs.

Proposition 1.3.8. *Quantum isomorphism is an equivalence relation on graphs.*

Proof. First, the identity map is a quantum isomorphism from any graph to itself, hence the relation is reflexive. Moreover, let P be a quantum isomorphism from G to H. Then, the matrix P^* with coefficients $(P^*)_{ij} = p_{ji}$ is still a quantum permutation matrix. Moreover,

$$\begin{aligned}P^* A_G &= (A_G P)^*\\ &= (P A_H)^*\\ &= A_H P^*,\end{aligned}$$

hence P^* is a quantum isomorphism from H to G, so that the relation is symmetric.

We are left with proving transitivity. Let G, H and K be graphs and let $P = (p_{wv})_{w \in V(H), v \in V(G)}$ and $Q = (q_{zw})_{z \in V(K), w \in V(H)}$ be quantum isomorphisms respectively from G to H and from H to K. The operators act on some Hilbert spaces $\mathscr{H}_1$ and $\mathscr{H}_2$ respectively, and we will use the tensor product Hilbert space $\mathscr{H}_3 = \mathscr{H}_1 \otimes \mathscr{H}_2$. We set

$$r_{zv} = \sum_{w \in V(H)} q_{zw} \otimes p_{wv} \in B(\mathscr{H}_3)$$

and claim that the matrix $R = (r_{zv})_{z \in V(K), v \in V(G)}$ is a quantum isomorphism from G to K. Note that apart from the tensor product in the middle, this is the formula for matrix multiplication. However, if we had written a genuine matrix multiplication, the resulting entries would not be projections (a product of projections which do not commute is not a projection). This is therefore a slight modification that at least has some chance to produce a quantum permutation.

Let us first check that r_{zv} is an orthogonal projection for all $z \in V(K)$ and $v \in V(G)$. Self-adjointness follows from the fact that $(S \otimes T)^* = S^* \otimes T^*$ for any bounded operators S and T, while the idempotency is given by an elementary computation :

$$\begin{aligned}r_{zv}^2 &= \left(\sum_{w \in V(H)} q_{zw} \otimes p_{wv}\right)\\ &= \sum_{w, w' \in V(H)} q_{zw} q_{zw'} \otimes p_{wv} p_{w'v}\\ &= \sum_{w \in V(H)} q_{zw} q_{zw} \otimes p_{wv} p_{wv}\\ &= \sum_{w \in V(H)} q_{zw} \otimes p_{wv}\\ &= r_{zv}.\end{aligned}$$

Moreover, for any $v \in V(G)$.

$$\begin{aligned}\sum_{z\in V(K)} r_{zv} &= \sum_{z\in V(K)}\sum_{w\in V(H)} q_{zw}\otimes p_{wv}\\ &= \sum_{w\in V(H)}\sum_{z\in V(K)} q_{zw}\otimes p_{wv}\\ &= \sum_{w\in V(H)}\left(\sum_{z\in V(K)} q_{zw}\right)\otimes p_{wv}\\ &= \sum_{w\in V(H)} \mathrm{Id}_{\mathscr{H}_1}\otimes p_{wv}\\ &= \mathrm{Id}_{\mathscr{H}_1}\otimes \mathrm{Id}_{\mathscr{H}_2}\\ &= \mathrm{Id}_{\mathscr{H}_3}.\end{aligned}$$

The same argument works *mutatis mutandis* for the sum over rows, showing that R is a quantum permutation.

To prove that R is a quantum isomorphism, we will use the criterion of **Proposition** 1.3.7. Let therefore $(z,z') \in E(K)$ and $(v,v') \notin E(G)$. Then,

$$\begin{aligned}r_{zv}r_{z'v'} &= \left(\sum_{w\in V(H)} q_{zw}\otimes p_{wv}\right)\left(\sum_{w'\in V(H)} q_{z'w'}\otimes p_{w'v'}\right)\\ &= \sum_{w,w'\in V(H)} q_{zw}q_{z'w'}\otimes p_{wv}p_{w'v'}.\end{aligned}$$

Because $z \sim z'$, $q_{zw}q_{z'w'}$ unless $w \sim w'$. But then, $p_{wv}p_{w'v'} = 0$ so that in the end one of the two tensor factors always vanishes. The case $(z,z') \notin E(K)$ and $(v,v') \in E(G)$ is done similarly, hence the result. ■

It is a natural and difficult problem to understand which properties and which invariants of a graph are preserved under quantum isomorphism. On the one hand, there are results showing that connectivity and some « tree-like » structures are preserved (see for instance [DdBvNKR+25] [Meu26], [FMP25] and [DdBvFNK+25]), while invariants like the chromatic, clique or independence numbers are not, as we will see in the next lecture (see **Proposition 2.3.3**). These problems are not the focus of these notes, hence we will not elaborate more on them now. We will nevertheless give one elementary result, because it is needed in the very end of this text. The *complement* of a graph G is the graph G^c with vertex set $V(G)$ and with an edge between two distinct vertices v and w if and only if $(v,w) \notin E(G)$.

Lemma 1.3.9. *Two graphs G and H are quantum isomorphic if and only if their complements are quantum isomorphic.*

Proof. Because $(G^c)^c = G$, it is enough to prove that if G and H are quantum isomorphic, then their complements are. Let therefore P be a quantum isomorphism, so that $PA_G = A_HP$. The adjacency matrix of the complement is

$$A_{G^c} = J_{V(G)} - I_{V(G)} - A_G,$$

where $I_{V(G)}$ is the identity matrix acting on $\mathbf{C}^{V(G)}$ and $J_{V(G)}$ is the all-ones matrix. Noting that $PJ_{V(G)} = J_{V(H)}P$ and $PI_{V(G)} = I_{V(H)}P$ then yields the result. ■

1.4 COUNTING HOMORPHISMS

We now turn to a very different approach to graph isomorphism, which is purely combinatorial. The starting point is a simple observation : if $f : V(G) \to V(H)$ is a graph isomorphism, then for any other graph K, the map

$$\Phi_f : \left\{\begin{array}{ccc}\mathrm{Hom}(K,G) & \to & \mathrm{Hom}(K,H)\\ g & \mapsto & f\circ g\end{array}\right.$$

induces a bijection. Therefore, we have the equality of *homomorphism counts*

$$|\mathrm{Hom}(K,G)| = |\mathrm{Hom}(K,H)|. \tag{1.2}$$

One may therefore wonder how much information Equation (1.2) contains on the relationship between G and H. Let us start with the extreme case : if the homomorphism counts are equal for all graphs, what can we say? Somewhat surprisingly, we can completely recover the relation between G and H. This is a seminal result by L. LOVÀSZ from [Lov67].

THEOREM 1.4.1 (LOVÀSZ) Let G and H be graphs, and assume that for any graph K,

$$|\mathrm{Hom}(K,G)| = |\mathrm{Hom}(K,H)|.$$

Then, G and H are isomorphic.

For the sake of exposition, we will split the proof and first establish a useful technical fact. Specifically, we need a canonical way of decomposing graph homomorphisms using a surjective one and an injective one. This is somewhat similar to the standard decomposition results for morphisms of algebraic structures like groups or rings. Making this precise requires some notations, which we now introduce. Recall that a partition $\mathscr{P}$ of a set X is the same as an equivalence relation $\sim_{\mathscr{P}}$ on X. Given a partition on a graph, we can naturally produce a new graph.

DEFINITION 1.4.2 (GRAPH ASSOCIATED TO A PARTITION). Let K be a graph and let $\mathscr{P}$ be a partition of $V(K)$. We associate with $\mathscr{P}$ the graph $K_{\mathscr{P}}$ whose vertices are the blocks of the partition as follows :

$$V(K_{\mathscr{P}}) = \mathscr{P}$$
$$E(K_{\mathscr{P}}) = \{(P,P') \mid (v,v') \in E(K) \text{ for some } v \in P \text{ and } v' \in P'\}.$$

That graph may be viewed as a quotient of the original one, and the next result makes it more precise.

Lemma 1.4.3. *Let K be a graph and let $\mathscr{P}$ be a partition of $V(K)$. Then, the map $\phi_{\mathscr{P}} : V(K) \to V(K_{\mathscr{P}})$ sending v to the unique $P \in \mathscr{P}$ such that $v \in P$ is a surjective graph homomorphism.*

Proof. Observe that $\phi_{\mathscr{P}}$ is surjective by definition of a partition, so that we simply have to prove that it respects edges. Let therefore $(v,v') \in E(K)$ and let $P,P' \in \mathscr{P}$ be such that $v \in P$ and $v' \in P'$. Then, by definition $(P,P') \in E(K_{\mathscr{P}})$, hence the result. ■

With that construction of « quotient graph », we can state and prove our decomposition result for homomorphisms.

Proposition 1.4.4 (CANONICAL DECOMPOSITION OF GRAPH HOMOMORPHISMS)**.** *Let K and G be graphs, and let $f : K \to G$ be a graph homomorphism. Then, there exists a unique partition $\mathscr{P}$ of $V(K)$, and a unique* injective homomorphism $\widetilde{f} : K_{\mathscr{P}} \to G$ *such that*

$$\boxed{f = \widetilde{f} \circ \phi_{\mathscr{P}}}$$

Proof. Let $\mathscr{P} = \mathscr{P}_f$ be the partition given by the subsets $f^{-1}(w)$ for $w \in V(G)$. Since f is constant on any $P \in \mathscr{P}$ by definition, we can define $\widetilde{f}(P)$ to be that constant value, yielding a map

$$\widetilde{f} : V(K_{\mathscr{P}}) \to V(G),$$

which is injective since distinct blocks have by definition distinct images under f and satisfies $\widetilde{f} \circ \phi_{\mathscr{P}} = f$. We therefore simply have to check that $\widetilde{f}$ is a graph homomorphism. Let (P,P') be an edge in $K_{\mathscr{P}}$. This means that there exist $v \in P$ and $v' \in P'$ such that $(v,v') \in E(K)$. But then,

$$(\widetilde{f}(P), \widetilde{f}(P')) = (f(v), f(v')) \in E(G).$$

We now turn to uniqueness. Assume that $f = g \circ \phi_{\mathscr{P}}$ for some injective homomorphism g and partition $\mathscr{P}$. If $f(v) = f(v')$, then by injectivity of g we must have $\phi_{\mathscr{P}}(v) = \phi_{\mathscr{P}}(v')$, hence $v \sim_{\mathscr{P}} v'$. The converse is of course true, proving that $\mathscr{P} = \mathscr{P}_f$. Therefore, for $P \in \mathscr{P}$ and $v \in P$, we have $g(P) = f(v)$ so that $g = \widetilde{f}$ and the proof is complete. ■

With this in hand, we can prove the announced result.

Proof of THEOREM 1.4.1. The key idea is to prove that the equality also holds when one restricts to injective homomorphisms. We will prove that second fact by induction on the number of vertices of K, using the following induction hypothesis where Inj denotes the set of injective homomorphisms :

$$H_k : \text{« For any graph } K \text{ on } k \text{ vertices, } |\mathrm{Inj}(K,G)| = |\mathrm{Inj}(K,H)|. \text{ »}$$

▷ **Initialisation :** for $k = 1$, the only possible graph K has just one vertex and no edge and any homomorphism from this is clearly injective, hence H_1.

▷ **Induction Step :** Assume that H_n holds for all $1 \leqslant n \leqslant k$ and consider a graph K with $k+1$ vertices. By THEOREM 1.4.4, we have a disjoint union decomposition

$$\mathrm{Hom}(K,G) = \coprod_{\mathscr{P} \in \mathscr{P}(V(K))} \mathrm{Inj}(K_{\mathscr{P}}, G),$$

which yields the equality

$$|\mathrm{Hom}(K,G)| = \sum_{\mathscr{P} \in \mathscr{P}(V(K))} |\mathrm{Inj}(K_{\mathscr{P}}, G)|.$$

To conclude, note that as soon as $\mathscr{P}$ is not the partition $\mathscr{P}_s$ into singletons, the graph $K_{\mathscr{P}}$ has at most k vertices. Therefore, by the induction hypothesis H_k,

$$\begin{aligned} |\mathrm{Hom}(K,G)| &= \sum_{\mathscr{P} \in \mathscr{P}(V(K))} |\mathrm{Inj}(K_{\mathscr{P}}, G)| \\ &= |\mathrm{Inj}(K,G)| + \sum_{\mathscr{P} \neq \mathscr{P}_s} |\mathrm{Inj}(K_{\mathscr{P}}, G)| \\ &= |\mathrm{Inj}(K,G)| + \sum_{\mathscr{P} \neq \mathscr{P}_s} |\mathrm{Inj}(K_{\mathscr{P}}, H)| \end{aligned}$$

Similarly,

$$\begin{aligned} |\mathrm{Hom}(K,H)| &= \sum_{\mathscr{P} \in \mathscr{P}(V(K))} |\mathrm{Inj}(K_{\mathscr{P}}, H)| \\ &= |\mathrm{Inj}(K,H)| + \sum_{\mathscr{P} \neq \mathscr{P}_s} |\mathrm{Inj}(K_{\mathscr{P}}, H)| \end{aligned}$$

Comparing the two expressions then yields $|\mathrm{Inj}(K,G)| = |\mathrm{Inj}(K,H)|$, hence H_{k+1}.

As a consequence, using $K = G$, we have $|\mathrm{Inj}(G,G)| = |\mathrm{Inj}(G,H)|$ so that there exists an injective homomorphism $f : V(G) \to V(H)$ since there is one (the identity) from G to G. Similarly, there is an injective homomorphism $f' : V(H) \to V(G)$ and we claim that f and f' are isomorphisms. By finiteness, f is a bijection, so that what is left is proving that it induces a bijection on edges. To prove that, consider the function

$$f^{(2)} : V(G) \times V(G) \to V(H) \times V(H)$$

sending (v,v') to $(f(v),f(v'))$. It is again injective, and because it is a graph homomorphism we have $f^{(2)}(E(G)) \subset E(H)$ because it preserves adjacency, so that $|E(G)| \leqslant |E(H)|$. By the same argument using this time $f'^{(2)}$, we also have $|E(H)| \leqslant |E(G)|$ so that in the end the two sets have equal cardinality. Consequently, $f^{(2)}(E(G)) = E(H)$ and same for f', which is exactly what we wanted. ■

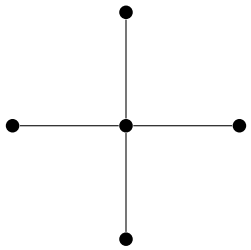
A natural interpretation of that result is that if $\mathscr{F}$ is a family of graphs, then having the same number of homomorphisms from every graph in $\mathscr{F}$ defines a weak notion of isomorphism between two graphs. Let us give it a name for convenience.

DEFINITION 1.4.5. Two graphs G and H are said to be *$\mathscr{F}$-isomorphic* if for every graph $K \in \mathscr{F}$,

$$|\mathrm{Hom}(K,G)| = |\mathrm{Hom}(K,H)|.$$

Let us give two examples.

Example 1.4.6 (STAR GRAPHS)**.** The *star graph* S_k is the graph on $k+1$ vertices where one vertex is connected to all the other vertices. Here is an illustration with $k = 4$.



A homomorphism from S_k to a graph G is equivalent to the choice of a vertex in G together with an ordered k-uple of its neighbours, possibly with repetitions. Therefore,

$$|\mathrm{Hom}(S_k,G)| = \sum_{v \in V(G)} \deg(v)^k.$$

We claim that if $\mathscr{S}$ is the set of all star graphs, then G and H are $\mathscr{S}$-isomorphic if and only if they have the same *degree sequence*. To see why, let $n_k(G)$ denote the number of vertices of degree k in G, let $n(G) \in \mathbf{C}^{\delta(G)}$ be the corresponding vector andlet $\delta(G)$ be the maximum degree of a vertex in G. Then,

$$|\mathrm{Hom}(S_k,G)| = \sum_{i=0}^{\delta(G)} n_i(G) i^k.$$

Let us first show that the maximum degrees of both graphs agree. By equality of the homomorphism counts, we have for all $k \in \mathbf{N}$,

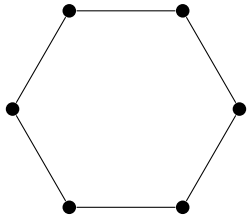
$$\begin{aligned}\frac{1}{\delta(G)^k} \sum_{i=0}^{\delta(H)} n_i(H) i^k &= \frac{1}{\delta(G)^k} |\mathrm{Hom}(S_k,G)| \\ &= \frac{1}{\delta(G)^k} |\mathrm{Hom}(S_k,H)| \\ &= \sum_{i=0}^{\delta(G)} n_i(G) \left(\frac{i}{\delta(G)}\right)^k.\end{aligned}$$

The right-hand side converges to $n_{\delta(G)}$ as $k \to +\infty$, hence the left-hand side does the same, which means that $\delta(H) = \delta(G)$. Now, setting for $1 \leqslant i,k \leqslant \delta(G)$

$$a_{ki} = i^k$$

produces a matrix $A \in M_{\delta(G)}(\mathbf{C})$ such that $An(G) = An(H)$. But A is an invertible Vandermonde matrix, hence $n(G) = n(H)$, as claimed.

Example 1.4.7 (CYCLE GRAPH)**.** The *cycle graph* C_k is the graph with vertices $\{1,\cdots,k\}$ and edges $(i, i+1 \mod k)$ for $1 \leqslant i \leqslant k$. Here is an illustration with $k = 6$.



A homomorphism from C_k to G is given by a closed path $v_1 \cdots v_k v_1$, meaning that $v_i \sim v_{i+1}$ and $v_k \sim v_1$. A standard computation shows that the number of closed paths of length k from v to v' in a graph G is $(A_G^k)_{vv'}$, so that

$$|\mathrm{Hom}(C_k, G)| = \sum_{v \in V(G)} (A_G^k)_{vv} = \mathrm{Tr}\left(A_G^k\right).$$

Since A_G is symmetric, it is diagonalizable. Writing $\mathrm{Sp}(A_G) = \{\lambda_1, \cdots, \lambda_m\}$ and denoting by μ_i the multiplicity of λ_i, we have

$$|\mathrm{Hom}(C_k, G)| = \sum_{i=1}^{m} \mu_i \lambda_i^k.$$

If $\mathscr{C}$ is the set of all cycle graphs and if two graphs G and H are $\mathscr{C}$-isomorphic, then these sums are equal for all k. Consider now the characteristic polynomials χ_{A_G} and χ_{A_H}. The previous equality means that the sum of the k-th power of their roots are equal for all k. But the coefficients of a polynomial are themselves polynomials in sums of powers of their roots (these are *symmetric polynomials*). Therefore, $\chi_{A(G)} = \chi_{A(H)}$. Such graphs are called *cospectral* : the combinatorics of homomorphism counts meets spectral graph theory !

One of the most important classes of graphs are the *planar* ones. Let us recall the definition.

DEFINITION 1.4.8. A graph is *planar* if it can be drawn in the plane in such a way that the edges do not cross except possibly at the vertices. If $\mathscr{F}$ is the set of all planar graphs, then two graphs are said to be *planar isomorphic* if they are $\mathscr{F}$-isomorphic.

For instance, the complete graph K_4 is planar, as the picture below shows. Meanwhile, the complete graph K_5 is not planar, even though proving it requires some basic results from combinatorial graph theory[3]. Planar graphs form a rich and extensively studied class. It is therefore natural to wonder how much information the homomorphism counts from planar graphs encapsulate. This is a question which was already asked in [Lov67] and we now explicitly state it.

Question 1.4.9. How can one characterize planar isomorphism ? Does it imply isomorphism ?

The question remained open for fifty years, until quantum isomorphism appeared and led to a surprising answer which is the topic of the next section.

1.5 THE FUNDAMENTAL THEOREM

It is now time to bring together all our definitions of generalized isomorphism and see that they are in fact equivalent. The following result is a combination of [AMR+19, Thm 5.8], [LMR20, Thm 4.4] and [MR20].

> **THEOREM 1.5.1** (THE FUNDAMENTAL THEOREM) For two graphs G and H, the following are equivalent :
>
> 1. There is a perfect quantum strategy for the graph isomorphism game ;
> 2. G and H are quantum isomorphic ;
> 3. The graphs G and H are planar isomorphic.

The proof of THEOREM 1.5.1 is long and involved. Parts of it use operator theory, while others involve the theory of compact quantum groups. The main goal of the next two lectures will be to explain as much of the proof as we can, while avoiding the development of too much additional abstract theory. Before doing that, we will comment on some consequences of the statement.

The first question that arises is : do there exist graphs which are quantum isomorphic but not isomorphic ? To see why such beasts do exist, let us first think algorithmically. Consider the problem of deciding whether two graphs are isomorphic. One can obviously devise an algorithm which takes two graphs as input and outputs `true` if they are isomorphic and `false` otherwise, for instance by proceeding as follows :

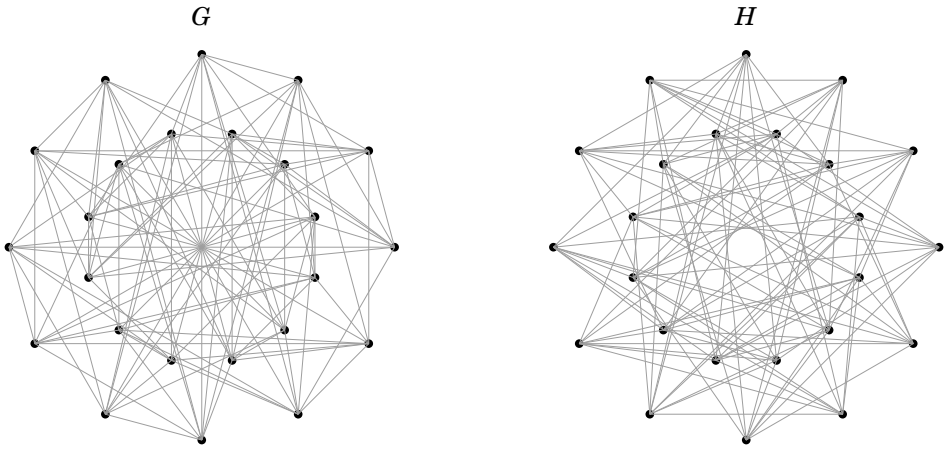
3. This is for instance a direct consequence of EULER'S FORMULA.

1. Compute the number of vertices of each graph ;
2. If they are different ⟶ `false` ;
3. Otherwise, let N be the common number of vertices and list all elements of $\mathfrak{S}_N$. Then,
   - For each $\sigma \in \mathfrak{S}_N$ do
     - For each edge of G, check whether its image under σ is an edge of H ;
     - If this works for all edges ⟶ `true` ;
     - Otherwise, go to the next permutation.
   - If no permutation works ⟶ `false`.

This is a brute-force algorithm with factorial (in N) complexity, hence not of much use in practice. Its interest is rather theoretical : in the vocabulary of computability theory, one says that the graph isomorphism problem is *decidable*. In contrast, it can be shown (see [AMR+19, Cor 6.9]) that quantum graph isomorphism is *undecidable*[4], which means that there is no program taking as input two arbitrary graphs and deciding whether they are quantum isomorphic or not. This has two important consequences :

- There must exist graphs which are quantum isomorphic but not isomorphic ;
- Proving that graphs are quantum isomorphic when they are not isomorphic is in general difficult.

Even though it is not straightforward to produce a pair of graphs which are quantum isomorphic but not isomorphic, this can be done explicitly as we will see in detail in the next lecture. The example that we will give involves two graphs with 24 vertices, and is the smallest known to this day. Here is an illustration :



It might nevertheless be possible that there are smaller ones, and the following question is still an open problem at the time of this writing.

Question 1.5.2. What is the smallest possible example of a pair of graphs which are quantum isomorphic but not isomorphic ?

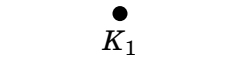
Remark 1.5.3. It was observed in the proof of [Meu26, Thm B.2] that such examples must have at least 6 vertices, and heuristic evidence suggest that the size should be at least 13.

Let us conclude with a problem related to another important topic in graph theory : *(vertex) colouring*. This means associating to each vertex of a graph an element of a fixed set C, called the *set of colours*, in such a way that two vertices which are connected by an edge are given distinct colours. The first step to study such a problem is to make it more formal, and that is done through a definition.

4. This only holds with our definition of a perfect quantum strategy.

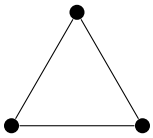
DEFINITION 1.5.4. For an integer n, the *complete graph* on n vertices is the graph K_C with vertex set $\{1,\cdots,n\}$ and edge set $\{(k,k') \in |\ k \neq k'\}$. In other words, every pari of distinct vertices is connected by an edge, hence the name.

The complete graphs on at most five vertices are shown below :

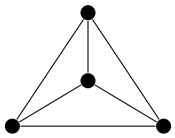


K_1

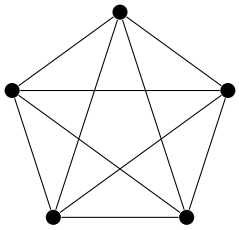
K_2



K_3



K_4



K_5

Consider now a colouring of a graph G, whose colour set can be relabelled to be $\{1,\cdots,n\}$ with $n = |C|$. Consider the map $c : V(G) \to K_n$ sending a vertex to its colour. Then, if $(v,v') \in E(G)$, $c(v) \neq c(v')$, hence $(c(v),c(v')) \in E(K_n)$. In other words, c is a graph homomorphism. Conversely, any graph homomorphism from G to K_n gives a colouring using n colours. Let us state this formally.

DEFINITION 1.5.5. An n-colouring of a graph G is a graph homomorphism $c : G \to K_n$.

The question is now, given a graph G, to find a colouring involving the smallest possible number of colours. That number is called the *chromatic number* of G and is denoted by $\chi(G)$. The problem first arose for a specific class of graphs. In fact, it started with an « experimental » observation that given a map of England (in the usual sense of the word), it was possible to colour each county in such a way that adjacent counties have different colours – in order to keep the map readable – using only four colours. It can be shown that colouring such a map is equivalent to colouring a specific *planar graph* obtained by a duality construction, therefore leading to the following question : is every planar graph 4-colourable ? Since $K_4$is planar, as illustrated above, is planar, one needs at lleast four colours to colour all planar graphs.

This famous *four-colour problem*, first publicly stated in 1854, attracted a lot of attention because of its elementary formulation, but resisted (despite several tentative proofs containing subtle issues) for more than a century. It was eventually proven that the answer is « yes » by K. APPEL and W. HAKEN in 1976 (see [AH77]). Their proof was later refined and checked by a formal theorem prover [Gon08]. Still, it relies partly on the automated verification of a number

of exceptional cases which a human cannot check by hand. Therefore, it is still considered an interesting problem to find a more understandable – or, some would say, more *human* – proof of the four-colour theorem. This is where quantum isomorphism enters the picture ! Indeed, consider the following problem :

Question 1.5.6. Can we build two graphs G and H satisfying the following properties :

- There are graph homomorphisms $f : K_4 \to G$ and $g : G \to K_4$ (in particular, G is four-colourable) ;
- The graph H is not four-colourable ;
- G and H are quantum isomorphic.

Assume that such a pair has been constructed. Then, the statement « Every planar graph has a homomorphism to H » implies the statement « Every planar graph has a homomorphism to K_4 ». At first sight, this does not help, except that the first statement is in principle easier to prove, because of the following observations :

- Any graph having a homomorphism to K_4 has a homomorphism to H ;
- Not every graph having a homomorphism to H has a homomorphism to K_4.

Indeed, since there is a homomorphism from K_4 – which is planar – to G, hence there is also a homomorphism from K_4 to H by THEOREM 1.5.1. As for the second point, H has a homomorphism to itself (the identity) but no homomorphism to K_4 since it is not four-colourable. We will give in Section 2.3.1 an explicit example of such a pair of graphs.

LECTURE 2

PERFECT ISN'T EASY

In this lecture, we focus on perfect quantum strategies and their connection to quantum graph isomorphisms. First, we investigate the connection between perfect quantum strategies and quantum isomorphisms, in order to prove the equivalence between the first two points of THEOREM 1.5.1. As we will see however, there is a catch. The quantum permutation that we produce out of a perfect quantum strategy has an extra feature, namely the existence of a *tracial positive linear map*, which is essential for proving the reverse implication. This is a subtle analytic aspect of the problem which is beyond the scope of these notes. We will therefore prove a slightly weaker statement in Corollary 2.1.6, and then comment on it.

Second, we will construct explicit examples of pairs of graphs which are quantum isomorphic but not isomorphic. Interestingly, the proof relies on solving systems of equations over the field $\mathbf{F}_2$ with two elements using operators in Hilbert spaces. We will in fact give a general recipe to produce such systems and the associated examples in great generality.

2.1 GRAPHS, GAMES AND THE QUANTUM

In this section, we will see how perfect quantum strategies enable us to construct quantum isomorphisms. As we will mention, resolving this issue much more advanced material from the theory of *compact quantum groups* which goes beyond the scope of these notes.

2.1.1 FROM GAMES TO QUANTUM

As already mentioned, the proof of THEOREM 1.5.1 is involved and uses techniques from various fields. For a start, we will focus on the equivalence between perfect quantum strategies and quantum isomorphisms. As it turns out, there is one subtle point which goes beyond the scope of these lectures. To understand why, we will first prove a slightly different statement than the one we want, which comes from [AMR+19]. The proof, though rather elementary, will use a small amount of techniques from operator algebras, which we will introduce separately for the sake of clarity. One key ingredient is about the linear form on $B(\mathscr{H})$ given by the formula

$$\phi_\psi : T \mapsto \langle T\psi, \psi\rangle.$$

The property of that map which will prove crucial is called *positivity* : for any $T \in B(\mathscr{H})$, $\phi_\psi(T^*T) = \|T\psi\|^2 \geqslant 0$. In other words, it sends positive operators (recall that an operator A on $B(\mathscr{H})$ is positive if and only if it is of the form $A = T^*T$) to positive real numbers. Such linear forms are said to be *positive* and automatically enjoy some useful properties, of which we will need two.

Lemma 2.1.1. *Let $\phi : B(\mathscr{H}) \to \mathbf{C}$ be a positive linear form. Then, for any $S, T \in B(\mathscr{H})$,*

$$\boxed{\phi(S^*T)^2 \leqslant \phi(S^*S)\phi(T^*T)}$$

Moreover, ϕ is bounded with norm $\|\phi\| = \phi(\mathrm{Id}_{\mathscr{H}})$.

Proof. For the first point, simply note that $(S,T) \mapsto \phi(S^*T)$ is a sesquilinear positive form, so that the Cauchy-Schwarz inequality applies. As for the second one, let us first prove that for any self-adjoint operator $T \in B(\mathscr{H})$, the operator $\|T\|\operatorname{Id}_{\mathscr{H}} - T$ and $T + \|T\|\operatorname{Id}_{\mathscr{H}}$ are positive. Indeed, by definition of the operator norm, we have for any $\xi \in \mathscr{H}$ that

$$\begin{aligned} |\langle T\xi, \xi\rangle| &\leqslant \|T\|\|\xi\|^2 \\ &= \langle \|T\|\operatorname{Id}_{\mathscr{H}}\xi, \xi\rangle \end{aligned}$$

Therefore, since ϕ sends positive operators to positive real numbers, we have

$$-\|T\|\phi(\operatorname{Id}_{\mathscr{H}}) \leqslant \big|\phi(T)\big| \leqslant \|T\|\phi(\operatorname{Id}_{\mathscr{H}}),$$

so that $|\phi(T)| \leqslant \|T\|\phi(\operatorname{Id}_{\mathscr{H}})$. If now T is an arbitrary operator, we set

$$S_1 = \frac{T+T^*}{2} \quad \& \quad S_2 = \frac{T-T^*}{2i}.$$

These are self-adjoint, and $T = S_1 + iS_2$. Moreover,

$$T^*T = S_1S_1 + iS_1S_2 - iS_2S_1 + S_2S_2,$$

but

$$\begin{aligned} S_1S_2 &= \frac{T^*+T}{2}\frac{T-T^*}{2i} \\ &= \frac{T^*T - T^*T^* + TT - TT^*}{4i} \\ &= \frac{T-T^*}{2i}\frac{T+T^*}{2} \\ &= S_2S_1 \end{aligned}$$

so that in the end $T^*T = S_1^2 + S_2^2$. As a consequence, if $\xi \in \mathscr{H}$, then

$$\begin{aligned} \langle (S_1^2+S_2^2)\xi, \xi\rangle &= \langle T^*T\xi, \xi\rangle \\ &= \langle T\xi, T\xi\rangle \\ &= \|T\xi\|^2 \\ &\leqslant \|T\|^2\|\xi\|^2. \end{aligned}$$

Dividing by $\|\xi\|^2$ and taking the supremum, we conclude that $\|S_1^2 + S_2^2\| \leqslant \|T\|^2$. Therefore, applying the first part of the proof with $S = \operatorname{Id}_{\mathscr{H}}$,

$$\begin{aligned} |\phi(T)|^2 &= \big|\phi(S_1)\big|^2 + \big|\phi(S_2)\big|^2 \\ &\leqslant \phi(S_1)^2\phi(\operatorname{Id}_{\mathscr{H}})^2 + \phi(S_2)^2\phi(\operatorname{Id}_{\mathscr{H}})^2 \\ &= \phi\left(S_1^2+S_2^2\right)\phi(\operatorname{Id}_{\mathscr{H}})^2 \\ &= \phi(T^*T)\phi(\operatorname{Id}_{\mathscr{H}})^2 \\ &\leqslant \|T\|^2\phi(\operatorname{Id}_{\mathscr{H}}) \end{aligned}$$

and the result follows. ∎

We now turn to the main technical ingredient that we need. This is a fundamental construction in operator algebras, called the GELFAND-NAIMARK-SEGAL CONSTRUCTION, usually abbreviated into *GNS construction*.

Proposition 2.1.2 (GNS CONSTRUCTION)**.** *Let $A \subset B(\mathscr{H})$ be a closed subalgebra stable under taking adjoints, and let $\phi : A \to \mathbf{C}$ be a positive linear form. Then, there exists a Hilbert space $\mathscr{H}'$, a continuous algebra homomorphism $\pi : A \to B(\mathscr{H}')$ preserving adjoints and a positive linear map $\phi' : B(\mathscr{H}') \to \mathbf{C}$ such that*

1. $\phi' \circ \pi = \phi$;
2. ϕ' *is* faithful *on* A *in the sense that* $\phi'(T^*T) > 0$ *for any non-zero* $T \in A$.

Proof. Let us consider the vector subspace

$$\mathscr{N} = \{T \in A \mid \phi(T^*T) = 0\}.$$

It is a closed vector subspace, and moreover it is a left ideal in A, since for any $S \in A$ and $T \in \mathscr{N}$ we have using Lemma 2.1.1

$$\begin{aligned}\phi((ST)^*(ST)) &= \phi(T^*S^*ST) \\ &\leqslant \phi((T^*S^*S)^*(T^*S^*S))\phi(T^*T) \\ &= 0.\end{aligned}$$

We now consider the vector space $A/\mathscr{N}$ and define a bilinear form on it through the formula

$$(T + \mathscr{N} \mid S + \mathscr{N}) = \phi(T^*S).$$

Observing that by Lemma 2.1.1, $\phi(\mathscr{N}) = \{0\}$, we see that $(\cdot \mid \cdot)$ is a well-defined sesquilinear form on $A/\mathscr{N}$, which is moreover positive definite since

$$\begin{aligned}(T + \mathscr{N} \mid T + \mathscr{N}) = 0 &\Leftrightarrow \phi(T^*T) = 0 \\ &\Leftrightarrow T \in \mathscr{N}.\end{aligned}$$

Let us denote by $\mathscr{H}'$ the completion of $A/\mathscr{N}$ with respect to the norm coming from $(\cdot \mid \cdot)$: this is a Hilbert space and we now have to find a *representation* of A on it.

For $T \in A$, define a linear map $\pi(T)$ on $A/\mathscr{N}$ through the formula

$$\pi(T)(S + \mathscr{N}) = TS + \mathscr{N}.$$

It therefore remains to prove that these operators are bounded so that they extend to $\mathscr{H}'$. We have

$$\|\pi(T)(S + \mathscr{N})\|^2_{\mathscr{H}'} = \phi(S^*T^*TS).$$

Define a new linear form $\psi : T \mapsto \phi(S^*TS)$. It is positive, hence bounded by Lemma 2.1.1 with $\|\psi\| = \psi(\mathrm{Id}_{\mathscr{H}})$, so that

$$\begin{aligned}\psi(T^*T) &\leqslant \psi(1)\|T^*T\|_A \\ &= \phi(S^*S)\|T^*T\|_A \\ &= \phi(S^*S)\|T\|^2_A\end{aligned}$$

Therefore,

$$\begin{aligned}\|\pi(T)(S + \mathscr{N})\|^2_{\mathscr{H}'} &= \psi(T^*T) \\ &\leqslant \phi(S^*S)\|T\|^2_A \\ &= \|S + \mathscr{N}\|^2_{\mathscr{H}'}\|T\|^2_A\end{aligned}$$

In other words, $\pi(T)$ is bounded with norm at most $\|T\|_A$.

Finally, set for $T \in B(\mathscr{H}')$,

$$\phi'(T) = (T(\mathrm{Id}_{\mathscr{H}} + \mathscr{N}), \mathrm{Id}_{\mathscr{H}} + \mathbf{N}).$$

If $T = \pi(S)^*\pi(S) = \pi(S^*S)$ is a positive operator[1] in $\pi(A)$, then $\phi'(T) = 0$ implies $\phi(S^*S) = 0$, hence $T = 0$. In other words, ϕ' is faithful on $\pi(A)$. ∎

Let us now state and prove the first main result of this lecture.

1. It is not straightforward to check that a positive element in $\pi(A)$ must be of the form $\pi(S)^*\pi(S)$. First observe that π is contractive and A is closed, so that $\pi(A)$ is complete and therefore also closed. If now $\pi(X) \in \pi(A)$ is positive, the restriction of square-root function on the spectrum of X is a uniform limit of polynomials $(f_n)_{n\in\mathbf{N}}$ and one can check that $f_n(\pi(X)) = \pi(f_n(X))$ converges to an element $\pi(S)$ satisfying $\pi(X) = \pi(S)^*\pi(S)$.

THEOREM 2.1.3 (FROM PERFECT QUANTUM STRATEGY TO QUANTUM ISOMORPHISM) Let G and H be two graphs and let

$$(\mathscr{E}_v^A)_{v\in V(G)},(\mathscr{E}_v^B)_{v\in V(G)})$$

be a perfect quantum strategy for the isomorphism game. Then, there exists a family of projections $(P_{vw})_{v\in V(G),w\in V(H)}$ and a positive linear form τ on the algebra $\mathscr{A}$ generated by them such that

1. τ is *tracial* in the sense that $\tau(ab)=\tau(ba)$ for all $a,b\in\mathscr{A}$;
2. The matrix $P=(P_{vw})$ is a quantum isomorphism from H to G;
3. For all $v,v\in V(G)$ and $w,w'\in V(H)$, $\langle E_{vw}F_{v'w'}\psi,\psi\rangle=\tau(P_{vw}P_{v'w'})$

Proof. We start with an elementary observation : if a positive operator $S=T^*T$ satisfies $\langle S\psi,\psi\rangle=0$, then $S\psi=0$ since the previous inner product equals $\|T\psi\|^2$. Therefore, the fact that for any $v\in V(G)$ and $w\neq w'\in V(H)$,

$$\langle E_{vw}F_{vw'}\psi,\psi\rangle=0$$

implies that $E_{vw}F_{vw'}\psi=0$ since the product of two commuting positive operators is positive. But then,

$$\begin{aligned}E_{vw}\psi&=E_{vw}\left(\sum_{w'\in V(H)}F_{vw'}\right)\psi\\&=\sum_{w'\in V(H)}E_{vw}F_{vw'}\psi\\&=E_{vw}F_{vw}\psi.\end{aligned}$$

Similarly, $F_{vw}\psi=F_{vw}E_{vw}\psi=E_{vw}F_{vw}\psi$, so that in the end we have the *synchronization identity* $E_{vw}\psi=F_{vw}\psi$ for all $v\in V(G)$ and $w\in V(H)$. We even have more :

$$E_{vw}\psi=E_{vw}\left(F_{vw}\psi\right)=E_{vw}E_{vw}\psi=E_{vw}^2\psi.$$

Consider now the closed subalgebra $A\subset B(\mathscr{H})$ generated *only* by the operators $(E_{vw})_{v\in V(G),w\in V(H)}$ and let $\phi:A\to\mathbf{C}$ be defined as

$$\phi(T)=\langle T\psi,\psi\rangle.$$

We perform the GNS construction and use the notations of **Proposition 2.1.2**. By the computation above, $(E_{vw}-E_{vw}^2)\psi=0$ which means that

$$\begin{aligned}\phi\left((E_{vw}-E_{vw}^2)^*(E_{vw}-E_{vw}^2)\right)&=\left\langle(E_{vw}-E_{vw}^2)\psi,(E_{vw}-E_{vw}^2)\psi\right\rangle\\&=0,\end{aligned}$$

i.e. $(E_{vw}-E_{vw}^2)\in\mathscr{N}$. Therefore, setting $P_{vw}=\pi(E_{vw})$, we have $P_{vw}^2=P_{vw}$. Since π preserves adjoints, this provides us with our family of orthogonal projections. Let us denote by $\tau=\phi'$ the positive faithful linear form on A obtained from ϕ through the GNS construction. We have to prove that it is tracial. To see why, let $v_1,\cdots,v_n\in V(G)$ and $w_1,\cdots,w_n\in V(H)$. Then,

$$\begin{aligned}\tau(P_{v_1w_1}\cdots P_{v_nw_n})&=\langle E_{v_1w_1}\cdots E_{v_nw_n}\psi,\psi\rangle\\&=\langle E_{v_1w_1}\cdots F_{v_nw_n}\psi,\psi\rangle\\&=\langle F_{v_nw_n}E_{v_1w_1}\cdots E_{v_{n-1}w_{n-1}}\psi,\psi\rangle\\&=\langle E_{v_1w_1}\cdots E_{v_{n-1}w_{n-1}}\psi,F_{v_nw_n}\psi\rangle\\&=\langle E_{v_1w_1}\cdots E_{v_{n-1}w_{n-1}}\psi,E_{v_nw_n}\psi\rangle\\&=\langle E_{v_nw_n}E_{v_1w_1}\cdots E_{v_{n-1}w_{n-1}}\psi,\psi\rangle\\&=\tau(P_{v_nw_n}P_{v_1w_1}\cdots P_{v_{n-1}w_{n-1}}).\end{aligned}$$

This proves traciality on $\mathscr{A}$.

Our next step is to make sure that the projections define a quantum isomorphism. We will use the following computation : for any $v,v' \in V(G)$ and $w,w' \in V(H)$,

$$\begin{aligned}\langle F_{v'w'}E_{vw}\psi,\psi\rangle &= \langle E_{vw}\psi,F_{v'w'}\psi\rangle\\ &= \langle E_{vw}\psi,E_{v'w'}\psi\rangle\\ &= \langle E_{v'w'}E_{vw}\psi,\psi\rangle\\ &= \phi(E_{v'w'}E_{vw})\\ &= \tau(P_{v'w'}P_{vw})\\ &= \tau(P_{v'w'}P_{vw}^2)\\ &= \tau(P_{vw}P_{v'w'}P_{vw})\end{aligned}$$

The fact that the sum over each row (i.e. for fixed $v \in V(G)$) is the identity is part of the definition of a quantum strategy. As for the columns, first note that because the strategy is perfect, ALICE and BOB cannot give the same answer if they are given different inputs, so that for $v \neq v'$,

$$\tau(P_{vw}P_{v'w}P_{vw}) = \langle F_{v'w'}E_{vw}\psi,\psi\rangle = 0.$$

By faithfulness of τ, we infer that $P_{vw}P_{v'w}P_{vw} = 0$ because that operator is positive :

$$P_{vw}P_{v'w}P_{vw} = (P_{v'w}P_{vw})^*(P_{v'w}P_{vw}).$$

Thus, P_{vw} and $P_{v'w}$ are orthogonal as projections. As a consequence,

$$T_w = \sum_{v\in V(G)} P_{vw} \leqslant \mathrm{Id}_{\mathscr{H}}$$

is a projection. But because

$$\sum_{w\in V(H)} T_w = |V(G)|.\mathrm{Id}_{\mathscr{H}} = |V(H)|.\mathrm{Id}_{\mathscr{H}}.$$

each T_w must be exactly equal to $\mathrm{Id}_{\mathscr{H}}$. Indeed, if there exist w_0 such that $T_{w_0} < \mathrm{Id}_{\mathscr{H}}$ and if $\xi \in \ker(T_{w_0})$, then

$$\begin{aligned}|V(H)|\|\xi\|^2 &= \left\langle \sum_{w\in V(H)} T_w(\xi),\xi \right\rangle\\ &= \sum_{w\in V(H)} \|T_w(\xi)\|^2\\ &= \sum_{w\in V(H)\setminus\{w_0\}} \|T_w(\xi)\|^2\\ &< (|V(H)|-1)\|\xi\|^2,\end{aligned}$$

a contradiction. It follows that each T_w is an injective projection, that is to say the identity.

It remains to check the last assertion of the statement. Let $(v,v') \in E(G)$ and $(w,w') \notin E(H)$. Then, by definition of a perfect quantum strategy,

$$\begin{aligned}0 &= \langle F_{v'w'}E_{vw}\psi,\psi\rangle\\ &= \tau(P_{vw}P_{v'w'}P_{vw})\end{aligned}$$

so that by faithfulness of τ, $P_{vw}P_{v'w'}P_{vw} = 0$. Because this is equal to $(P_{vw}P_{v'w'})(P_{vw}P_{v'w'})^*$, we conclude that $P_{vw}P_{v'w'} = 0$. The same argument works if $(v,v') \notin E(G)$ and $(w,w') \in E(H)$, hence the result by **Proposition 1.3.7**. ■

Remark 2.1.4. One might wonder where the operators F_{vw} have gone in the process. In fact, this is a subtlety of the proof. If we applied the GNS construction on the algebra generated by all the operators of both POVMs, then the equalities $E_{vw}\psi = E_{vw}F_{vw}\psi = F_{vw}E_{vw}\psi = F_{vw}\psi$ would force $\pi(E_{vw}) = \pi(F_{vw})$, which together with the commutativity assumption implies that our quantum isomorphism is classical. The trick is therefore that applying the method of the proof to the operators of ALICE or of BOB yields the same result, but applying it to both at the same time makes everything collapse.

Starting now from a quantum permutation matrix, one can define two families of POVMs by setting

$$E_{xy} = P_{xy} = F_{xy}.$$

However, two things are missing :

- There is no tracial state on the algebra generated by the projections :
- The POVMs will not commute unless the projections all pairwise commute, which is only possible for a classical solution.

The first point is an issue on which we will comment in the next section. As for the second one, it can be easily dealt with, as we shall now explain. In order to get a clear statement, let us first give a definition.

DEFINITION 2.1.5. A quantum permutation matrix $P = (P_{ij})_{1\leqslant i,j\leqslant N} \in \mathrm{M}_N(\mathscr{B}(H))$ is said to be *tracial* if there exists a tracial positive linear form on the $*$-algebra $\mathscr{A} \subset \mathscr{B}(H)$ generated by its coefficients.

Our result will then be

Corollary 2.1.6. *There exists a perfect quantum strategy for the graph isomorphism game if and only if there exists a tracial quantum permutation matrix P such that $A_G P = P A_H$.*

Proof. Setting $E_{vw} = P_{vw} = F_{vw}$ does not work because of commutativity, but almost works. More precisely, in the proof of the GNS construction given in **Proposition 2.1.2**, one might as well define a homomorphism $\rho : A \to B(\mathscr{H}')$ such that

$$\rho(T)(S + \mathscr{N}) = ST + \mathscr{N}.$$

This again defines bounded operators and moreover we have for any $T, T' \in A$ that

$$\begin{aligned}\pi(T)\big(\rho(T')(S+\mathscr{N})\big) &= \pi(T)\big(ST'+\mathscr{N}\big)\\ &= TST' + \mathscr{N}\\ &= \rho(T')(TS+\mathscr{N}))\\ &= \rho(T')(\pi(T)(S+\mathscr{N}))\end{aligned}$$

so that $[\pi(T), \rho(T')] = 0$. Therefore, we can set

$$E_{vw} = \pi(P_{vw}) \quad \& \quad F_{vw} = \rho(P_{vw})$$

to produce two commuting POVMs. ∎

2.1.2 THE TRACE PROBLEM

In the previous section, we showed that the existence of a tracial quantum permutation matrix implies the existence of a perfect quantum strategy. To prove the converse implication, one now needs to produce a faithful tracial positive linear map on the algebra generated by the coefficients of a quantum permutation. To understand why this is a non-trivial task, we will construct an explicit example of a quantum permutation whose coefficients generate an algebra with no tracial positive linear form at all. We start with the Hilbert space

$$\mathscr{H} = \ell^2(\mathbf{N}) \oplus \ell^2(\mathbf{N}).$$

It is separable and infinite-dimensional, allowing us to exploit one of the peculiar features of Hilbert spaces : there exists a unitary linear isomorphism

$$\Phi : \mathscr{H} \to \ell^2(\mathbf{N}).$$

Consider now the inclusion maps $\widetilde{s}_1, \widetilde{s}_2 : \ell^2(\mathbf{N}) \to \mathscr{H}$ respectively into the first and second summands. Then, setting

$$s_i = \Phi \circ \widetilde{s}_i \in B(\ell^2(\mathbf{N}))$$

for $i = 1,2$ produces two isometries on $\mathscr{H}$ satisfying the relations

$$\boxed{s_1^* s_1 = 1 = s_2^* s_2 \quad \& \quad s_1 s_1^* + s_2 s_2^* = 1}$$

Denoting by $\mathscr{A}$ the algebra generated by s_1, s_1^*, s_2 and s_2^*, we will show that it yields a counter-example. Let us start with an elementary fact : $\mathscr{A}$ does not admit any tracial positive linear map.

Lemma 2.1.7. *There is no non-zero tracial positive linear map on $\mathscr{A}$.*

Proof. Let τ be a tracial positive linear map. Then by traciality,

$$\tau(s_i s_i^*) = \tau(s_i^* s_i) = \tau(\mathrm{Id}_{\mathscr{H}}) = 1$$

for $i = 1,2$, while by linearity

$$\begin{aligned}\tau(\mathrm{Id}_{\mathscr{H}}) &= \tau(s_1 s_1^*) + \tau(s_2 s_2^*) \\ &= 2\tau(\mathrm{Id}_{\mathscr{H}}.\end{aligned}$$

Therefore, $\tau(\mathrm{Id}_{\mathscr{H}}) = 0$ and applying Lemma 2.1.1 with $S = \mathrm{Id}_{\mathscr{H}}$, we have for any $T \in A$,

$$\tau(T^* T) \leqslant \|T\|^2 \tau(\mathrm{Id}_{\mathscr{H}}) = 0.$$

■

Building a quantum permutation matrix whose coefficients generate $\mathscr{A}$ is not obvious and will we rather perform the construction in the algebra $\mathrm{M}_2(\mathscr{A}) \subset \mathrm{M}_2(B(\mathscr{H})) \simeq B(\mathscr{H} \oplus \mathscr{H})$. On the way, we will need a basic property of the generators.

Lemma 2.1.8. *We have $s_1^* s_2 = 0$.*

Proof. We compute

$$\begin{aligned}(s_1^* s_2)(s_1^* s_2)^* &= s_1^* s_2 s_2^* s_1 \\ &= s_1^*(1 - s_1 s_1^*) s_1 \\ &= s_1^* s_1 - (s_1^* s_1)^2 \\ &= \mathrm{Id}_{\mathscr{H}} - \mathrm{Id}_{\mathscr{H}}^2 \\ &= 0\end{aligned}$$

from which the result follows. ■

Let us define, for $i = 1,2$, the following elements of $\mathrm{M}_2(A)$:

$$x_1 = \begin{pmatrix} 0 & s_1^* \\ s_1 & s_2 s_2^* \end{pmatrix} \quad ; \quad x_2 = \begin{pmatrix} 0 & s_2^* \\ s_2 & s_1 s_1^* \end{pmatrix}$$
$$x_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad ; \quad x_4 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Proposition 2.1.9. *The elements x_i for $1 \leqslant i \leqslant 4$ are self-adjoint operators satisfying $x_i^2 = \mathrm{Id}_{\mathscr{H} \oplus \mathscr{H}}$. Moreover, they generate $\mathrm{M}_2(\mathscr{A})$ as an algebra.*

Proof. The first part of the statement is clear for x_3 and x_4, and the proof for the first two ones are similar, hence we only do it for x_1. By definition, $x_1^* = x_1$ and moreover

$$x_1^2 = \begin{pmatrix} s_1^* s_1 & s_1^* s_2 s_2^* \\ s_2 s_2^* s_1 & s_1 s_1^* + s_2 s_2^* \end{pmatrix} = \begin{pmatrix} \mathrm{Id}_{\mathscr{H}} & 0 \\ 0 & \mathrm{Id}_{\mathscr{H}} \end{pmatrix}.$$

For the generation result, we will first prove that x_3 and x_4 generate $\mathrm{M}_2(\mathbf{C})$. Let us denote by E_{ij} the matrix with a coefficient 1 in position (i,j) and 0 elsewhere. These form a basis of $\mathrm{M}_2(\mathbf{C})$. First, we have $x_3^2 = \mathrm{Id}_{\mathrm{M}_2(\mathbf{C})}$ so that $\langle x_3, x_4 \rangle$ contains

$$2E_{11} = x_3 + x_3^2 - 2E_{22} \qquad = x_3 - x_3^2.$$

Second,

$$x_3x_4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

so that $\langle x_3, x_4\rangle$ also contains

$$2E_{12} = x_4 + x_3x_4$$
$$2E_{21} = x_4 - x_3x_4,$$

concluding the proof.

Let us now denote by B the sub-C*-algebra of $\mathrm{M}_2(A)$ generated by x_1, x_2, x_3 and x_4. By the preceding question, $\mathrm{M}_2(\mathbf{C}) \subset B$. Moreover, observe that for $i = 1, 2$,

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} x_i \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ s_i & 0 \end{pmatrix}.$$

Multiplying this last matrix with well-chosen elements of $\mathrm{M}_2(\mathbf{C})$, one gets that $s_k E_{ij} \in B$ for all $1 \leqslant i, j, k \leqslant 2$, hence $B = \mathrm{M}_2(A)$. ■

Observe that the elements

$$p_i = \frac{x_i + 1}{2}$$

are orthogonal projections which generate $\mathrm{M}_2(\mathscr{A})$. All that is left to do is to write them as the coefficients of a quantum permutation, and then to check that there is still no trace on $\mathrm{M}_2(\mathscr{A})$.

THEOREM 2.1.10 The algebra $M_2(\mathscr{A})$ is generated by the coefficients of a quantum permutation, and has no non-zero tracial positive linear map.

Proof. Let us define matrices $\mathrm{M}_i \in \mathrm{M}_2(\mathscr{A})$ as follows :

$$\mathrm{M}_i = \begin{pmatrix} p_i & 1 - p_i \\ 1 - p_i & p_i \end{pmatrix}.$$

Let P be the block-diagonal matrix with diagonal blocks $(\mathrm{M}_i)_{1 \leqslant i \leqslant 4}$. This is a quantum permutation matrix by construction, and its coefficients generate $\mathrm{M}_2(\mathscr{A})$.

Assume now that there is a non-zero tracial positive linear map τ on $\mathrm{M}_2(\mathscr{A})$, and define a linear form $\widetilde{\tau} : \mathscr{A} \to \mathbf{C}$ through the formula

$$\widetilde{\tau}(a) = \tau \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}.$$

Observe that because $E_{12}E_{12}^* = E_{11}$ and $E_{12}^*E_{12} = E_{22}$, we must have $\tau(E_{11}) = \tau(E_{22})$. Summing these two gives $\alpha = \tau(\mathrm{Id}_{\mathscr{H}}) > 0$, hence $\tau(E_{11}) = \alpha/2 > 0$ and τ is non-zero. Moreover, if follows directly from the definition that for any $a \in A$,

$$\widetilde{\tau}(a^*a) = \tau \begin{pmatrix} a^*a & 0 \\ 0 & 0 \end{pmatrix} = \tau \left(\begin{pmatrix} a^* & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right) \geqslant 0$$

and for any $a, b \in A$,

$$\begin{aligned} \widetilde{\tau}(ab) &= 2\tau \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} = 2\tau \left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \right) \\ &= 2\tau \left(\begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \right) = 2\tau \begin{pmatrix} ba & 0 \\ 0 & 0 \end{pmatrix} \\ &= \widetilde{\tau}(ba). \end{aligned}$$

Therefore, $\widetilde{\tau}$ is a tnon-zero tracial positive linear map on $\mathscr{A}$, in contradiction with Lemma 2.1.7. ■

Remark 2.1.11. The closure of $\mathscr{A}$ with respect to the operator norm is called the *Cuntz algebra* and denoted by $\mathcal{O}_2$. It plays an important role in the study of the structure and classification of the so-called *C*-algebras*.

This example shows that the existence of a tracial positive linear form is not a formal consequence of the defining relations of a quantum permutation matrix. Any proof of THEOREM 1.5.1 must therefore use additional structure. How can we get around this obstruction? The point is that even though we cannot guarantee the existence of a faithful tracial state on the algebra generated by the coefficients, one can always build *another* quantum isomorphism for which such a state exists. This is done by considering an abstract algebra defined by the relations that any quantum isomorphism must satisfy. On the one hand, the existence of a specific quantum isomorphism means that the abstract algebra is non-trivial. On the other hand, the abstract algebra can always be embedded into a larger one, given by the so-called *quantum automorphism group* of the disjoint union $G \sqcup H$ of the two graphs. The key fact now is that the algebra of such a quantum group always admits a tracial positive linear map, which is a generalization of the linear form obtained by integration of functions on a classical compact group with respect to its *Haar measure*. Details about the theory of compact quantum groups and the proof of these results can be found in [Fre23].

2.2 CONSTRAINTS

In the second part of this lecture, we will construct an explicit pair of graphs which are quantum isomorphic but not isomorphic. As it will appear, such a construction is not straightforward, and requires a detour through another type of combinatorial problem. In fact, this will ultimately lead us to a general algorithm for building such a pair of graphs starting from any *non-planar* graph, following [Ark12]. The general strategy is to turn the problem of quantum graph isomorphism into a simpler one, involving systems of equations modulo 2. We therefore first introduce these.

DEFINITION 2.2.1. A *linear binary constraint system* (LBCS in short) $\mathscr{F}$ is a system of finitely many linear equations over the field $\mathbf{F}_2$. In other words, it is given by an integer n, non-empty subsets $S_\ell \subset \{1, \cdots n\}$ for $1 \leqslant \ell \leqslant m$ and elements $b_\ell \in \mathbf{F}_2$ such that the equations are

$$\boxed{\sum_{i \in S_\ell} x_i = b_i}$$

The equation above will be called *the ℓ-th equation* of the system.

Let us immediately give an example of LBCS which will play a central role throughout the lecture.

Example 2.2.2 (MERMIN-PERES MAGIC SQUARE)**.** Consider the following LBCS from [Mer90] :

$$\begin{cases} x_1 + x_2 + x_3 &= 0 \\ x_4 + x_5 + x_6 &= 0 \\ x_7 + x_8 + x_9 &= 0 \\ x_1 + x_4 + x_7 &= 0 \\ x_2 + x_5 + x_8 &= 0 \\ x_3 + x_6 + x_9 &= 1 \end{cases} \tag{2.1}$$

This system was introduced independently by N. MERMIN in [Mer90] and A. PERES in [Per]. It is usually called the *magic square* because it can be written in the following way :

	C_1	C_2	C_3	
R_1	x_1	x_2	x_3	$=0$
R_2	x_4	x_5	x_6	$=0$
R_3	x_7	x_8	x_9	$=0$
	$=0$	$=0$	$=1$	

At first sight, this system looks completely innocuous, but a quick look at the right-hand sides of the system (2.1) shows that there is no solution in $\mathbf{F}_2$. Indeed, the sum of the right-hand sides is 1 while, since each variable appears exactly twice, adding all six equations modulo 2 yields 0. As one may guess, this is on purpose : we want to define a suitable notion of « quantum solution » to the system, which will somehow correspond to quantum isomorphism for graphs, while the classical solutions will yield classical isomorphism.

To make this precise, we need a notion of quantum solution, and that is a bit tricky. Indeed, the equation $x_i + x_i = 0$ has no non-trivial operator solution over a Hilbert space ! Things become clearer if we first rewrite the system using the multiplicative notation for $\mathbf{F}_2 = \{-1, 1\}$. More precisely write the ℓ-th equation as

$$\prod_{i \in S_\ell} x_i = (-1)^{b_\ell}.$$

Then, we are looking for operators satisfying $X^2 = \mathrm{Id}_{\mathscr{H}}$ and whose product is a multiple of the identity. Here is the precise definition.

DEFINITION 2.2.3. A *quantum solution* of an LBCS $\mathscr{F}$ is given by a Hilbert space $\mathscr{H}$ and operators $(X_i)_{1 \leqslant i \leqslant n}$ in $B(\mathscr{H})$ such that

- $X_i^* = X_i$ and $X_i^2 = \mathrm{Id}_{\mathscr{H}}$ for all $1 \leqslant i \leqslant n$;
- For every $1 \leqslant \ell \leqslant m$, the operators $(X_i)_{i \in S_\ell}$ pairwise commute ;
- For every $1 \leqslant \ell \leqslant m$,

$$\boxed{\prod_{i \in S_\ell} X_i = (-1)^{b_\ell} \mathrm{Id}_{\mathscr{H}}}$$

Remark 2.2.4. One can freely permute the variables in any equation of $\mathscr{F}$ without changing the system, and that is why the second condition in Definition 2.2.3 is necessary to make the concept depend only on the system and not on the way it is written. From a more physical point of view, this is the requirement that the observables appearing in a given equation should be measurable simultaneously.

Remark 2.2.5. In linear algebra, an operator $X \in B(\mathscr{H})$ satisfying $X^* = X$ and $X^2 = \mathrm{Id}_{\mathscr{H}}$ is called a *symmetry*.

The key idea is now to produce out of a LBCS a pair of graphs whose quantum and classical isomorphism is related to the existence of quantum and classical solutions for the original system.

DEFINITION 2.2.6. Let $\mathscr{F}$ be a LBCS with m equations. We define a graph $G_{\mathscr{F}}$ with vertex set given by pairs (ℓ, f), where $1 \leqslant \ell \leqslant m$ and $f : S_\ell \to \mathbf{F}_2$ is a *partial solution* of the ℓ-th equation in the sense that

$$\sum_{i \in S_\ell} f(i) = b_\ell,$$

i.e. setting $x_i = f(i)$ solves the ℓ-th equation of the system. Moreover, two vertices (ℓ, f) and (ℓ', f') are connected by an edge if they are *inconsistent* in the sense that there exists $i \in S_\ell \cap S_{\ell'}$ with $f(i) \neq f'(i)$.

The procedure above produces a graph $G_{\mathscr{F}}$, but we need two of them. To produce the second one, we will simply modify the right-hand sides of $\mathscr{F}$ to ensure the existence of a classical solution. This is very easy : if $b_i = 0$ for all $1 \leqslant i \leqslant m$, then assigning 0 to all variables gives a solution.

DEFINITION 2.2.7. For an LBCS $\mathscr{F}$, we denote by $\mathscr{F}_0$ the LBCS obtained by setting $b_i = 0$ for all $1 \leqslant i \leqslant m$ and call it the *homogenization* of $\mathscr{F}$.

Our second graph will be $G_{\mathscr{F}_0}$. We now have three problems to solve, namely

1. Characterize when $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ are isomorphic;
2. Characterize when $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ are *quantum* isomorphic;
3. Produce an explicit $\mathscr{F}$ for which the first criterion above is satisfied while the second one is not.

We will proceed in the order above and therefore start with classical isomorphism.

2.2.1 CLASSICAL ISOMORPHISM

Proving that two graphs are not isomorphic can be an easy task : there are many combinatorial and geometric invariants and finding one which differs between the two graphs is enough to decide non-isomorphism. In our case, we will use the so-called *independence number*, the definition of which we now give.

DEFINITION 2.2.8. The *independence number* of a graph G is the maximal cardinality $\alpha(G)$ of a set of vertices such that no two elements share an edge (a so-called *independent set*).

Observe that any vertex (ℓ, f) of $G_{\mathscr{F}}$ is connected to any other (ℓ, f') by definition, so that the vertices to which it is not connected are of the form (ℓ', f') for some $\ell' \neq \ell$. Therefore, any independent set contains at most one vertex per constraint. In other words,

$$\alpha(G_{\mathscr{F}}) \leqslant m.$$

Observe also that if $f_0^S : S \to \mathbf{F}_2$ is the function mapping everything to 0, then $\{(\ell, f_0^{S_\ell} \mid 1 \leqslant \ell \leqslant m)\}$ is an independent set in $G_{\mathscr{F}_0}$, so that $\alpha(G_{\mathscr{F}_0}) = m$. We will now show that this gives a sufficient criterion to decide isomorphism.

THEOREM 2.2.9 Given a LBCS $\mathscr{F}$, the following are equivalent :

i) $\mathscr{F}$ has a classical solution

ii) The graphs $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ are isomorphic;

iii) $\alpha(G_{\mathscr{F}}) = m$.

Proof. Let us proceed through a chain of implications.

i) $\Rightarrow$ ii) We will construct the desired isomorphism explicitly. Let $F : \{1, \cdots n\} \to \mathbf{F}_2$ be a solution to $\mathscr{F}$ and let F_ℓ be its restriction to S_ℓ for $1 \leqslant \ell \leqslant m$. Then, for a vertex (ℓ, f) of $G_{\mathscr{F}}$, we define a function $f \oplus F_\ell : i \in S_\ell \mapsto f(i) + F_\ell(i)$ and set

$$\varphi(\ell, f) = (\ell, f \oplus F_\ell).$$

We claim that φ maps $V(G_{\mathscr{F}})$ to $V(G_{\mathscr{F}_0})$ bijectively, and that it is a graph isomorphism. To prove this, observe first that for every $1 \leqslant \ell \leqslant m$,

$$\begin{aligned} \sum_{i \in S_\ell} (f \oplus F_\ell)(i) &= \sum_{i \in S_\ell} f(i) + \sum_{i \in S_\ell} F_\ell(i) \\ &= b_\ell + b_\ell \\ &= 0 \end{aligned}$$

so that $\varphi(\ell,f)$ is indeed a vertex of $G_{\mathscr{F}_0}$. Similarly, setting for $(\ell,f)\in V(G_{\mathscr{F}_0})$

$$\psi(\ell,f)=(\ell,f\oplus F_\ell)$$

we see by the same argument – *mutatis mutandis* – that ψ has range $V(G_{\mathscr{F}})$ and is inverse to φ, proving that it is a bijection.

Next, if (ℓ,f) and (ℓ',f') are adjacent in $G_{\mathscr{F}}$, then there exists $i\in S_\ell\cap S_{\ell'}$ such that $f(i)\neq f'(i)$. As a consequence,

$$\begin{aligned}(f\oplus F_\ell)(i)&=f(i)+F_\ell(i)\\&=f(i)+F_{\ell'}(i)\\&\neq f'(i)+F_{\ell'}(i)\\&=(f'\oplus F_\ell)(i)\end{aligned}$$

so that $\varphi(\ell,f)$ is adjacent to $\varphi(\ell',f')$. Similarly, if (ℓ,f) and (ℓ',f') are *not* adjacent, then for all $i\in S_\ell\cap S_{\ell'}$,

$$\begin{aligned}(f\oplus F_\ell)(i)&=f(i)+F_\ell(i)\\&=f(i)+F_{\ell'}(i)\\&=f'(i)+F_{\ell'}(i)\\&=(f'\oplus F_\ell)(i)\end{aligned}$$

and $\varphi(\ell,f)$ is not adjacent to $\varphi(\ell',f')$. This proves that φ is a graph isomorphism.

ii) $\Rightarrow$ iii) Two isomorphic graphs have the same independence number by definition, and we have already seen that $\alpha(G_{\mathscr{F}_0})=m$.

iii) $\Rightarrow$ i) Let $\mathscr{S}\subset V(G_{\mathscr{F}})$ be an independent set of size m. For each $1\leqslant\ell\leqslant m$, $\mathscr{S}$ cannot contain more than one vertex of the form (ℓ,f) by the discussion preceding the theorem. Therefore, it contains exactly one, and we denote it by (ℓ,f_ℓ). Our claim is that the functions f_ℓ are restrictions of a global function $F:\{1,\cdots,n\}\to\mathbf{F}_2$ giving a classical solution. To prove this, simply observe that for any $1\leqslant i\leqslant n$ and $\ell\neq\ell'$ such that $i\in S_\ell\cap S_{\ell'}$, we have $f_\ell(i)=f_{\ell'}(i)$ since otherwise there would be an edge between (ℓ,f_ℓ) and $(\ell',f_{\ell'})$. As a consequence, there is a well-defined function F such that $F_{S_\ell}=f_\ell$. Since f_ℓ satisfies the ℓ-th equation, F satisfies the whole system. ■

2.2.2 QUANTUM ISOMORPHISM

Our next goal is to find at least a sufficient criterion to ensure that $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ are quantum isomorphic. To do this, let us first construct our candidate for a quantum isomorphism out of a quantum solution of $\mathscr{F}$. More precisely, let $(X_i)_{1\leqslant i\leqslant m}$ be such a solution. Each X_i, being a symmetry, has spectrum contained in $\{-1,1\}$ and can even be written as

$$X_i=P_1^i-P_{-1}^i$$

with $P_{\pm1}^i$ being orthogonal projections whose product vanishes. Given vertices (ℓ,f) and (ℓ',f') of $G_{\mathscr{F}}$, we set (with $\oplus$ denoting as before addition modulo 2)

$$p_{(\ell,f),(\ell',f')}=\begin{cases}\prod_{i\in S_\ell}P^i_{g(i)} & \text{if } \ell=\ell' \text{ and } f'=f\oplus g\\ 0 & \text{otherwise}\end{cases}$$

It is not even clear that the elements defined above are projections, let alone that they form a quantum permutation. This is an elementary though tedious computation, so let us get rid of it right away.

Lemma 2.2.10. *With the notations above, the elements $p_{(\ell,f),(\ell',f')}$ form a quantum permutation.*

Proof. First observe that

$$P_1^i = \frac{1+X_i}{2} \quad \& \quad P_{-1}^i = 1 - P_1^i,$$

so that the spectral projections of X_i and X_j commute as soon as the symmetries commute. In particular, $p_{(\ell,f),(\ell',f')}$ is an orthogonal projection as a product of pairwise commuting orthogonal projections. Considering now the sum over a given row (ℓ,f), we have by definition

$$\sum_{(\ell',f')} p_{(\ell,f),(\ell',f')} = \sum_{g:S_\ell \to \mathbf{F}_2} \prod_{i \in S_\ell} P_{g(i)}^i.$$

Let us write $S_\ell = \{i_1, \cdots, i_k\}$ and $S'_\ell = S_\ell \setminus \{i_1\}$. Then, splitting according to the value of $g(i_1)$, we get

$$\begin{aligned}
\sum_{g:S_\ell \to \mathbf{F}_2} \prod_{i \in S_\ell} P_{g(i)}^i &= \sum_{g:S'_\ell \to \mathbf{F}_2} P_1^{i_1} \prod_{i \in S'_\ell} P_{g(i)}^i + \sum_{g:S'_\ell \to \mathbf{F}_2} P_{-1}^{i_1} \prod_{i \in S'_\ell} P_{g(i)}^i \\
&= (P_1^i + P_{-1}^i) \sum_{g:S'_\ell \to \mathbf{F}_2} \prod_{i \in S'_\ell} P_{g(i)}^i \\
&= \sum_{g:S'_\ell \to \mathbf{F}_2} \prod_{i \in S'_\ell} P_{g(i)}^i
\end{aligned}$$

and an elementary induction yields that the sum is $\mathrm{Id}_{\mathscr{H}}$. The same argument works *mutatis mutandis* for columns, concluding the proof. ■

We are now ready to show that the existence of a quantum solution implies quantum isomorphism of the associated graphs.

THEOREM 2.2.11 Let $\mathscr{F}$ be a LBCS which has a quantum solution. Then, the graphs $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ are quantum isomorphic.

Proof. It suffices to verify the criterion from **Proposition 1.3.7**. Consider therefore two adjacent vertices (ℓ,f) and (ℓ',f') in $G_{\mathscr{F}}$ and two non-adjacent vertices (k,g) and (k',g') in $G_{\mathscr{F}_0}$ and let us prove that the product $p_{(\ell,f),(k,g)} p_{(\ell',f'),(k',g')}$ vanishes. Of course, the vanishing is automatic if $\ell \neq k$ or $\ell' \neq k'$ since at least one of the projections vanishes in that case. Writing $g = f \oplus h$ and $g' = f' \oplus h'$, we are therefore left with computing

$$T = \left(\prod_{i \in S_\ell} P_{h(i)}^i \right) \left(\prod_{i \in S_{\ell'}} P_{h'(i)}^i \right).$$

Because (ℓ,f) and (ℓ',f') are adjacent, they are inconsistent, hence there is some $i_0 \in S_\ell \cap S_{\ell'}$ such that $f(i_0) \neq f'(i_0)$ while $g(i) = g'(i)$ for all $i \in S_\ell \cap S_{\ell'}$. This implies that $h'(i_0) \neq h(i_0)$, for instance through the following computation :

$$\begin{aligned}
h(i_0) + h'(i_0) &= f(i_0) + g(i_0) + f'(i_0) + g'(i_0) \\
&= f(i_0) + f'(i_0) \\
&\neq 0.
\end{aligned}$$

Using commutativity of the projections in each of the two products, we see that

$$T = \left(\prod_{i \in S_\ell \setminus \{i_0\}} P_{h(i)}^i \right) P_{h(i_0)}^{i_0} P_{h'(i_0)}^{i_0} \left(\prod_{i \in S_{\ell'} \setminus \{i_0\}} P_{h'(i)}^i \right)$$

and the product in the middle vanishes since these are two different spectral projections of the same operator. As a consequence, $T = 0$ as needed. The same argument works *mutatis mutandis* when (ℓ,f) and (ℓ',f') are not adjacent while (k,g) and (k',g') are adjacent, hence the result. ■

2.2.3 EXCURSUS : QUANTUM INDEPENDENCE

The reader will have surely have noticed that THEOREM 2.2.11 is weaker in its formulation than THEOREM 2.2.9 : we did not prove an equivalence between the two properties in the quantum case, for two reasons. First, the implication which is proven is the one which is useful for producing examples. Second, proving an equivalence requires developping a quantum version of the independence number of a graph, which takes a bit of time. Nevertheless, for the sake of completeness, we will now do this and provide a full quantum analogue of THEOREM 2.2.9.

A definition

We defined the classical independence number in terms of independent sets in a graph. Quantizing this is not straightforward with our approach. However, there is an equivalent description in terms of graph homomorphisms : a independent set of m vertices is the same as a homomorphism from the complete graph K_m to the complement G^c of the graph G. Since we have encoded graph isomorphisms of the vertices into square matrices of projections, we can extend the setting by implementing "quantum graph homomorphisms" with rectangular matrices of projections. A bit of care is needed though : we have already shown in Lemma 1.3.4 that the sum cannot be the indentity on both rows and columns if the matrix is not square. We therefore have to make some choice. Instead of giving a general definition, we will simply give the special form $K_m \to G^c$.

DEFINITION 2.2.12 (Quantum independent set). Let G be a graph and $m \geqslant 1$ be an integer. A *quantum independent set of size m* in G is a Hilbert space $\mathscr{H}$ together with a family of orthogonal projections $(E_{iv})_{1\leqslant i\leqslant m, v\in V(G)}$ in $B(\mathscr{H})$ such that

1. For every $1 \leqslant i \leqslant m$, $\sum_{v\in V(G)} E_{iv} = \mathrm{Id}_{\mathscr{H}}$;
2. For $i \neq j$ and $v \in V(G)$, $E_{iv}E_{jv} = 0$;
3. For $i \neq j$ and $(v,w) \in E(G)$, $E_{iv}E_{jw} = 0$.

The *quantum independence number* of G is

$$\boxed{\alpha_q(G) = \max\{m \in \mathbf{N} \mid G \text{ has a quantum independent set of size } m\}}$$

It is quite clear that $\alpha_q(G)$ is invariant under isomorphism. But for it to be a sound notion, we need to check that it is also invariant under quantum isomorphim.

Proposition 2.2.13. *If G and H are quantum isomorphic, then $\alpha_q(G) = \alpha_q(H)$.*

Proof. Because quantum isomorphism is a symmetric relation by **Proposition 1.3.8**, it suffices to prove that $\alpha_q(G) \geqslant \alpha_q(H)$. The proof is in fact very close to that of **Proposition 1.3.8**. Let $P = (p_{wv})_{w\in V(H), v\in V(G)}$ be a quantum isomorphism from G to H on a Hilbert space $\mathscr{H}_2$, and let $(E_{iw})_{1\leqslant i\leqslant m, w\in V(H)}$ be a quantum independent set of size $m = \alpha_q(H)$ on some other Hilbert space $\mathscr{H}_1$. Consider the tensor product Hilbert space $\mathscr{H} = \mathscr{H}_1 \otimes \mathscr{H}_2$ and set for $1 \leqslant i \leqslant m$ and $v \in V(G)$,

$$F_{iv} = \sum_{w\in V(H)} E_{iw} \otimes p_{wv}.$$

These are orthogonal projections, and we have to check that they satisfy the conditions of Definition 2.2.12.

1. This is exactly the same computation as in the proof of **Proposition 1.3.8** :

$$\begin{aligned}\sum_{v\in V(G)} F_{iv} &= \sum_{w\in V(H)} E_{iw} \otimes \left(\sum_{v\in V(G)} p_{wv}\right)\\ &= \sum_{w\in V(H)} E_{iw} \otimes \mathrm{Id}_{\mathscr{H}_2}\\ &= \mathrm{Id}_{\mathscr{H}_1} \otimes \mathrm{Id}_{\mathscr{H}_2}.\end{aligned}$$

2. Let $i \neq j$ and $v \in V(G)$. We split the product

$$F_{iv}F_{jv} = \sum_{w,w'} E_{iw}E_{jw'} \otimes p_{wv}p_{w'v}$$

according to whether $w = w'$ or $w \neq w'$. If $w = w'$, then the first tensor factor vanishes by the second condition in Definition 2.2.12 ; if $w \neq w'$, then the second tensor factor vanishes since $p_{wv}p_{w'v} = 0$ (same column of the quantum permutation matrix P). Therefore, $F_{iv}F_{jv} = 0$.

3. Let $i \neq j$ and $(v,v') \in E(G)$. By the criterion of **Proposition 1.3.7** applied to P, $p_{wv}p_{w'v'} = 0$ unless $(w,w') \in E(H)$ (this covers both the case $w \neq w'$ with $(v,v') \notin E(G)$, and the case $w = w'$, since graphs have no loops hence $(v,v) \notin E(G)$). As a consequence, in

$$F_{iv}F_{jv'} = \sum_{w,w'} E_{iw}E_{jw'} \otimes p_{wv}p_{w'v},$$

every term with $(w,w') \notin E(H)$ already vanishes through its second tensor factor, while every term with $(w,w') \in E(H)$ vanishes through its first tensor factor by the last condition in Definition 2.2.12 (as $i \neq j$). Therefore, $F_{iv}F_{jv'} = 0$.

This proves $(F_{iv})_{1\leqslant i\leqslant m, v\in V(G)}$ is a quantum independent set in G, yielding $m = \alpha_q(H) \leqslant \alpha_q(G)$. ■

Before proving that our quantum independence number characterizes quantum isomorphism for graphs coming from a LBCS, let us give a very simple inequality relating it to the classical independence number.

Lemma 2.2.14. *For every graph G, $\alpha(G) \leqslant \alpha_q(G) \leqslant |V(G)|$.*

Proof. Given an independent set $\{v_1, \cdots, v_m\}$, one might take $\mathscr{H} = \mathbf{C}$ and set $E_{iv} = \delta_{iv_i}$. This is easily seen to be a quantum independent set of size m, hence the first inequality. As for the second one, let $(E_{iv})_{1\leqslant i\leqslant m, v\in V(G)}$ be a quantum independent set of size m. For $v \in V(G)$,

$$Q_v = \sum_{i=1}^{m} E_{iv}$$

is a sum of pairwise orthogonal projections, hence a projection itself. In particular, $Q_v \leqslant \mathrm{Id}_{\mathscr{H}}$. Summing over $v \in V(G)$,

$$\begin{aligned} m.\mathrm{Id}_{\mathscr{H}} &= \sum_{i=1}^{m} \left(\sum_{v\in V(G)} E_{iv} \right) \\ &= \sum_{v\in V(G)} \left(\sum_{i=1}^{m} E_{iv} \right) \\ &\leqslant |V(G)|.\mathrm{Id}_{\mathscr{H}}, \end{aligned}$$

Applying this to a non-zero vector and taking norms yields $m \leqslant |V(G)|$. ■

Connection to quantum isomorphism

We now want to prove a quantum analogue of THEOREM 2.2.9. There was one trivial direction in the classical case : the equality $\alpha(G_{\mathscr{F}_0}) = m$. We will first prove the quantum version of this, relying on the following fact :

Lemma 2.2.15. *Let G be a graph such that $V(G) = C_1 \sqcup \cdots \sqcup C_m$, with C_i being a clique for all $1 \leqslant i \leqslant m$. Then, $\alpha_q(G) \leqslant m$. In particular, $\alpha_q(G_{\mathscr{F}_0}) = m$.*

Proof. Let $(E_{iv})_{1\leqslant i\leqslant k, v\in V(G)}$ be a quantum independent set of size k. For $1 \leqslant i \leqslant k$ and $1 \leqslant \ell \leqslant m$, set

$$T_i^{\ell} = \sum_{v\in C_\ell} E_{iv}.$$

This is a sum of pairwise orthogonal projections, hence a projection again, which implies $T_i^\ell \leqslant \mathrm{Id}_{\mathscr{H}}$. Moreover, for every $1 \leqslant i \leqslant k$,

$$\begin{aligned}\sum_{\ell=1}^{m} T_i^\ell &= \sum_{v \in V(G)} E_{iv} \\ &= \mathrm{Id}_{\mathscr{H}}.\end{aligned}$$

Now fix $1 \leqslant \ell \leqslant m$ and consider $1 \leqslant i \neq j \leqslant k$. For $v, w \in C_\ell$, we have the following possibilities :

- If $v = w$, the second condition in Definition 2.2.12 yields $E_{iv}E_{jv} = 0$;
- If $v \neq w$, then $(v,w) \in E(G)$ since C_ℓ is a clique, hence the third condition in Definition 2.2.12 gives $E_{iv}E_{jw} = 0$.

In both cases, $E_{iv}E_{jw} = 0$ hence

$$T_i^\ell T_j^\ell = \sum_{v,w \in C_\ell} E_{iv}E_{jw} = 0.$$

Once again, this means that they are pairwise orthogonal projections and therefore add up to a projection which by definition is smaller than $\mathrm{Id}_{\mathscr{H}}$. Therefore, adding up gives

$$\begin{aligned}k.\mathrm{Id}_{\mathscr{H}} &= \sum_{i=1}^{k}\left(\sum_{\ell=1}^{m} T_i^\ell\right) \\ &= \sum_{\ell=1}^{m}\left(\sum_{i=1}^{k} T_i^\ell\right) \\ &\leqslant m.\mathrm{Id}_{\mathscr{H}},\end{aligned}$$

which implies $k \leqslant m$ (for insance by applying the inequality to a non-zero vector and taking norms).

To prove the second assertion, observe that on the one hand, $G_{\mathscr{F}_0}$ has m distinct cliques and on the other hand, $\alpha_q(G_{\mathscr{F}_0}) \geqslant \alpha(G_{\mathscr{F}_0}) = m$ by Lemma 2.2.14. ■

Starting with a quantum independent set of size m in $G_{\mathscr{F}}$, denoted by $(E_{\alpha,(\ell,f)})_{1\leqslant\alpha\leqslant m,(\ell,f)\in V(G_{\mathscr{F}})}$, it is natural to try to build the symmetries $(X_i)_{1\leqslant i\leqslant m}$ through their spectral projections. The simplest guess for that is

$$P_\epsilon^i = \sum_{\alpha=1}^{m}\sum_{f\,|\,f(i)=\epsilon} E_{\alpha,(\ell,f)}.$$

But what is ℓ above? It should be an index such that $i \in S_\ell$, but what if there is a distinct ℓ' such that $i \in S_\ell \cap S_{\ell'}$? We will first prove that this does not create any issue.

Lemma 2.2.16. *For $1 \leqslant i \leqslant n$ and $1 \leqslant \ell \leqslant m$ such that $i \in S_\ell$, the operator*

$$P_\epsilon^{i,\ell} = \sum_{\alpha=1}^{m}\sum_{f\,|\,f(i)=\epsilon} E_{\alpha,(\ell,f)}$$

is a projection satisfying

$$P_1^{i,\ell} + P_{-1}^{i,\ell} = \mathrm{Id}_{\mathscr{H}}.$$

Moreover, it is independent from ℓ.

Proof. First,

$$Q_f^\ell = \sum_{\alpha=1}^{m} E_{\alpha,(\ell,f)}$$

is a sum of pairwise orthogonal projections, hence an orthogonal projection itself. Second, by definition of a quantum independent set,

$$\begin{aligned}Q_f^\ell Q_{f'}^\ell &= \sum_{\alpha=1}^{m}\sum_{\beta=1}^{m} E_{\alpha,(\ell,f)}E_{\beta,(\ell,f')} \\ &= 0\end{aligned}$$

because (ℓ, f) and (ℓ, f') form an edge of $G_{\mathscr{F}}$ since they are inconsistent. Therefore,

$$P_\epsilon^{i,\ell} = \sum_{f|f(i)=\epsilon} Q_f^\ell$$

is an orthogonal projection. Moreover, consider

$$T_\ell = P_1^{i,\ell} + P_{-1}^{i,\ell} = \sum_{\alpha=1}^{m} \sum_f E_{\alpha,(\ell,f)}$$

These are m orthogonal projections, satisfying

$$\begin{aligned}\sum_{\ell=1}^{m} T_\ell &= \sum_{\ell=1}^{m}\sum_{\alpha=1}^{m}\sum_f E_{\alpha,(\ell,f)} \\ &= \sum_{\alpha=1}^{m}\sum_{\ell=1}^{m}\sum_f E_{\alpha,(\ell,f)} \\ &= \sum_{\alpha=1}^{m} \mathrm{Id}_{\mathscr{H}} \\ &= m.\mathrm{Id}_{\mathscr{H}}.\end{aligned}$$

By the same argument as in the proof of THEOREM 2.1.3, this implies $T_\ell = \mathrm{Id}_{\mathscr{H}}$ as claimed.

Assume now that we have $\ell \neq \ell'$ such that $i \in S_\ell \cap S_{\ell'}$. Then,

$$P_1^{i,\ell} P_{-1}^{i,\ell'} = \sum_{\alpha,\beta=1}^{m} \sum_{f|f(i)=1} \sum_{g|g(i)=-1} E_{\alpha,(\ell,f)} E_{\beta,(\ell',g)}.$$

Because f and g take different values on i, (ℓ, f) and (ℓ', g) are inconsistent, hence there is an edge in $G_{\mathscr{F}}$ between the two vertices. But then, by definition of a quantum independent set, $E_{\alpha,(\ell,f)} E_{\beta,(\ell',g)} = 0$ whenever $\alpha \neq \beta$. If $\alpha = \beta$, then since $(\ell, f) \neq (\ell', g)$, the product also vanishes so that in the end, $P_1^{i,\ell} P_{-1}^{i,\ell'} = 0$. This further implies

$$\begin{aligned}P_1^{i,\ell} &= P_1^{i,\ell}.\mathrm{Id}_{\mathscr{H}} \\ &= P_1^{i,\ell}\left(P_1^{i,\ell'} + P_{-1}^{i,\ell'}\right) \\ &= P_1^{i,\ell} P_1^{i,\ell'}.\end{aligned}$$

A similar reasoning yields $P_1^{i,\ell'} = P_1^{i,\ell} P_1^{i,\ell'}$, from which the result follows. ■

Setting

$$X_i = P_1^{i,\ell} - P_{-1}^{i,\ell}$$

for any ℓ such that $i \in S_\ell$ therefore yields a family of symmetries, and we are left with checking that they provide a quantum solution of $\mathscr{F}$. We will now prove this after properly stating the complete quantum version of THEOREM 2.2.9.

THEOREM 2.2.17 Given a LBCS $\mathscr{F}$, the following are equivalent :

i) $\mathscr{F}$ has a quantum solution

ii) The graphs $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ are quantum isomorphic ;

iii) $\alpha_q(G_{\mathscr{F}}) = m$.

Proof. The first implication was proven in THEOREM 2.2.11 while the second implication follows from **Proposition 2.2.13** together with Lemma 2.2.15. As for the third implication – from $iii)$ to $i)$ – we will now complete its proof by showing that $(X_i)_{1\leqslant i\leqslant m}$ as defined above is a quantum solution of $\mathscr{F}$.

We first check that for a fixed ℓ and $i,j \in S_\ell$, X_i and X_j commute. For that, we compute

$$\begin{aligned} P^{i,\ell}_{\epsilon} P^{j,\ell}_{\epsilon'} &= \left(\sum_{\alpha=1}^{m} \sum_{f \mid f(i)=\epsilon} E_{\alpha,(\ell,f)}\right)\left(\sum_{\beta=1}^{m} \sum_{g \mid g(j)=\epsilon'} E_{\beta,(\ell,g)}\right) \\ &= \sum_{\alpha,\beta=1}^{m} \sum_{f \mid f(i)=\epsilon} \sum_{g \mid g(j)=\epsilon'} E_{\alpha,(\ell,f)} E_{\beta,(\ell,g)} \end{aligned}$$

The product appearing above vanishes whenever $f \neq g$ because the vertices (ℓ,f) and (ℓ,g) are then adjacent in $G_{\mathscr{F}}$. Moreover, $E_{\alpha,(\ell,f)} E_{\beta,(\ell,f)}$ also vanishes if $\alpha \neq \beta$. Therefore, the sum reduces to

$$\sum_{\alpha=1}^{m} \sum_{f \mid f(i)=\epsilon, f(j)=\epsilon'} E_{\alpha,(\ell,f)}.$$

The same computation starting with $P^{j,\ell}_{\epsilon'} P^{i,\ell}_{\epsilon}$ yields the same result, hence these two projections commute, implying the commutation of the corresponding symmetries.

Second, we have to make sure that our symmetries satisfy the equations of $\mathscr{F}$. We once again fix some $1 \leqslant \ell \leqslant m$. Observe that for some fixed partial solution f, we have

$$\begin{aligned} X_i P^{i,\ell}_{f(i)} &= \left(P^{i,\ell}_{1} - P^{i,\ell}_{-1}\right) P^{i,\ell}_{f(i)} \\ &= P^{i,\ell}_{1} P^{i,\ell}_{f(i)} + P^{i,\ell}_{-1} P^{i,\ell}_{f(i)} \\ &= f(i) P^{i,\ell}_{f(i)}. \end{aligned}$$

Using this we first compute, using the notations of the proof of Lemma 2.2.16,

$$\begin{aligned} \left(\prod_{i \in S_\ell} X_i\right) Q^{\ell}_{f} &= \left(\prod_{i \in S_\ell} X_i\right)\left(\prod_{i \in S_\ell} P^{i,\ell}_{f(i)}\right) \\ &= \left(\prod_{i \in S_\ell} X_i P^{i,\ell}_{f(i)}\right) \\ &= \left(\prod_{i \in S_\ell} f(i) P^{i,\ell}_{f(i)}\right) \\ &= \left(\prod_{i \in S_\ell} f(i)\right)\left(\prod_{i \in S_\ell} P^{i,\ell}_{f(i)}\right) \\ &= (-1)^{b_\ell} Q^{\ell}_{f} \end{aligned}$$

Summing this over f, and using the fact already proven for Lemma 2.2.16 that

$$\sum_{f} Q^{\ell}_{f} = \mathrm{Id}_H,$$

then yields the desired equality. ∎

2.3 EXAMPLES

2.3.1 THE MAGIC SQUARE

We are now almost done, and our last step is to produce an explicit LBCS with no classical solution but at least one quantum solution. The simplest known example is the system (2.1) from Example 2.2.2 given above, which was introduced by N. MERMIN in [Mer90]. We already noticed that it has no classical solution by the parity argument from Example 2.2.2. As for quantum

solutions, there is an explicit one which we will now explain. First, we recall some standard operators from quantum mechanics : the *Pauli* matrices are the following elements of $\mathrm{M}_2(\mathbf{C})$

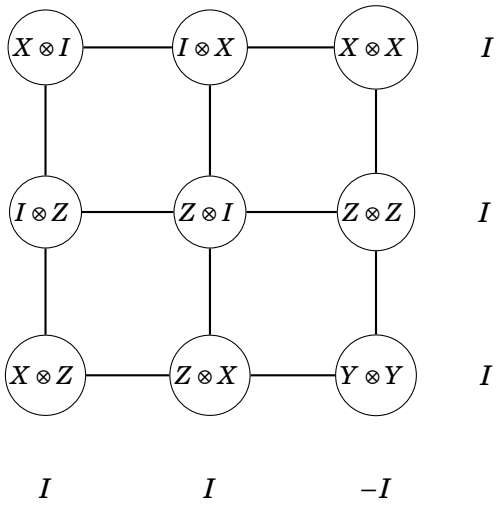
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad ; \quad Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad ; \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

They enjoy a number of nice properties and we will list just a few of them. The proof are sraightforward matrix computations and are left to the reader.

Proposition 2.3.1. *The Pauli matrices are symmetries which pairwise anti-commute. Moreover, they satisfy the identities*

$$XY = iZ$$
$$ZX = iY$$
$$YZ = iX$$

In particular, any product of two distinct Pauli matrices commutes with the third one. But to produce a quantum solution, this is not enough since we need to build nine operators with commutation properties. This is achieved by passing to tensor products of Pauli matrices. In the end, we can write down a solution in magic square form as follows, writing I for $\mathrm{Id}_{\mathbf{C}^2}$. The reader may check that each row and each column consists of pairwise commuting symmetries, and that their products have the prescribed signs.

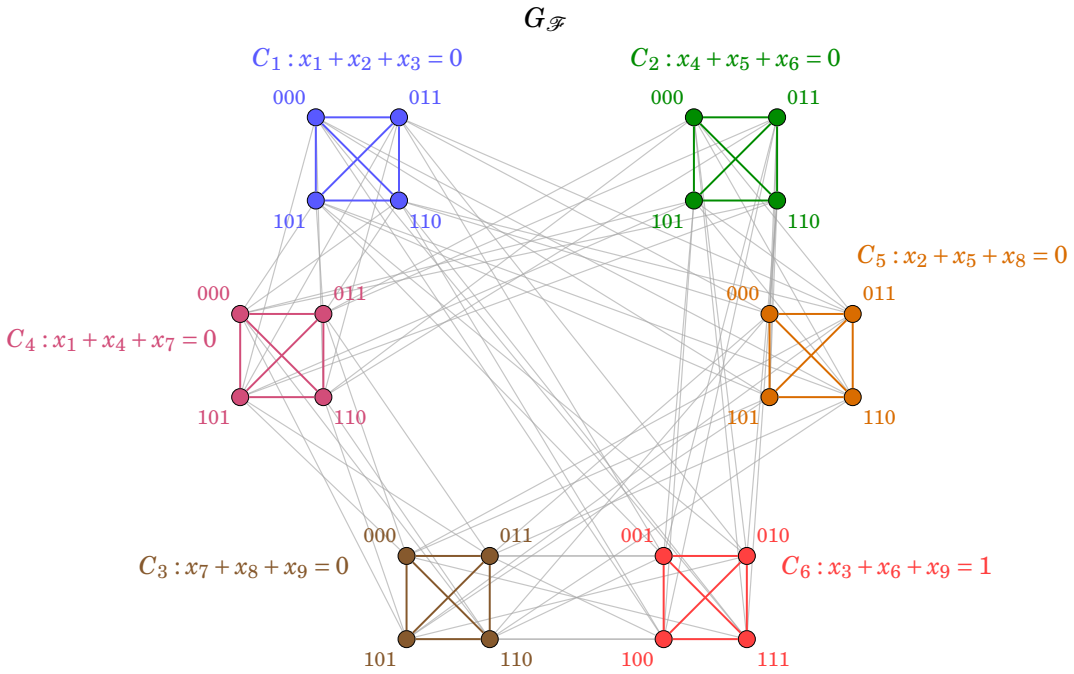


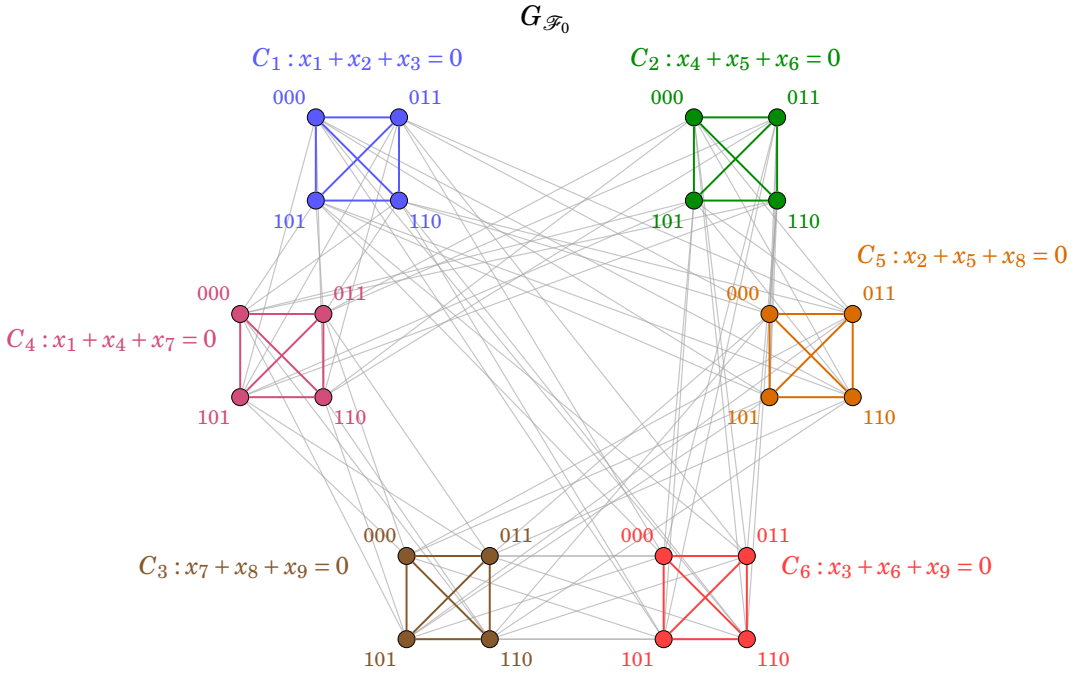
We can now prove the second main result of this lecture.

THEOREM 2.3.2 There exist two graphs which are quantum isomorphic but not isomorphic.

Proof. THEOREM 2.2.9 shows that the graphs coming from the LBCS (2.1) are not isomorphic while THEOREM 2.2.11 guarantees that they are quantum isomorphic. ■

The LBCS $\mathscr{F}$ has six equations, each of which has four possible solutions because there are three unknowns in $\mathbf{F}_2$ by definition. Therefore the graphs $G_{\mathscr{F}}$ and $G_{\mathscr{F}_0}$ have 24 vertices. To draw them, it can help to observe that each equation produces a copy of K_4 coming from its four partial solutions since two distinct local solutions cannot be consistent. This produces six such copies. Furthermore, the first five copies are connected exactly in the same way in both graphs, since the only equation which changes is the sixth one. The two graphs are shown below, with colours labelling the equations.





In the next section, we will extend the construction to produce infinitely many distinct pairs. But before that, let us comment on the connection with the four-colour theorem mentionned in the end of Lecture 1. Following the problem stated there, we are interested in finding homomorphisms from and to K_4. But it is not very difficult to see that the conditions we were looking for are indeed satisfied.

Proposition 2.3.3. *The graph $G_{\mathscr{F}_0}$ is 4-colourable and contains K_4, while the graph $G_{\mathscr{F}}$ is not 4-colourable but still contains K_4.*

Proof. As we already noticed, each equation produces a copy of K_4 in each graph so that one needs at least four colours for both. To see why this is attained for $G_{\mathscr{F}_0}$, we first give four distinct global solutions of $\mathscr{F}_0$. For $a, b \in \mathbb{F}_2$, let us set

$$(x_1, x_2, x_3) = (a, b, a+b)$$
$$(x_4, x_5, x_6) = (a, b, a+b)$$
$$(x_7, x_8, x_9) = (a, b, a+b)$$

It is a straightforward computation to check that this is a solution of $\mathscr{F}_0$. Moreover, for any equation, the four corresponding local solutions are incompatible. As a consequence, if $F_{a,b}$ denotes the solution above, we can colour the vertices of $G_{\mathscr{F}_0}$ by the unique pair (a,b) such that the vertex is the restriction of $F_{a,b}$. Any two vertices with the same colour are by definition not joined by an edge, hence we have a 4-colouring of $G_{\mathscr{F}_0}$.

Turning to $G_{\mathscr{F}}$, assume that we have a 4-colouring. Then, for each equation the corresponding four vertices have distinct colours. Pick therefore a colour and consider the six vertices with that colour. They are all pairwise compatible partial solutions, hence come from a global solution, which is impossible. Therefore, $G_{\mathscr{F}}$ is nto 4-colourable. ■

2.3.2 MORE EXAMPLES : THE ARKHIPOV CONSTRUCTION

We have constructed a pair of graphs which are quantum isomorphic but not isomorphic. To better understand what happens, it would be useful to have more examples. And in fact, the magic square is only the smallest instance of a much more general phenomenon. In this section, we will recast the previous results in a broader setting from [Ark12], in order to produce infinitely many such pairs. To start with, let G be a graph and let us pick a distinguished vertex $v^* \in V(G)$. We then define a LBCS $L(G,v^*)$ with equations indexed by $V(G)$ and variables indexed by $E(G)$ as follows :

- If $v \neq v^*$ then the corresponding equation is, with $E(G)_v$ denoting the set of edges having v as an endpoint,
$$\sum_{e \in E(G)_v} x_e = 0$$
- The equation corresponding to v^* is
$$\sum_{e \in E(G)_{v^*}} x_e = 1$$

Before studying the construction in details, let us give some examples.

Example 2.3.4 (TRIANGLE)**.** The complete graphs on one or two vertices do not yield interesting systems, hence let us consider K_3. If we take v^* to be the vertex 3, then we get

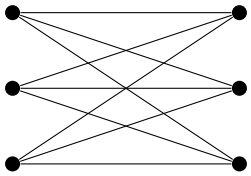
$$\begin{cases} x_{12} + x_{13} &= 0 \\ x_{12} + x_{23} &= 0 \\ x_{13} + x_{23} &= 1 \end{cases}$$

Assume that we have a quantum solution $(X_{ij})_{1 \leqslant i \neq j \leqslant 3}$ of that system. Then, $X_{12}X_{13} = I$ implies $X_{12} = X_{13}$. Similarly, $X_{12}X_{23} = I$ so that $X_{23} = X_{12} = X_{13}$. But then,

$$I = X_{13}X_{23} = -I,$$

a contradiction. Therefore, this is an example of a LBCS having neither classical nor quantum solution.

Example 2.3.5 (COMPLETE BIPARTITE GRAPH)**.** We consider now a so-called *complete bipartite graph* $K_{3,3}$. It has vertex set $\{1,\cdots,6\}$ and two vertices are connected if and only if they have different parity. This can be drawn as follows :



$K_{3,3}$

A direct computation shows that if $v^* = 6 \in V(K_{3,3})$ and if the edges are indexed from left to right and ordered lexicographically, then the associated LCBS is exactly the one from Example 2.2.2.

To better understand the system, let us check that the LCBS $L(G, v^*)$ has no classical solution.

Lemma 2.3.6. *The LCBS $L(G, v^*)$ has no classical solution.*

Proof. Because each edge has exactly two endpoints, each variable appears in exactly two equations of $L(G, v^*)$. Therefore, summing all the equations yields twice the sum of all the variables – which is 0 in $\mathbf{F}_2$ – in the left-hand side, and 1 in the right-hand side. The result follows. ■

The difficulty is now to determine whether $L(G, v^*)$ has a quantum solution. Quite surprisingly, even though the LCBS depends in general on the choice of the vertex v^*, the fact that it has quantum solutions does not! However, we will make our life simpler and just consider the problem whether there is a choice of v^* such that there is a solution. To give a sufficient criterion in that direction, we have to introduce first some extra notions from graph theory.

DEFINITION 2.3.7. A graph H is said to be a *minor* of G if H can be obtained from G by repeatedly using the following three operations :

- Deleting a vertex with all incident edges;
- Deleting an edge and keeping its two endpoints;
- Contracting an edge, i.e. deleting the edge and replacing its endpoints by a single vertex.

The key observation is that it is enough to find a nice minor to ensure the existence of quantum solutions.

Proposition 2.3.8 (QUANTUM SOLUTIONS FROM MINORS)**.** *Assume that G has a minor H for which there exists $w^* \in V(H)$ such that $L(H, w^*)$ has a quantum solution. Then, there exists $v^* \in V(G)$ such that $L(G, v^*)$ has a quantum solution.*

Proof. Let us consider a quantum solution $(X_e)_{e \in E(H)}$ of $L(H, w^*)$ on some Hilbert space $\mathscr{H}$. Our goal is to extend this to G by adding new operators for all the additional edges. For that it is enough to do it for one of the operations of Definition 2.3.7, and then repeat the procedure.

- Assume that H was obtained from G by deleting a vertex v. Then, simply set $X_e = \mathrm{Id}_{\mathscr{H}}$ for all $e \in E(G)_v$. These operators satisfy the new equation corresponding to v in $L(G, w^*)$ since $w^* \neq v$. Also, for any vertex adjacent to v in G, the corresponding equation is still satisfied since this mutiplies it by $\mathrm{Id}_{\mathscr{H}}$, which commutes with every operator. Therefore, $L(G, w^*)$ has a quantum solution.

- Assume that H was obtained from G by deleting and edge e. Then setting $X_e = \mathrm{Id}_{\mathscr{H}}$ provides a quantum solution for $L(G, w^*)$. Indeed, there are only two equations which are modified (corresponding to the endpoints of e), and they are still satisfied when multiplying by the identity (which commutes with every operator).

- Assume now that H was obtained from G by contracting and edge $e = (v, v')$ to a vertex $w \in V(H)$. Then, in G, no edge except for e is adjacent to both v and v'. Moreover, each edge with w as an endpoint, when seen in G has either v or v' as an endpoint but not both. Therefore,
$$E(H)_w = E(G)^*_v \sqcup E(G)^*_{v'}$$
where the star means that we remove the contracted edge e. Let us now consider a quantum solution for $L(H, w^*)$ and set,
$$X = \prod_{f \in E(G)^*_v} X_f \quad \& \quad Y = \prod_{f \in E(G)^*_{v'}} X_f.$$
If $w^* \neq w$, these are two symmetries whose product is $\mathrm{Id}_{\mathscr{H}}$. Then, setting $X_e = X$ provides a quantum solution for $L(G, w^*)$: the equations corresponding to v and v' are clearly satisfied, and the other ones do not involve X_e. If $w^* = w$, then $XY = -\mathrm{Id}_{\mathscr{H}}$ so that if we set $X = X_e$, we get a quantum solution for $L(G, v')$: the equation for v still yields $\mathrm{Id}_{\mathscr{H}}$ while that for v' now yields $XY = -\mathrm{Id}_{\mathscr{H}}$.

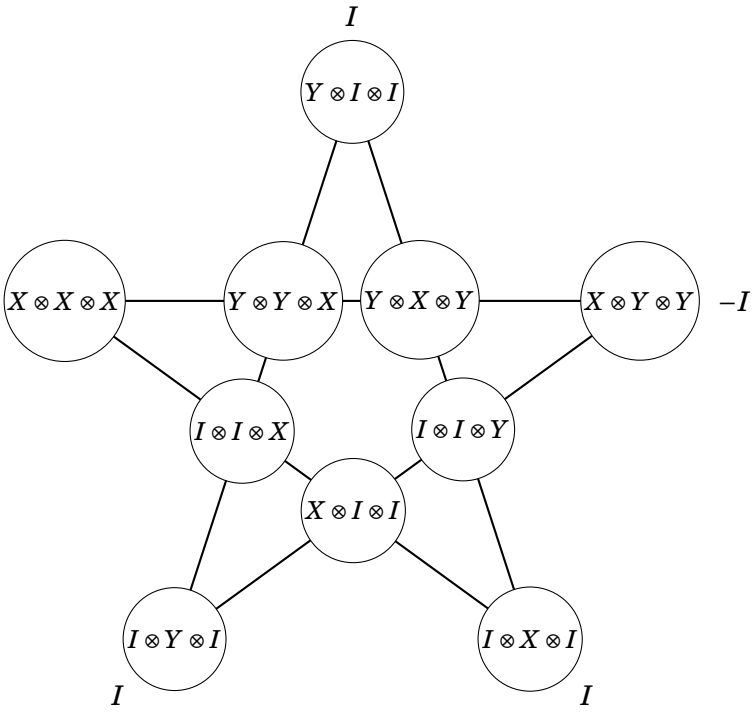
■

To produce our final criterion, we need one more example.

Example 2.3.9 (COMPLETE GRAPH AGAIN)**.** Consider the complete graph K_5 on 5 vertices. The corresponding LBCS has 5 equations and 10 variables. Denoting by x_{ij} the variable corresponding to the edge (i,j), we get for $v^* = 5$ the system

$$\begin{cases} x_{12}+x_{13}+x_{14}+x_{15} &= 0 \\ x_{12}+x_{23}+x_{24}+x_{25} &= 0 \\ x_{13}+x_{23}+x_{34}+x_{35} &= 0 \\ x_{14}+x_{24}+x_{34}+x_{45} &= 0 \\ x_{15}+x_{25}+x_{35}+x_{45} &= 1 \end{cases}$$

It turns out that one can give an explicit quantum solution to this system using once again tensor products of Pauli matrices. However, due to the number of variables, one needs to tensor at least thrice. We will show that this suffices using a generalization of the MERMIN-PERES magic square. Since this time each equation has four variables, we need a *magic pentagram* to represent them.



THEOREM 2.3.10 (ARKHIPOV'S THEOREM) For a graph G, there exists $v^* \in V(G)$ such that the LBCS $L(G,v^*)$ has a quantum solution as soon as G is not planar.

Proof. The proof consists of verifying that the hypotheses of the previous construction are satisfied. It is a deep and fundamental result of graph theory, named WAGNER'S THEOREM, that a non-planar graph always contains either $K_{3,3}$ or K_5 as a minor (see for instance [BM07, Sec 10.5] for a proof). The result therefore follows directly from **Proposition 2.3.8** and the fact that we have given explicit quantum solutions for both graphs in Examples 2.3.5 and 2.3.9 ■

Remark 2.3.11. We have a little bit more : there is always a perfect quantum strategy (hence a quantum isomorphism) using the eight-dimensional Hilbert space $\mathbf{C}^2 \otimes \mathbf{C}^2 \otimes \mathbf{C}^2$ since this is the space on which the tensor products of Pauli matrices act for K_5.

Remark 2.3.12. The original result of ARKHIPOV is stronger : if G is non-planar, then there is a quantum solution to $L(G,v^*)$ for all $v^* \in V(G)$ while if G is planar, then there is no quantum solution whatever the distinguished vertex is (see [Ark12]).

Remark 2.3.13. Even though THEOREM 2.3.10 produces infinitely many pairs of quantum isomorphic graphs which are not isomorphic, the quantum strategies provided are all built from those of Examples 2.3.5 and 2.3.9 by adding identity operators. Therefore, this does not tell us much more than the two examples in a sense.

Let us conclude by getting back to the undecidability result for quantum isomorphism mentionned in Lecture 1. Any LBCS yields a pair of graphs which are quantum isomorphic if and only the system has a quantum solution. But a deep result of W. SLOFSTRA in [Slo20] says that determining whether a LBCS has a quantum solution is undecidable. Therefore quantum isomorphism is indecidable in general.

LECTURE 3

WHEN PLANAR MEETS QUANTUM

In this lecture, we will focus on the equivalence between the second and third points in THEOREM 1.5.1. Unfortunately, it will not be possible to give complete proofs of the equivalence with quantum isomorphism because this would involve technicalities related to planar graphs which are not directly relevant to our subject. Nevertheless, we will endeavour to give an idea of why quantum isomorphism implies planar isomorphism, which is the implication underlying the connection with the FOUR-COLOUR THEOREM discussed at the end of Lecture 1. The central construction of this lecture is a graphical calculus for manipulating homomorphism counts from planar graphs.

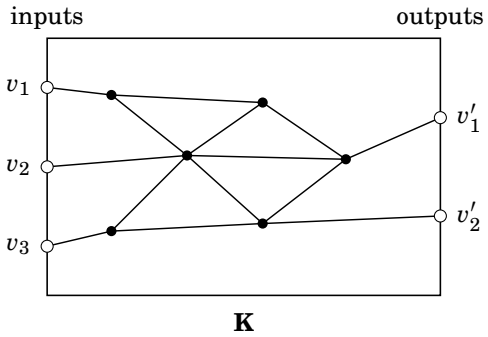
3.1 THE STRATEGY

The general strategy is to consider not just the number of homomorphisms between two graphs, but to count more precisely those sending some prescribed vertices to prescribed vertices. The following will be our working definition.

DEFINITION 3.1.1. A (k,ℓ)-*planar gadget* $\mathbf{K} = (K, \mathbf{v}, \mathbf{v}')$ is given by

- A planar graph K, drawn in a rectangle;
- A tuple of vertices $\mathbf{v} = (v_1, \cdots, v_k)$ lying on the left side of the rectangle – called the *inputs* – each of which is connected to exactly one vertex inside the rectangle;
- A tuple of vertices $\mathbf{v}' = (v'_1, \cdots, v'_\ell)$ lying on the right side of the rectangle – called the *outputs* – each of which is connected to exactly one vertex inside the rectangle.

Here is an example of a $(3,2)$-planar gadget.



As the name suggests, the specific assumptions on the rectangle and the input/output vertices are merely technical devices enabling us to work smoothly with these objects while avoiding some issues related to planarity. Ultimately however, we will mainly be interested in the part that lies inside the rectangle. Let us give it a name for convenience.

DEFINITION 3.1.2. A vertex of a planar gadget is said to be an *interior vertex* if it is not an input nor an output. The subgraph induced by interior vertices is called the *interior graph* of the gadget and denoted by $\iota(K)$.

Given a planar gadget and a fixed graph G, we can count the number of homomorphisms from K to G sending the inputs and outputs to some chosen vertices, but as we already mentioned this is not exactly the key quantity for us. To define the better suited one, let us denote, for an input vertex v (respectively for an output vertex v') by $\iota(v)$ (respectively $\iota(v')$) the unique interior vertex connected to it. As already explained, these vertices are the relevant ones, the boundary vertices being « gadgets » enabling us to easily access them. Therefore, the following definition should not surprise the reader : the gadget defines a linear map by counting homomorphisms with prescribed boundary values.

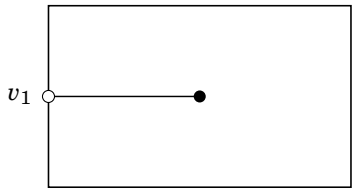
DEFINITION 3.1.3. For a (k,ℓ)-planar gadget $\mathbf{K}$ and a graph G, we set

$$\boxed{F_{\mathbf{K}}^{G}(z_1,\cdots,z_k,z'_1,\cdots,z'_\ell) = \Big|\{\phi : \iota(K) \to G \mid \phi(\iota(v_i)) = z_i, \phi(\iota(v_j)) = z'_j \text{ for all } 1 \leqslant i \leqslant k \text{ and } 1 \leqslant j \leqslant \ell\}\Big|}$$

Remark 3.1.4. If $k = 0 = \ell$, then the planar gadget is just a planar graph, and the formula reduces to the usual homomorphism count.

It will be convenient to extend $F_{\mathbf{K}}^{G}$ to a linear map from $\mathbf{C}^{V(G)^k} \to \mathbf{C}^{V(G)^\ell}$ in the form of a matrix given by the coefficients above in the canonical bases. Let us try our hands on some examples.

Example 3.1.5 (THE VERTEX GADGET)**.** Consider the complete graph K_1 with only one vertex v. We could declare v to be an input, or an output, but we then need an extra interior vertex. Instead, we will consider the complete graph K_2 and declare one vertex to be an input, while the second one stays interior. Intuitively, the relevant feature of that gadget is the internal vertex, hence we will call it the *vertex gadget* and denote it by $\mathbf{V}$.

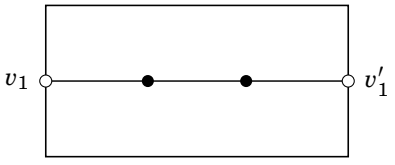


$\mathbf{V}$

One easily computes

$$\begin{aligned} F_{\mathbf{V}}^{G} w &= \sum_{w' \in V(G)} \big|\{\phi : K_1 \to G \mid \phi(v) = w'\}\big|\, w' \\ &= \sum_{w' \in V(G)} w'. \end{aligned}$$

Example 3.1.6 (THE EDGE GADGET)**.** Consider again the complete graph $K = K_2$. We could declare the two endpoints to be respectively an input and an output, but then there would be no interior vertex to connect these to. Therefore, we will once again consider instead a *path of length three*, that is to say the graph on vertex set $\{1,2,3,4\}$ with edges $(1,2)$, $(2,3)$ and $(3,4)$. We then declare 1 to be the input and 4 to be the output, and we call it the *edge gadget* and denote it by $\mathbf{E}$. The name might sound surprising, but it is meant to emphasize that the interior graph is an edge, and that is what will be important in the sequel.

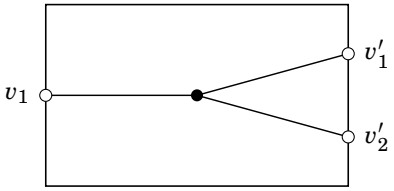


$\mathbf{E}$

Observe that for any $w \in V(G)$,

$$F_{\mathbf{E}}^{G} w = \sum_{w' \in V(G)} \left|\{\phi : K_2 \to G \mid \phi(2) = w, \phi(3) = w'\}\right| w'$$
$$= \sum_{w' \in V(G)} \delta_{(w,w') \in E(G)} w' \qquad = A_G w.$$

Example 3.1.7 (THE TRIPOD GADGET)**.** Our final example is based on a graph which is known as the *complete bipartite graph* $K_{1,3}$. Concretely, K has vertices $\{1,2,3,4\}$ and edges $(1,2)$, $(1,3)$ and $(1,4)$. To turn it into a planar gadget, we declare 2 to be an input and 3 and 4 to be outputs. We will denote this by $\mathbf{T}$ and call it the *tripod gadget*.



$\mathbf{C}$

We have

$$F_{\mathbf{T}}^{G} w = \sum_{w', w'' \in V(G)} \left|\{\phi : K_1 \to G \mid \phi(v) = w, \phi(v) = w', \phi(v) = w''\}\right| w \otimes w''$$
$$= w \otimes w.$$

This is called the *diagonal map* on $\mathbf{C}^{V(G)}$ and denoted by Δ_G.

Assume now that we have a quantum isomorphism P between two graphs G and H. We will need to enlarge it so as to be able to compare it with our operators involving tuples of vertices. This is easily done using *tensor powers*. More concretely, we will denote by $P^{\otimes k}$ the matrix with coefficients

$$P^{\otimes k}_{(w_1,\cdots,w_k),(v_1,\cdots,v_k)} = p_{w_1 v_1} \cdots p_{w_k v_k}.$$

Remark 3.1.8. We are not claiming that this is a quantum permutation matrix, and it is not one in general because a product of non-commuting projections need not be a projection.

The central result underlying the proof that quantum isomorphism implies planar isomorphism is the following formula from [MR20].

THEOREM 3.1.9 (THE INTERTWINING FORMULA) If P is a quantum isomorphism from G to H, then for any (k,ℓ)-planar gadget $\mathbf{K}$, the following intertwining relation holds :

$$\boxed{F_{\mathbf{K}}^{H} P^{\otimes \ell} = P^{\otimes k} F_{\mathbf{K}}^{G}}$$

Remark 3.1.10. The formula in THEOREM 3.1.9 is written as an equality of operator-valued matrices indexed by $V(H)^k \times V(G)^\ell$. Concretely, it means that the coefficients of the two matrices are equal as operators on $B(\mathscr{H})$. In other words, it is a concise way of writing a system of $N^{k\times\ell}$ linear equations in $B(\mathscr{H})$.

Before discussing why THEOREM 3.1.9 holds, let us first see why it is useful. Let K be a planar graph drawn in a rectangle. Attach one input vertex v and one output vertex v', both connected to the same vertex w of K chosen so that the resulting graph defines a planar gadget $\widetilde{\mathbf{K}} = (\widetilde{K}, v, v')$ (we will make this more precise in Section 3.3.2). We can then relate the homomorphism count

from K to G to the matrix $F^G_{\widetilde{\mathbf{K}}}$ by observing that

$$\begin{aligned}\left|\{\phi : K \to G\}\right| &= \left|\{\phi : \iota(\widetilde{K}) \to G\}\right| \\ &= \sum_{z\in V(G)} \left|\{\phi : \iota(\widetilde{K}) \to G \mid \phi(w) = z\}\right| \\ &= \sum_{z\in V(G)} \left|\{\phi : \widetilde{K} \to G \mid \phi(w) = z, \phi(w) = z\}\right| \\ &= \sum_{z\in V(G)} F^G_{\widetilde{\mathbf{K}}}(z,z) \\ &= \mathrm{Tr}\left(F^G_{\widetilde{\mathbf{K}}}\right)\end{aligned}$$

This reduces the problem to equality of the trace of the linear map $F_{\widetilde{\mathbf{K}}}$. But applying THEOREM 3.1.9, we know that

$$\left(F^H_{\widetilde{\mathbf{K}}}\right) P^{\otimes \ell} = P^{\otimes k} \left(F^G_{\widetilde{\mathbf{K}}}\right)$$

and because P satisfies $P^*P = \mathrm{Id}$, we can write this as

$$P^* \left(F^H_{\widetilde{\mathbf{K}}}\right) P = F^G_{\widetilde{\mathbf{K}}},$$

so that taking traces gives the result. One might be suspicious that we are applying classical matrix calculus to matrices with values in non-commutative operators, so let us check that there is indeed no issue.

Lemma 3.1.11. *Let $P \in M_N(B(\mathscr{H}))$ be a quantum permutation and let $A, B \in M_N(\mathbf{C})$ be such that $AP = PB$. Then,* $\mathrm{Tr}(A) = \mathrm{Tr}(B)$.

Proof. First, let us check that P is « unitary » in the sense that $P^*P = \mathrm{Id}$. We compute

$$\begin{aligned}(P^*P)_{ij} &= \sum_{k=1}^N (P^*)_{ik} P_{kj} \\ &= \sum_{k=1}^N p_{ki} p_{kj} \\ &= \delta_{ij} \sum_{k=1}^N p_{ki} \\ &= \delta_{ij}\, \mathrm{Id}_{\mathscr{H}}\end{aligned}$$

so that P^*P is diagonal with coefficients $\mathrm{Id}_{\mathscr{H}}$. Now, we can embed $M_N(\mathbf{C})$ into $M_N(B(\mathscr{H}))$ by mapping a scalar λ to $\lambda.\mathrm{Id}_{\mathscr{H}}$. In that way, the product is associative and P^*P is the image of $\mathrm{Id}_{M_N(\mathbf{C})}$, hence we indeed have

$$P^*AP = P^*(PB) = (P^*P)B = B.$$

Let us now compute the trace :

$$\begin{aligned}\mathrm{Tr}(B) &= \mathrm{Tr}(P^*AP) \\ &= \sum_{i,j=1}^N (P^*)_{ij} A_{jj} (P)_{ji} \\ &= \sum_{i,j=1}^N p_{ji} A_{jj} p_{ji} \\ &= \sum_{i,j=1}^N A_{jj} p_{ji} \\ &= \sum_{j=1}^N A_{jj} \sum_{i=1}^N p_{ji} \\ &= \sum_{j=1}^N A_{jj} \\ &= \mathrm{Tr}(A)\end{aligned}$$

and the proof is complete. ∎

3.2 THE BASIC OPERATIONS

We have reduced the problem to the formula in THEOREM 3.1.9, and that is when things become tricky. The general strategy is as follows :

1. Check that THEOREM 3.1.9 holds for the planar gadgets of Examples 3.1.5, 3.1.6 and 3.1.7 ;
2. Find a finite set of operations enabling us to build any planar gadget starting from the three examples above ;
3. Check that the formula in THEOREM 3.1.9 is preserved by these operations.

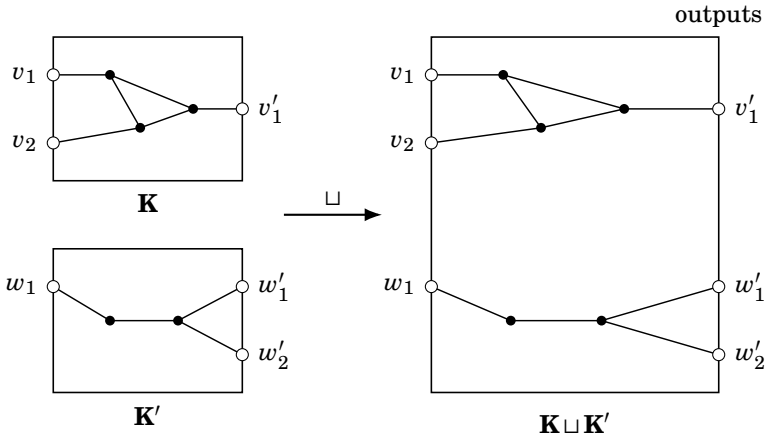
The first point is easy and will be done in Section 3.3.2. As for the second point, this is difficult and would take us far away from our main topic. We will therefore focus now on simply describing the operations that we need, and translating them at the level of the operators $F^G_{\mathbf{K}}$.

3.2.1 DISJOINT UNION

We start with a simple one. Given two planar gadgets $\mathbf{K} = (K, \mathbf{v}, \mathbf{v}')$ and $\mathbf{K}' = (K', \mathbf{w}, \mathbf{w}')$, their *disjoint union* is obtained by taking the disjoint union of the graphs and of the sets of input vertices and output vertices respectively. Formally, this yields

$$\mathbf{K} \sqcup \mathbf{K}' = (K \sqcup K', \mathbf{v} \sqcup \mathbf{w}, \mathbf{v}' \sqcup \mathbf{w}').$$

As for the rectangle, we simply draw $\mathbf{K}'$ below $\mathbf{K}$ and erase the top line of the former and the bottom line of the latter. Here is an illustration :



It is straightforward to check that this defines again a planar gadget, but what matters for us is how such a construction translates at the level of the linear maps. Fortunately, this is quite easy to describe : disjoint union corresponds to tensor product.

Lemma 3.2.1. *For any graph G and planar gadgets $\mathbf{K}$, $\mathbf{K}'$, we have the equality*

$$\boxed{F^G_{\mathbf{K} \sqcup \mathbf{K}'} = F^G_{\mathbf{K}} \otimes F^G_{\mathbf{K}'}}$$

Proof. For graphs, a homomorphism from a disjoint union is simply a pair of homomorphisms, one on each connected component. We will prove a version of that statement for planar gadgets, which then directly yields the restul. Let us write $\mathbf{v} = (v_1, \cdots, v_k)$, $\mathbf{v}' = (v'_1, \cdots, v'_\ell)$, $\mathbf{w} = (w_1, \cdots, w_{k'})$ and $\mathbf{w}' = (w'_1, \cdots, w'_{\ell'})$. Observe that $\iota(K \sqcup K') = \iota(K) \sqcup \iota(K')$ and that the map

$$\begin{array}{ccc} \mathrm{Hom}(\iota(K) \sqcup \iota(K'), G) & \to & \mathrm{Hom}(\iota(K), G) \times \mathrm{Hom}(\iota(K'), G) \\ \phi & \mapsto & (\phi_{|\iota(K)}, \phi_{|\iota(K')}) \end{array}$$

is bijective. Moreover, given $\mathbf{z} \in V(G)^k$ and $\mathbf{r} \in V(G)^\ell$, a graph homomorphism $\phi : \iota(K) \sqcup \iota(K') \to G$ sends $\iota(\mathbf{v}) \sqcup \iota(\mathbf{w})$ to $\mathbf{z} \sqcup \mathbf{r}$ if and only if $\phi_{|\iota(K)}$ sends $\iota(\mathbf{v})$ to $\mathbf{z}$ and $\phi_{|\iota(K')}$ sends $\iota(\mathbf{v}')$ to $\mathbf{r}$. The same holds for output vertices, so that in the end we have a bijection

$$\mathrm{Hom}\left(\mathbf{K} \sqcup \mathbf{K}', (G, \mathbf{z} \sqcup \mathbf{r}, \mathbf{z}' \sqcup \mathbf{r}')\right) \cong \mathrm{Hom}\left(\mathbf{K}, (G, \mathbf{z}, \mathbf{r})\right) \times \mathrm{Hom}\left(\mathbf{K}', (G, \mathbf{z}', \mathbf{r}')\right).$$

Passing to cardinalities then yields

$$F^G_{\mathbf{K}\sqcup\mathbf{K}'}(\mathbf{z}\sqcup\mathbf{r},\mathbf{z}'\sqcup\mathbf{r}') = F^G_{\mathbf{k}}(\mathbf{z},\mathbf{r}) \times F^G_{\mathbf{K}'}(\mathbf{z}',\mathbf{r}')$$

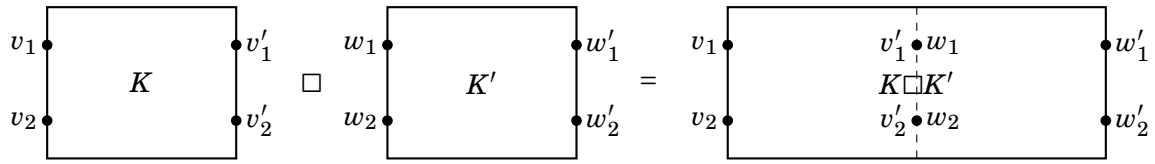
and these are exactly the coefficients of the tensor product of the linear maps. ■

3.2.2 COMPOSITION

We have just seen that we can encode the tensor product of linear maps with an operation on planar gadgets, and that raises the following question : can we also express composition at the level of planar gadgets? The answer is « yes » and is also the reason why we are carrying these input and output vertices all along. Nevertheless, a subtlety will appear here. More precisely, consider two planar gadgets $\mathbf{K} = (K, \mathbf{v}, \mathbf{v}')$ and $\mathbf{K}' = (K', \mathbf{w}, \mathbf{w}')$ such that the number of outputs of K equals the number of inputs of $\mathbf{K}'$. Let the $K\square K'$ be the graph obtained from the disjoint union $K \sqcup K'$ by gluing each output of K to an input of K'. Then the *concatenation* of $\mathbf{K}$ and $\mathbf{K}'$ is

$$\mathbf{K}\square\mathbf{K}' = (K\square K', \mathbf{v}, \mathbf{w}').$$

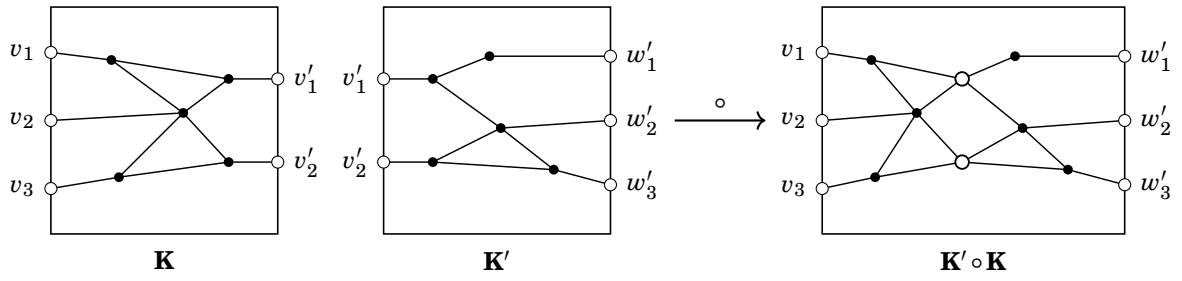
We are obviously sweeping something under the rug here : why is it possible to chose a pairing between the inputs and outputs such that the resulting graph is still planar? This is exactly where the rectangles play their role. If we draw the two rectangles next to one another, then we just glue the sides and this does not produce any crossing!



If we call that operation *concatenation* instead of *composition*, it is because it is not the correct gadget-theoretic translation of the composition of linear maps. The reason for that is that the output vertices of $\mathbf{K}$, once merged with the input vertices of $\mathbf{K}'$ remain in the resulting graph. This is in contradiction with our claim that the boundary vertices are just gadgets and should not be considered part of the graph. The correct definition is then clear : we have to remove these extra vertices.

DEFINITION 3.2.2. The *composition* of two planar gadgets $\mathbf{K} = (K, \mathbf{v}, \mathbf{v}')$ and $\mathbf{K}' = (K', \mathbf{w}, \mathbf{w}')$ is the planar gadget $\mathbf{K} \circ \mathbf{K}'$ obtained from $\mathbf{K}\square\mathbf{K}'$ by erasing the vertices coming from outputs of $\mathbf{K}$ (or equivalently inputs of $\mathbf{K}'$) and identifying the interior vertices incident to these. In other words, we merge $\iota(v'_j)$ and $\iota(w_j)$ for all $1 \leqslant j \leqslant \ell$.

Let us give an example to illustrate the operation. We indicate with white circles the interior vertices obtained by contracting the edges.



The composition procedure has one potential drawback : two interior vertices might get merged in the process, thereby creating loops or multiple edges. This means that our use of the term *graph* is not in accordance with the conventions of the text. However, this does not give rise to any issue in the sequel. Indeed, we are only interested in counting homomorphisms $\iota(K) \to G$ with G not containing loops or multiple edges. Such homomorphisms do not exist if there is a loop in $\iota(K)$. If there is a multiple edge, then any homomorphism "factors" through the graph obtained by merging these multiple edges into a single one.

With this, we can now prove our expected relation at the level of linear maps.

Proposition 3.2.3. *For any graph G, any (k,ℓ)-planar gadget $\mathbf{K}$ and any (ℓ,m)-planar gadget $\mathbf{K}'$,*

$$\boxed{F^G_{\mathbf{K}\circ\mathbf{K}'} = F^G_{\mathbf{K}} \circ F^G_{\mathbf{K}'}}$$

Proof. Let us denote by $\mathbf{v}'$ the outputs of $\mathbf{K}$ and by $\mathbf{w}$ the inputs of $\mathbf{K}'$. We fix tuples $\mathbf{z} \in V(G)^k$ and $\mathbf{z}' \in V(G)^m$, and for a homomorphism ϕ from $\mathbf{K}\circ\mathbf{K}'$ to $(G,\mathbf{z},\mathbf{z}')$, we consider its restrictions $\phi_{|\iota(K)}$ and $\phi_{|\iota(K')}$. Then, setting

$$\mathbf{z}'' = \phi(\iota(\mathbf{v}')) = \phi(\iota(\mathbf{w})),$$

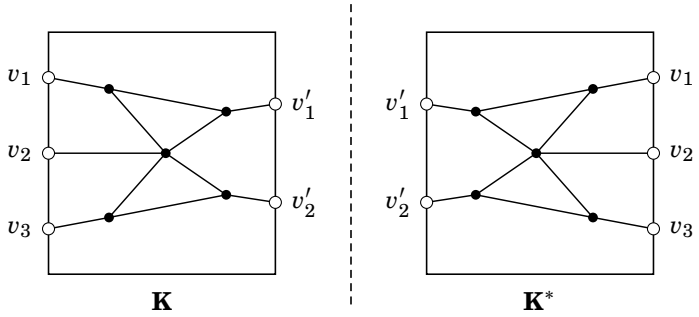
$\phi_{|\iota(K)}$ is a graph homomorphism from $\mathbf{K}$ to $(G,\mathbf{z},\mathbf{z}'')$ while $\phi_{|\iota(K')}$ is a graph homomorphism from $\mathbf{K}'$ to $(G,\mathbf{z}'',\mathbf{z}')$. Conversely, for any choice of $\mathbf{z}'' \in V(G)^\ell$ and any graph homomorphisms $\phi_1 : \mathbf{K} \to (G,\mathbf{z},\mathbf{z}'')$ and $\phi_2 : \mathbf{K}' \to (G,\mathbf{z},\mathbf{z}'')$, there is a unique graph homomorphism $\phi : \mathbf{K}\circ\mathbf{K}' \to (G,\mathbf{z},\mathbf{z}')$ such that $\phi_{|\mathbf{K}} = \phi_1$ and $\phi_{|\mathbf{K}'} = \phi_2$. Therefore,

$$\begin{aligned} F^G_{\mathbf{K}\circ\mathbf{K}'}(\mathbf{z},\mathbf{z}') &= \sum_{\mathbf{z}''\in V(G)^\ell} F^G_{\mathbf{K}}(\mathbf{z},\mathbf{z}'')F^G_{\mathbf{K}'}(\mathbf{z}'',\mathbf{z}') \\ &= \left(F^G_{\mathbf{K}} \circ F^G_{\mathbf{K}'}\right)(\mathbf{z},\mathbf{z}'). \end{aligned}$$

■

3.2.3 REFLECTION

We conclude with a simple operation. Given a planar gadget $\mathbf{K} = (K,\mathbf{v},\mathbf{v}')$, we can reflect the rectangle drawing with respect to a vertical line, and this produces an isomorphic graph, but with inputs and outputs exchanged. The interior graph is not changed (up to isomorphism) by that operation and planarity is obviously preserved, so that this defines a new planar gadget $\mathbf{K}^* = (K,\mathbf{v}',\mathbf{v})$. Here is an example :



Once again, the operator translation is straightforward : reflection corresponds to taking adjoints.

Proposition 3.2.4. *For any graph G,*

$$\boxed{F^G_{\mathbf{K}^*} = \left(F^G_{\mathbf{K}}\right)^*}$$

Proof. By definition we have

$$\begin{aligned} F^G_{\mathbf{K}^*}(\mathbf{z},\mathbf{z}') &= \left|\left\{\phi : \iota(K) \to G \mid \phi(\iota(\mathbf{v}')) = \mathbf{z}, \phi(\iota(\mathbf{v})) = \mathbf{z}'\right\}\right| \\ &= F^G_{\mathbf{K}}(\mathbf{z}',\mathbf{z}) \end{aligned}$$

and the result follows since the matrices have real coefficients. ■

3.3 GADGET CALCULUS

We will now use the operations introduced above to sketch a proof of the fact that quantum isomorphism implies planar isomorphism. As we already mentioned, the strategy is simple : starting from the elementary gadgets, we reconstruct arbitrary planar gadgets using disjoint union, composition and reflection. The key fact is therefore that these operations preserve the intertwining relation of THEOREM 3.1.9.

3.3.1 THE INTERTWINING PROPERTY

Before turning to the proof of THEOREM 3.1.9, we will isolate some computational results so as to keep the arguments clear afterwards. We have already translated the basic operations on planar gadgets into operations on linear maps. Our goal is to check that these operations are compatible with the intertwining equation of THEOREM 3.1.9, so that we can prove that it holds using decomposition of gadgets into smaller pieces. The verification is entirely formal

Proposition 3.3.1. *Let $P \in M_N(B(\mathscr{H}))$ be a quantum permutation matrix and let*

$$A, B : \mathbf{C}^{N^k} \to \mathbf{C}^{N^\ell}.$$

Suppose that

$$AP^{\otimes k} = P^{\otimes \ell} B.$$

Then,

1. *If $A', B' : \mathbf{C}^{N^{k'}} \to \mathbf{C}^{N^{\ell'}}$ satisfy $A'P^{\otimes k'} = P^{\otimes \ell'} B'$, then*
$$(A \otimes A')P^{\otimes(k+k')} = P^{\otimes(\ell+\ell')}(B \otimes B').$$
2. *If $A', B' : \mathbf{C}^{N^{k'}} \to \mathbf{C}^{N^{k}}$ satisfy $A'P^{\otimes k'} = P^{\otimes k} B'$, then*
$$(A \circ A')P^{\otimes k'} = P^{\otimes \ell}(B \circ B').$$
3. $A^* P^{\otimes \ell} = P^{\otimes k} B^*$.

Proof. We will prove the assertions one by one.

1. We simply compute
$$\begin{aligned}(A \otimes A')P^{\otimes(k+k')} &= (AP^{\otimes k}) \otimes (A'P^{\otimes k'}) \\ &= (P^{\otimes \ell} B) \otimes (P^{\otimes \ell'} B') \\ &= P^{\otimes(\ell+\ell')}(B \otimes B').\end{aligned}$$
2. Similarly
$$\begin{aligned}(A \circ A')P^{\otimes k'} &= A\left(A'P^{\otimes k}\right) \\ &= A\left(P^{\otimes k} B'\right) \\ &= \left(AP^{\otimes k}\right) B' \\ &= \left(P^{\otimes \ell} B\right) B' \\ &= P^{\otimes \ell}(B \circ B').\end{aligned}$$
3. Taking adjoints yields
$$\left(P^{\otimes k}\right)^* A^* = B^* \left(P^{\otimes \ell}\right)^*$$
but recalling that $PP^* = P^*P = \mathrm{Id}_N$ (see the proof of Lemma 3.1.11), we get when multiplying by $P^{\otimes k}$ on the left and $P^{\otimes \ell}$ on the right
$$A^* P^{\otimes \ell} = P^{\otimes k} B^*.$$

■

3.3.2 CRAFTING GADGETS

It therefore remains to show that every planar gadget can indeed be built from the elementary ones. This is a deep result from [MR20], and the proof is long and involved. It goes beyond the scope of these lectures, so that we will simply give a sketch of how one can proceed. Let us first give a formal statement.

THEOREM 3.3.2 Any planar gadget can be obtained from **V**, **E** and **T** using disjoint unions, composition and reflection.

Proof. The proof proceeds by induction, but it is intricate and requires both care and heavy notation to be able to produce rigorous arguments. We will not give it because this would require too much space and time. Let us simply mention that our planar gadgets are almost the same as the graphs K° produced out of a *bi-labelled planar graph* in the work [MR20]. Therefore, our theorem is in some sense a restatement of [MR20, Theorem 6.7] and the proof of the latter can be adapted to our setting.

Even though we do not provide a complete proof, let us roughly explain how things work. The basic planar gadgets are tools for the following operations :

- Disjoint union with **V** adds new inner vertices ;
- Composition with **E** allows one to add edges between inner vertices ;
- This can only produce graphs with degree at most 2, and **T** enables to further increase the degree of inner vertices ;
- Composition with **V** removes outer vertices without changing the inner graph.

The reader is invited to try their hands on a few examples to convince themselves that this works. ■

With this in hand, we can complete the proof of Theorem 3.1.9.

Proof of Theorem 3.1.9. In view of THEOREM 3.3.2, it is enough to prove that the linear maps associated to **V**, **E** and **T**, satisfy the intertwining property, and that the basic operations preserve intertwining. The second point was already checked in **Proposition 3.3.1**, hence we focus on the examples.

We start with **V**. In that case, we have seen in Example 3.1.5 that $F^G_{\mathbf{V}}(v) = 1$ for all $v \in V(G)$. This commutes with any quantum permutation since

$$\begin{aligned}\left(PF^G_{\mathbf{V}}\right)_{wv} &= \sum_{z\in V(G)} P_{wz} \\ &= \mathrm{Id}_{\mathscr{H}} \\ &= \sum_{z\in V(H)} P_{zv} \\ &= \left(F^H_{\mathbf{V}}P\right)_{wv}.\end{aligned}$$

Turning to **E**, we know from Example 3.1.6 that $F^G_{\mathbf{E}} = A_G$ is the adjacency matrix of G, which commutes with P by definition. The last case is the tripod gadget **T**, which gives rise to the *diagonal map* $\Delta_G : w \mapsto w \otimes w$ by Example 3.1.7. We compute

$$\begin{aligned}\left(P^{\otimes 2}\Delta_G\right)_{w\otimes w',v} &= \left(P^{\otimes 2}\right)_{w\otimes w',v\otimes v} \\ &= P_{wv}P_{w'v} \\ &= \delta_{w,w'}P_{wv} \\ &= \sum_{w''\in V(H)} (\Delta_H)_{w\otimes w',w''}P_{w'',v} \\ &= (\Delta_H P)_{w\otimes w',v}.\end{aligned}$$

■

We can – at last ! – understand the connection between quantum isomorphism and planar isomorphism.

Corollary 3.3.3. *If G and H are quantum isomorphic, then they are planar isomorphic.*

Proof. The only missing piece is the procedure for splitting a vertex of a planar graph in order to produce a planar gadget as outlined in Section 3.1. We will first do this for a *connected* planar graph K, that is to say one for which there is a path of edges between any two vertices. Such a graph can, by definition, be drawn in the plane so as to avoid crossings of edges. Moreover, the edges are straight lines, hence by Jordan's curve theorem the complement of K is a disjoint union of open sets of the plane, exactly one of which is unbounded : it is called the *outer face*. Now take a vertex v bounding the outer face, and create two new boundary vertices $\widetilde{v}$ and $\widetilde{v}'$ lying in the interior of the unbounded component. Then, one can connect v to these two without crossing K. Finally, draw a rectangle with $\widetilde{v}$ on the left-hand side and $\widetilde{v}'$ on the right-hand side. If K is not connected, then it is the disjoint union of its *connected component*. Simply apply the previous construction to one connected component, and move the remaining connected components if necessary. ■

3.4 CLOSING THE CYCLE

There is still one piece of THEOREM 1.5.1 missing : the fact that planar isomorphism implies the existence of a perfect quantum strategy, or equivalently quantum isomorphism. Even though we now have the powerful tool of planar gadgets and their graphical calculus, will once again have to remain elusive at one point. Nevertheless, we will give an almost complete picture of the proof.

3.4.1 YET ANOTHER ISOMORPHISM

The starting point is to take a closer look at the linear maps which *intertwine* the adjacency matrices, in the sense that

$$TP^{\otimes \ell} = P^{\otimes k}T.$$

These were crucial in the previous sections, because linear maps coming from planar gadgets do satisfy the intertwining property. We will now go the other way round and start from the intertwining relation. More precisely, for a single graph G, we will consider the maps satisfying that identity for A_G on both sides.

DEFINITION 3.4.1. For a graph G and two integers $k, \ell \in \mathbf{N}$, we set

$$\mathfrak{C}_G(k,\ell) = \left\{ T : \left(\mathbf{C}^{V(G)}\right)^{\otimes k} \to \left(\mathbf{C}^{V(G)}\right)^{\otimes \ell} \mid TP^{\otimes \ell} = P^{\otimes k}T \text{ for all } P \right\},$$

where P ranges over all quantum automorphisms of G (i.e. quantum isomorphisms from G to itself).

Remark 3.4.2. The correct mathematical object to consider here is a *category* $\mathfrak{C}_G$ with objects given by the integers and morphism spaces given by $\mathfrak{C}_G(k,\ell)$. It can then be « completed » in a natural way to produce a so-called *rigid C*-tensor category*. That is precisely the structure needed to make the connection with the theory of compact quantum groups.

A byproduct of the results of Section 3.3.2 is that for any (k,ℓ)-planar gadget $\mathbf{K}$, $F_G^K \in \mathfrak{C}_G(k,\ell)$. The converse cannot hold, because $\mathfrak{C}_G(k,\ell)$ is a vector space while the sum of the maps associated to two planar gadgets need not come from a planar gadget again. This is however easy to bypass by taking linear spans.

Proposition 3.4.3. *For any graph G and any integers $k, \ell \in \mathbf{N}$,*

$$\mathfrak{C}_G(k,\ell) = \mathrm{Span}\left\{ F_{\mathbf{K}}^G \mid \mathbf{K} \text{ is a } (k,\ell)-\text{planar gadget} \right\}.$$

Proof. We have already mentioned that the inclusion of the righ-hand side into the left-hand side follows from our previous results. The converse inclusion is subtler, though intuitive. Indeed, we can try to describe the axioms of a quantum automorphism in terms of commuting with some linear maps. For instance, the relation involving the adjacency matrix A_G is already a commutation relation with $F_{\mathbf{E}}^G$. Similarly, we have shown in the proof of THEOREM 3.1.9 that P commutes with Δ_G if and only if its coefficients are projections. We have also shown that commuting with $F_{\mathbf{V}}^G$ encodes the fact that the projections add up to one on columns. Using the commutation with

the adjoints of these maps, we conclude the following fact : P is a quantum automorphism if and only if it commutes with the linear maps associated to the basic gadgets and their adjoints.

The conclusion of the proof requires results beyond our scope, which can be stated as follows : $\mathfrak{C}_G(k,\ell)$ is in a sense the « smallest » space of linear maps which can be built from the ones encoding the quantum automorphism property – the basic planar gadgets – and which is closed under tensor products, composition and taking adjoints (because these operations obviously preserve the commutation relation). This is of course implies the converse inclusion. ■

Remark 3.4.4. The precise machinery needed in the proof is the *Tannaka-Krein-Woronowicz* duality, which enables to reconstruct a nice object – a *compact quantum group* – out of $\mathfrak{C}_G$.

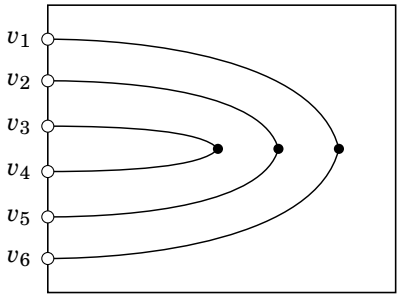
We will now use $\mathfrak{C}_G$ as an intermediate step between planar and quantum isomorphism. However, doing this is not straightforward, since the maps $F^G_{\mathbf{K}}$ involve homomorphism counts from planar gadgets and not just planar graphs. We therefore need to relate these two quantities. The simplest solution would be to remove the boundary points, but what do we do with their corresponding interior vertices? They should be merged in some way like when boundary points are erased in composition. The technique for that is a kind of « closure » operation. Intuitively, for a (k,k)-planar gadget, we want to connect each input vertex v_i to the output vertex v'_i, so that no crossing is produced in the process, and then contract the edges. We however have to do this using only our basic operations, and the following gadgets will come in handy for that purpose.

DEFINITION 3.4.5. The *identity gadget* is the $(1,1)$-planar gadget $\mathbf{I} = \mathbf{E}\circ\mathbf{V}$. The *n-th pairing gadget* is the planar gadget $\mathbf{P}_n$ with n internal vertices, $2n$ inputs and no outputs. The inputs v_i and v_{2n-i+1} being both connected to the i-th internal vertex.

More formally, we have $\mathbf{P}_1 = (\mathbf{V}\circ\mathbf{C})^*$. From this we can build the other pairing gadgets inductively through the formula

$$\mathbf{P}_{n+1} = (\mathbf{I}\sqcup\mathbf{P}_n\sqcup\mathbf{I})\circ\mathbf{P}.$$

Here is an illustration for $n = 3$.



$\mathbf{P}_3$

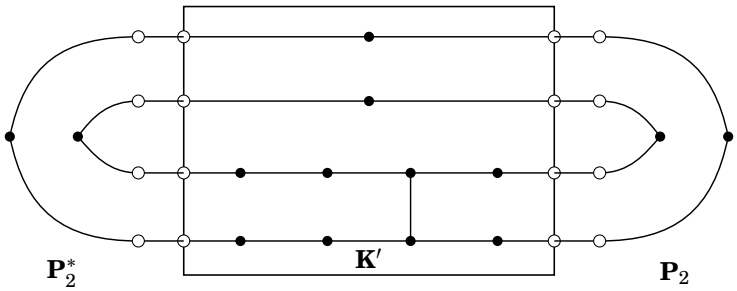
We can now define the closure operation.

DEFINITION 3.4.6. Let $\mathbf{K}$ be a (k,k)-planar gadget. Its *closure* is the planar gadget

$$c(\mathbf{K}) = C_k^*\circ\left(\mathbf{I}^{\sqcup k}\sqcup\mathbf{K}\right)\circ C_k.$$

It is a $(0,0)$-planar gadget, hence just a planar graph.

There is nothing better than an example :



$c(\mathbf{K}') = \mathbf{P}_2^*\circ\left(I\sqcup I\sqcup\mathbf{K}'\right)\circ\mathbf{P}_2$

produces the planar graph

$c(\mathbf{K}')$

Our motivation is to relate the maps associated to planar gadgets to homomorphism counts from planar graphs. It turns out that this is precisely what the closure operation does. Let us prove this.

Lemma 3.4.7. *For any (k,k)-planar gadget $\mathbf{K}$, we have*

$$\boxed{\mathrm{Hom}(c(\mathbf{K}),G) = \mathrm{Tr}\left(F^G_{\mathbf{K}}\right)}$$

Proof. First observe that for any graph G, $F^G_{\mathbf{I}} = \mathrm{Id}_{V(G)}$ and

$$F^G_{\mathrm{P}_n}(v_1 \otimes \cdots \otimes v_{2n}) = \prod_{i=1}^{n} \delta_{v_i, v_{2n-i+1}}.$$

Moreover, since $c(\mathbf{K})$ is a $(0,0)$-gadget, the corresponding linear map is just a scalar, which equals by **Proposition 3.2.3**

$$\begin{aligned} F^G_{c(\mathbf{K})} &= \sum_{z_1,\cdots,z_{2k}} \sum_{z'_1,\cdots,z'_{2k}} F^G_{\mathbf{K}}((z_1,\cdots,z_k),(z'_{k+1},\cdots,z'_{2k})) \prod_{i=1}^{k} \delta_{z_i, z_{2k-i+1}} \prod_{i=1}^{k} \prod_{i=1}^{n} \delta_{z'_i, z'_{2k-i+1}} \prod_{i=1}^{k} \delta_{z_i, z'_i} \\ &= \sum_{z_1,\cdots,z_k} F^G_{\mathbf{K}}((z_1,\cdots,z_k),(z_1,\cdots,z_k)) \\ &= \mathrm{Tr}\left(F^G_{\mathbf{K}}\right). \end{aligned}$$

On the other hand, the scalar $F^G_{c(\mathbf{K})}$ is also given by homomorphism counts, with no restrictions on the vertices since there is no input and no output. In other words,

$$F^G_{c(\mathbf{K})} = |\mathrm{Hom}\,(c(\mathbf{K}),G)|$$

hence the result. ■

Now, how can we use this to understand planar isomorphism? The key is to make a detour through another notion of graph isomorphism, involving the sets $\mathfrak{C}_G(k,\ell)$. Here is a definition to make things clearer.

DEFINITION 3.4.8. Two graphs G and H are said to be *gadget isomorphic* if there exist linear isomorphisms

$$\Phi_{k,\ell} : \mathfrak{C}_G(k,\ell) \to \mathfrak{C}_H(k,\ell)$$

for all $k,\ell \in \mathbf{N}$ such that for any (k,ℓ)-planar gadget $\mathbf{K}$,

$$\Phi_{k,\ell}\left(F^G_{\mathbf{K}}\right) = F^H_{\mathbf{K}}.$$

Remark 3.4.9. At first sight, this notion appears stronger than planar isomorphism and weaker than quantum isomorphism. The remainder of the lecture shows that it is in fact equivalent to both.

We can now give the intermediate result needed to relate planar isomorphism to quantum isomorphism.

Proposition 3.4.10. *If two graphs are planar isomorphic, then they are gadget isomorphic.*

Proof. The statement means that the knowledge of the homomorphism counts from planar graphs is enough at least to reconstruct all the combinatorics of homomorphism counts from planar gadgets. To prove it, we look at the situation from a higher point of view : define $\mathfrak{C}(k,\ell)$ to be the vector space with basis given by all (k,ℓ)-planar gadgets. Then, there exist by definition for each graph G a surjective linear map $F^G : \mathfrak{C}(k,\ell) \to \mathfrak{C}_G(k,\ell)$ sending the basis element $\mathbf{K}$ to $F^G_{\mathbf{K}}$. Let now G and H be planar isomorphic. We claim that this implies

$$\ker(F^G) = \ker(F^H).$$

This allows to factor both maps into isomorphism with the same initial space, hence through composition we get the desired isomorphism.

To prove the equality of the kernels, we first slightly improve Lemma 3.4.7 : for two (k,ℓ)-planar gadgets $\mathbf{K}$ and $\mathbf{K}'$, we can then form the (ℓ,ℓ)-planar gadget $\mathbf{K}^* \circ \mathbf{K}'$, take its closure and compute

$$\begin{aligned}\mathrm{Tr}\left((F^G_{\mathbf{K}})^* F^G_{\mathbf{K}'}\right) &= \mathrm{Hom}(c(\mathbf{K}^* \circ \mathbf{K}'), G)\\ &= \mathrm{Hom}(c(\mathbf{K}^* \circ \mathbf{K}'), H)\\ &= \mathrm{Tr}\left((F^H_{\mathbf{K}})^* F^H_{\mathbf{K}'}\right)\end{aligned}$$

Consider therefore (k,ℓ)-planar gadgets $\mathbf{K}_1,\cdots,\mathbf{K}_n$ and scalars $\lambda_1,\cdots,\lambda_n \in \mathbf{C}$ such that

$$T_G = \sum_{i=1}^n \lambda_i F^G_{\mathbf{K}_i} = 0.$$

Set

$$T_H = \sum_{i=1}^n \lambda_i F^H_{\mathbf{K}_i}$$

and compute

$$\begin{aligned}\mathrm{Tr}\left(T_H^* T_H\right) &= \sum_{i,j=1}^n \overline{\lambda}_i \lambda_j \mathrm{Tr}\left((F^H_{\mathbf{K}_i})^* F^H_{\mathbf{K}_j}\right)\\ &= \sum_{i,j=1}^n \overline{\lambda}_i \lambda_j \mathrm{Tr}\left((F^G_{\mathbf{K}_i})^* F^G_{\mathbf{K}_j}\right)\\ &= \mathrm{Tr}\left(T_G^* T_G\right)\\ &= 0.\end{aligned}$$

This forces $T_H = 0$, hence $\ker(F^G) \subset \ker(F^H)$. Since planar isomorphism is a symmetric relation, we also have the converse inclusion, hence the result. ■

We have now replaced quantum isomorphism by an equivalent family of linear maps preserving the gadget calculus. The remaining question is whether these linear maps still retain enough combinatorial information to reconstruct a quantum permutation. The final ingredient for that is what we call the *orbits trick*.

3.4.2 THE ORBITS TRICK

The last step is to go from gadget isomorphism to quantum isomorphism. There, the intuition comes from a more geometric point of view exploiting the (quantum) symmetries of graphs. It is crucial to understand the classical concepts in order to see how they can be extended to our setting, hence we recall a few elementary facts. Our central concept will be that of an *orbit* of a graph. Formally, this is just an orbit of $V(G)$ under the action of the automorphism group of G, but a more down-to-earth description is sometimes more useful.

DEFINITION 3.4.11. For $v,w \in V(G)$, we set $v \sim w$ if there is an automorphism ϕ of G such that $\phi(v) = w$. This is an equivalence relation, and its equivalence classes are the orbits of G.

Writing ϕ as the matrix with coefficients $P(\phi)_{wv} = \delta_{w\phi(v)}$, we see that the condition $\phi(v) = w$ is equivalent to $P(\phi)_{wv} \neq 0$. This leads us to a quantum version of our previous binary relation.

DEFINITION 3.4.12. We define a binary relation $\sim_q$ on $V(G)$ by setting $v \sim_q w$ if $P_{wv} \neq 0$ for some quantum automorphism P of G.

For this to be interesting and even useful, it would be good that $\sim_q$ defines an equivalence relation. Let us check that.

Lemma 3.4.13. *The relation $\sim_q$ is an equivalence relation on $V(G)$. The equivalence classes are called the* quantum orbits *of G.*

Proof. First, the matrix Id_N is a quantum automorphism, hence $v \sim_q v$ for all $v \in V(G)$, proving reflexivity. Moreover, if P is a quantum automorphism, then so is P^*, hence $\sim_q$ is symmetric. As for transitivity, consider $v, w, z \in V(G)$ and quantum automorphisms P and Q such that $P_{wv} \neq 0$ and $Q_{zw} \neq 0$. We have already seen in the proof of **Proposition 1.3.8** that setting

$$r_{ab} = \sum_{c \in V(G)} q_{ac} \otimes p_{cb}$$

defines a new quantum automorphism of G. Moreover, each coefficient is a sum of pairwise orthogonal projections, hence is non-zero as soon as one of the summands is non-zero. But R_{zv} has $Q_{zw} \otimes P_{wv}$ as a summand, hence the result. ∎

The notion of orbit enables to characterize graph isomorphism in a slightly convoluted way which will prove useful for us. Indeed, consider two graphs G and H. Both their automorphism groups can be embedded into the automorphism group of their disjoint union $G \sqcup H$ by fixing the other graph. Moreover, any isomorphism $\phi : G \to H$, also yields an automorphism of $G \sqcup H$: send $v \in V(G)$ to $\phi(v)$ and $w \in V(H)$ to $\phi^{-1}(w)$. A direct consequence is that v and w are now in the same orbit of $G \sqcup H$! The converse of that assertion does not hold in general, unless we make an extra assumption.

DEFINITION 3.4.14. A graph G is said to be *connected* if for any $v, w \in V(G)$, there exists an integer n and vertices $v_1, \cdots, v_n$ such that

- $v_1 = v$;
- $v_n = w$;
- $(v_i, v_{i+1}) \in E(G)$ for all $1 \leqslant i \leqslant n-1$.

Remark 3.4.15. As the name suggests, a graph is connected if any two vertices can be joined through a path.

Proposition 3.4.16. *Let G and H be connected graphs. Then, G is isomorphic to H if and only if there exists a vertex $v \in V(G)$ and a vertex $w \in V(H)$ which are in the same orbit of $G \sqcup H$.*

Proof. The fundamental observation is that the image of a connected graph under a graph homomorphism is again connected. Let ϕ be an automorphism of $G \sqcup H$ sending v to w. Then, $\phi(V(G))$ defines a connected subgraph of $G \sqcup H$ which contains w, hence $\phi(V(G)) \subset V(H)$. Injectivity of ϕ then implies $|V(G)| \leqslant |V(H)|$. Applying the same reasoning to ϕ^{-1}, we conclude that G and H have the same number of vertices and that ϕ induces a bijection between $V(G)$ and $V(H)$, concluding the proof. ∎

The strategy of [MR20] to prove that gadget isomorphism implies quantum isomorphism builds on that idea, through the following result [LMR20, Thm 4.5].

> **THEOREM 3.4.17** Let G and H be connected graphs. Assume that there exist $v \in V(G)$ and $w \in V(H)$ which are in the same quantum orbit of $G \sqcup H$. Then, G and H are quantum isomorphic.

For the sake of completeness, we will give a proof of that result before proceeding further. The argument relies on a variation of **Proposition 1.3.7**.

Lemma 3.4.18. *Let G and H be two finite graphs with G* connected*, and let P be a quantum automorphism of $G \sqcup H$. If $v, v', v'' \in V(G)$ and $w \in V(H)$, then*

$$P_{v''v} P_{wv'} = 0.$$

Proof. Because G is connected, there is a finite path $v_0 = v, v_1, \cdots, v_n = v'$ connecting v to v', i.e. such that $(v_i, v_{i+1}) \in E(G)$ for all $1 \leqslant i \leqslant n-1$. Thus,

$$\begin{aligned} P_{v''v} P_{wv'} &= P_{v''v} \left(\sum_{z \in V(G) \sqcup V(H)} P_{zv_1} \right) \cdots \left(\sum_{z \in V(G) \sqcup V(H)} P_{zv_{n-1}} \right) P_{wv'} \\ &= P_{v''v} \left(\sum_{z_1, \cdots z_n \in V(G) \sqcup V(H)} P_{z_1 v_1} \cdots P_{z_{n-1} v_{n-1}} \right) P_{wv'} \end{aligned}$$

Let us consider one tuple $z_1, \cdots, z_{n-1} \in V(G) \sqcup V(H)$. Because $v'' \in V(G)$ and $w \in V(H)$ there exists an index $0 \leqslant m \leqslant n-1$ such that $z_m \in V(G)$ and $z_{m+1} \in V(H)$ (with the convention that $z_n = y$). But then, $(v_m, v_{m+1}) \in V(G) \subset V(G) \sqcup V(G) \sqcup V(H) = V(G \sqcup H)$ while by definition of the disjoint union of graphs, $(z_m, z_{m+1}) \notin V(G \sqcup H)$. We therefore have, by **Proposition 1.3.7**,

$$P_{z_m x_m} P_{z_{m+1} x_{m+1}} = 0$$

and the result follows. ∎

We are now ready for our quantum isomorphism criterion.

Proof of THEOREM 3.4.17. By assumption, there exists a quantum automorphism P of $G \sqcup H$ such that $P_{wv} \neq 0$. Let us write it in block form as

$$P = \begin{pmatrix} P_G & Q \\ Q' & P_H \end{pmatrix}.$$

The intuition is that P_G and P_H should be quantum automorphisms of G and H respectively, while Q and Q' should be quantum isomorphisms between the two. In order to make this precise, let us set, for $x \in V(G)$ and $y \in V(H)$,

$$Q_x = \sum_{w' \in V(H)} P_{w'x} \quad \& \quad Q_y = \sum_{v' \in V(G)} U_{yv'}.$$

These are orthogonal projections, and we claim that they are all equal. Indeed, for $x, x' \in V(G)$,

$$\begin{aligned} (1 - Q_x) Q_{x'} &= \left(\sum_{v' \in V(G)} U_{v'x} \right) Q_{x'} \\ &= \sum_{v' \in V(G)} \sum_{w' \in V(H)} U_{v'x} P_{w'x'} \\ &= 0 \end{aligned}$$

by Lemma 3.4.18. This implies that $Q_x Q_{x'} = Q_{x'}$ and since x and x' play symmetric roles, we conclude that $Q_x = Q_{x'}$. The same reasoning shows that $Q_y = Q_{y'}$ for any $y, y' \in V(Y)$. Moreover,

$$\begin{aligned} NQ_x &= \sum_{x' \in V(G)} Q_{x'} \\ &= \sum_{x' \in V(G)} \sum_{y' \in V(H)} P_{x'y} \\ &= \sum_{y' \in V(H)} Q_{y'} \\ &= NQ_y \end{aligned}$$

so that our claim is proven.

Let us denote by R the common value of all the projections projection and observe that it is designed to cut down the P_G and P_H parts of P and only keep Q and Q'. We will now use the new Hilbert space $\mathscr{H}' = R\mathscr{H}$. It comes with an algebra homomorphism $\rho : B(\mathscr{H}) \to B(\mathscr{H}')$ defined by the formula

$$\rho(T) = RTR,$$

which also satisfies $\rho(T^*) = \rho(T)^*$. The crucial fact is that ρ is non-zero, because since $Q_{wv} = P_{wv} \neq 0$, we also have $R \neq 0$. Applying ρ entrywise to Q now produces a matrix $\widetilde{Q}$ which is by construction a quantum permutation. More generally, applying ρ entrywise to P yields

$$\widetilde{P} = \begin{pmatrix} 0 & \widetilde{Q} \\ \widetilde{Q}' & 0 \end{pmatrix}$$

To conclude, observe that since ρ is an algebra homomorphism, the equality $\widetilde{P}A_{G\sqcup H} = A_{G\sqcup H}\widetilde{P}$. Recalling that $A_{G\sqcup H}$ is just block diagonal with blocks A_G and A_H, we see that

$$\begin{pmatrix} 0 & \widetilde{Q}A_H \\ \widetilde{Q}'A_G & 0 \end{pmatrix} = \begin{pmatrix} 0 & A_G\widetilde{Q} \\ A_H\widetilde{Q}' & 0 \end{pmatrix}.$$

This yields in particular $A_H\widetilde{Q}' = \widetilde{Q}'A_G$, proving that G and H are indeed quantum isomorphic. ■

Forgetting about the connectedness assumption for the moment, this reduces the problem to finding v and w in the same quantum orbit. For that, one must understand the relationship between the quantum orbits of G and H. For this we will need an operation on linear maps which might look a bit strange at first sight.

DEFINITION 3.4.19. Given two matrices $A, B \in M_{k,\ell}(\mathbf{C})$, their *Schur* product is the matrix $A \bullet B \in M_{k,\ell}(\mathbf{C})$ with coefficients

$$\boxed{(A \bullet B)_{i,j} = A_{ij}B_{ij}}$$

Schur product is interesting because it is compatible with gadget isomorphism, at least at low levels.

Lemma 3.4.20. *Let G and H be gadget isomorphic. Then, for any $\chi, \chi' \in \mathfrak{C}_G(0,1)$, we have*

$$\boxed{\Phi_{0,1}(\chi \bullet \chi') = \Phi_{0,1}(\chi) \bullet \Phi_{0,1}(\chi')}$$

Similarly, for any $A, A' \in \mathfrak{C}_G(1,1)$,

$$\boxed{\Phi_{1,1}(A \bullet A') = \Phi_{1,1}(A) \bullet \Phi_{1,1}(A')}$$

Proof. The first equality comes from the observation that for two vectors $\chi, \chi' \in \mathbf{C}^{V(G)}$, we have

$$\chi \bullet \chi' = \Delta_G^*(\chi \otimes \chi').$$

Since

$$\Phi_{0,1}(\Delta_G) = \Phi_{0,1}(F_{\mathbf{C}}^G) = F_{\mathbf{C}}^H = \Delta_H,$$

and since Φ is compatible with composition, involution and tensor products, the result follows. As for the second equality, it proceeds in the same way, starting this time with the formula

$$A \bullet A' = \Delta_G^*(A \otimes A')\Delta_G.$$

■

We are now ready to describe the effect of gadget isomorphism on quantum orbits.

Proposition 3.4.21. *Let $\chi_1, \cdots, \chi_n$ be the indicator functions of the quantum orbits of G seen as vectors in $\mathbf{C}^{V(G)}$. Then,*

1. $\chi_i \in \mathfrak{C}_G(0,1)$ *for all* $1 \leqslant i \leqslant n$ *;*
2. *The vectors* $\Phi_{0,1}(\chi_i)$ *are the indicator functions of the quantum orbits of* $V(H)$*.*

Thus, $\Phi_{0,1}$ *induces a bijection between the quantum orbits.*

Proof. Let us prove the two assertions one after the other.

1. Observe that if $\chi_i(w) = 1$, then $P_{wv}\chi_i(v) = P_{wv}$ for all $v \in V(G)$ by definition of a quantum orbit, hence

$$\begin{aligned}\big(P\chi_i\big)_w &= \sum_{v\in V(G)} P_{wv}\chi_i(v)\\ &= \sum_{v\in V(G)} P_{wv}\\ &= 1.\end{aligned}$$

   If now $\chi_i(w) = 0$, then $P_{wv}\chi_i(v) = 0$ for all $v \in V(G)$, hence

$$\big(P\chi_i\big)_w = 0$$

   in that case. In conclusion, we have $P\chi_i = \chi_i$, which is precisely the statement that $\chi_i \in \mathfrak{C}_G(0,1)$.

2. We first show that the functions $\psi_i = \Phi_{0,1}(\chi_i)$ is an indicator functions of a partition of $V(H)$. We have shown in Lemma 3.4.20 that Φ preserves Schur products, hence

$$\begin{aligned}\psi_i \bullet \psi_j &= \Phi_{0,1}(\chi_i) \bullet \Phi_{0,1}(\chi_j)\\ &= \Phi_{0,1}(\chi_i \bullet \chi_j)\\ &= \delta_{ij}\Phi_{0,1}(\chi_i)\\ &= \delta_{ij}\psi_i.\end{aligned}$$

   This means that the ψ_i's indicator functions of pairwise disjoint subsets $S_i \subset V(H)$. Moreover, denoting by $\mathbf{1}_G$ all-ones vector in $\mathbf{C}^{V(G)}$, we have $\mathbf{1} = F^G_{\mathbf{V}^*}$ hence

$$\begin{aligned}\sum_{i=1}^n \psi_i &= \Phi_{0,1}\left(\sum_{i=1}^n \psi_i\right)\\ &= \Phi_{0,1}\left(\mathbf{1}_G\right)\\ &= \Phi_{0,1}\left(F^G_{\mathbf{V}^*}\right)\\ &= F^H_{\mathbf{V}^*}\\ &= \mathbf{1}_H.\end{aligned}$$

   This means that the ψ_i's are the indicator functions of a partition of $V(H)$.

   We further claim that any vector $\psi \in \mathfrak{C}_H(0,1)$ is constant on quantum orbits. Indeed, if $P_{wv} \neq 0$, then

$$\begin{aligned}\psi(w)P_{wv} &= \big(\psi(w)P_{wv}\big)P_{wv}\\ &= \big(P\psi\big)_w P_{wv}\\ &= \left(\sum_{v'\in V(G)} \psi_{v'}P_{wv'}\right)P_{wv}\\ &= \psi(v)P_{wv}\end{aligned}$$

   hence $\psi(v) = \psi(w)$. It follows that each ψ_i is the indicator function of a union of quantum orbits of H. In particular, the number of quantum orbits of H is at most n. Applying the same argument to $\Phi_{0,1}^{-1}$, we conclude that both G and H have the same number of quantum orbits, which in turn forces each ψ_i to be the indicator function of a single quantum orbit.

■

The last ingredient of the proof is related to the connectedness assumption in **Proposition 3.4.21**. We need a way to guarantee that we are not losing any generality when assuming G and H to be connected.

Lemma 3.4.22. *If G and H are gadget isomorphic, then either both are connected or both are not connected.*

Proof. Let N be the number of vertices of G and set

$$S_G = \sum_{i=1}^{N-1} A_G^i.$$

The coefficient $(S_G)_{vv'}$ is non-zero if and only if v and v' are connected by a path of length at most $N-1$ in G, which is the same as saying that they are just connected by a path. We then define another matrix R_G by

$$(R_G)_{vv'} = \begin{cases} 1 & \text{if} \quad v \text{ and } v' \text{ are connected by a path} \\ 0 & \text{otherwise} \end{cases}$$

Then, G is connected if and only if $R_G = J_{V(G)}$, where $J_{V(G)}$ is the all-ones matrix.

We now claim that $\Phi_{1,1}(R_G) = R_H$. Indeed, let $\mathscr{F}$ be the finite set of all possible values of non-zero coefficients of S_G and let $p \in \mathbf{C}[X]$ be a polynomial such that $p(x) = 1$ for all $x \in \mathscr{F}$ and $p(0) = 0$ (such a polynomial exists, for instance by LAGRANGE'S INTERPOLATION THEOREM). If

$$p(X) = \sum_{k=1}^{n} a_k X^k,$$

then

$$R_G = \sum_{k=1}^{n} a_k S_G^{\bullet k}.$$

Since $\Phi_{1,1}$ is linear, preserves composition and Schur products (by Lemma 3.4.20), and since $\Phi_{1,1}(A_G) = A_H$, we conclude that $\Phi_{1,1}(R_G) = R_H$. Since on the other hand

$$J_{V(G)} = F_{\mathbf{V}}^G \circ (F_{\mathbf{V}}^G)^*,$$

we have $\Phi_{1,1}(J_{V(G)}) = J_{V(H)}$ so that in the end, $R_H = J_{V(H)}$ if and only if $R_G = J_{V(G)}$, hence the result. ■

We can now complete the proof of the FUNDAMENTAL THEOREM

End of proof of THEOREM 1.5.1. Recall that we have reduced the problem to proving that if G and H are gadget isomorphic, then we can find $v \in V(G)$ and $w \in V(H)$ which are in the same quantum orbit of $X = G \sqcup H$. We will first do this assuming that G and H are both connected.

Let us fix a vertex $v \in \chi_1$ and a vertex $w \in \psi_1 = \Phi_{0,1}(\chi_1)$. Given a *connected* $(0,1)$-planar gadget $\mathbf{K}$, $T_{\mathbf{K}}^G \in \mathfrak{C}_G(0,1)$ is constant on quantum orbits (this was shown for any element of $\mathfrak{C}_G(0,1)$ in the proof of **Proposition 3.4.21**). In particular, there is $\lambda \in \mathbf{C}$ such that

$$T_{\mathbf{K}}^G \bullet \chi_1 = \lambda \chi_1.$$

Applying $\Phi_{0,1}$ then yields $T_{\mathbf{K}}^H \bullet \psi_1 = \lambda \psi_1$ so that in particular, evaluating at $v \in V(G)$ on the one hand at $w \in V(H)$ on the other hand leads to

$$T_{\mathbf{K}}^G(v) = \lambda = T_{\mathbf{K}}^H(w).$$

This translates into the following equality of homomorphism counts

$$|\mathrm{Hom}(\mathbf{K}, (G,v))| = |\mathrm{Hom}(\mathbf{K}, (H,w))|.$$

Because $\mathbf{K}$ is connected, any homomorphism to $G \sqcup H$ sending a vertex to v must send all the graph to G, and similarly for H, hence we deduce that

$$|\mathrm{Hom}(\mathbf{K},(X,v))| = |\mathrm{Hom}(\mathbf{K},(X,w))|,$$

which also reads

$$T^X_{\mathbf{K}}(v) = T^X_{\mathbf{K}}(w).$$

The previous equality has only been shown for connected $\mathbf{K}$, but an arbitrary $(0,1)$-planar gadget is a disjoint union of a connected $(0,1)$-planar gadget and a number of $(0,0)$-planar gadgets, hence the result extends directly. Now, because the maps associated to gadgets span the whole space, we have in fact $T(v) = T(w)$ for all $T \in \mathfrak{C}_X(0,1)$. In particular, this is true for any indicator function of a quantum orbit, which is only possible if both v and w are in the same quantum orbit, thereby concluding the proof.

What if the graphs are not both connected? By Lemma 3.4.22, they are then both non-connected. In that case, their complements are connected[1]. Moreover, because as shown in the proof of Lemma 1.3.9, $A_{G^c} = J_{V(G)} - I_{V(G)} - A_G$, G^c and H^c are again gadget isomorphic. By the first part of the proof, we conclude that G^c and H^c are quantum isomorphic, and the result then follows from Lemma 1.3.9. ■

We have therefore completed the proof of the FUNDAMENTAL THEOREM 1.5.1 announced in Lecture 1. Although several technical ingredients were omitted – related to compact quantum groups and planar graphs – the key ideas should now be apparent : quantum isomorphism can be translated into an intertwining relation, encoded graphically through planar gadgets, and finally recovered using the orbit structure of the associated quantum permutation group.

1. Indeed, if $v,w \in V(G)$, then either v and w are not connected in G, in which case they are connected in X^c, or they are connected in G but by lack of connectedness, there exists $z \in V(X)$ such that both x and y are not connected to z. It then follows that z is connected to both x and y in G^c, hence G^c is connected.

REFERENCES

[AH77] K. APPEL & W. HAKEN – « Every planar map is four folorable », *Illinois J. Math.* **21** (1977), no. 3, p. 429–567.

[AMR+19] A. ATSERIAS, L. MANČINSKA, D. ROBERSON, R. ŠÁMAL, S. SEVERINI & A. VARVITSIOTIS – « Quantum and non-signalling graph isomorphisms », *Journal of Combinatorial Theory, Series B* **136** (2019), p. 289–328.

[Ark12] A. ARKHIPOV – « Extending and characterizing quantum magic games », *arXiv preprint* (2012).

[BM07] J. BONDY & U. MURTY – *Graph theory with applications*, Graduate Texts in Mathematics, vol. 290, Springer, 2007.

[DdBvFNK+25] J. DOBBEN DE BRUYN (VAN), A. FRESLON, P. NIGAM KAR, D. ROBERSON & P. ZEMAN – « Free inhomogeneous wreath product of compact quantum groups », *arXiv preprint* (2025).

[DdBvNKR+25] J. DOBBEN DE BRUYN (VON), P. NIGAM KAR, D. ROBERSON, S. SCHMIDT & P. ZEMAN – « Quantum automorphism groups of trees », *J. Noncommut. Geom.* **20** (2025), no. 2, p. 489–505.

[FMP25] A. FRESLON, P. MEUNIER & P. POURNAJAFI – « Block structures of graphs and quantum isomorphism », *arXiv preprint* (2025).

[Fre23] A. FRESLON – *Compact matrix quantum groups and their combinatorics*, LMS Student Texts in Mathematics, Cambridge University Press, 2023.

[Gon08] G. GONTHIER – « Formal proof of the four-color theorem », *Notices of the AMS* **55** (2008), no. 11, p. 1382–1393.

[LMR20] M. LUPINI, L. MANČINSKA & D. ROBERSON – « Nonlocal games and quantum permutation groups », *J. Funct. Anal.* **279** (2020), no. 5, p. 108592.

[Lov67] L. LOVÁSZ – « Operations with structures », *Acta Math. Acad. Sci. Hungar.* **18** (1967), no. 3-4, p. 321–328.

[Mer90] N. MERMIN – « Simple unified form for the major no-hidden-variables theorems », *Phys. Rev. Lett.* **65** (1990), no. 27, p. 3373.

[Meu26] P. MEUNIER – « Quantum properties of $\mathscr{F}$-cographs », *J. Noncommut. Geom.* (2026).

[MR20] L. MANČINSKA & D. ROBERSON – « Quantum isomorphism is equivalent to equality of homomorphism counts from planar graphs », in *2020 IEEE 61st Annual Symposium on Foundations of Computer Science (FOCS)*, IEEE, 2020, p. 661–672.

[Per] A. PERES – « Incompatible results of quantum measurements », *Phys. Lett. A* **151**, no. 3–4, p. 107–108.

[Slo20] W. SLOFSTRA – « Tsirelson's problem and an embedding theorem for groups arising from non-local games », *J. Amer. Math. Soc.* **33** (2020), no. 1, p. 1–56.

[Web23] M. WEBER – « Quantum permutation matrices », *Complex. Anal. Oper. Theory* **17** (2023), no. 3.

[Wil13] M. WILDE – *Quantum information theory*, Cambridge University Press, 2013.