

THE INVERSE QUIVER PROBLEM IS NP-COMPLETE

PAUL COUTANT–DENORD

*Department of Mathematics, Ecole normale supérieure, Université
PSL, 75005 Paris, France*

ABSTRACT. We prove that the inverse quiver problem is NP-complete.
We also present a new proof that the quiver problem is NP-complete.
We present a way to translate arithmetical/algebraic geometry
problems in terms of (inverse) quiver problem.

1. INTRODUCTION

E. Bellini, R. Makarim, C. Sanna, and J. Verbel prove in [1] that the MQ problem is NP-complete. It consists of determining whether a system of quadratic polynomial equations $p_1, \dots, p_m$ in n variables in this field, whose coefficients belong to a finite field, has a solution. The problem of determining whether a family of polynomials $P_1, \dots, P_m$ defined over a finite field has a common root is directly NP-complete. Let q be the cardinality of the field. Then $P = 1 - \prod_{k=1}^m (1 - P_k^{q-1})$ has a zero if and only if the family $P_1, \dots, P_m$ has a common zero. Thus, the problem of determining whether a polynomial in n variables has a root is NP-complete. The complexity depends on the number of coefficients.

Recall that a quiver is an oriented graph, and that a representation of a quiver over $\mathbb{F}$ consists of a finite-dimensional vector space at each vertex and a linear map for each edge, compatible with the vector spaces at the source and target of that edge. A representation is indecomposable (resp. absolutely indecomposable) if it cannot be written as the direct sum of two non-trivial quiver representations over $\mathbb{F}$ (resp. over $\overline{\mathbb{F}}$).

V. Kac and B. Li defined the quiver problem in [2] and proved that it is NP-complete. Let Γ a quiver and $R(X_1, \dots, X_M)$ a representation of Γ , where the entry of the matrices are in $\mathbb{F} \cup \{X_1, \dots, X_M\}$. The answer to the quiver problem is YES if it exists $x_1, \dots, x_M$ such that $R(x_1, \dots, x_M)$ is absolutely indecomposable. The answer to the inverse

Email address: paul.coutant--denord@ens.psl.eu.

Date: October 7, 2026.

quiver problem is YES if there exist $x_1, \dots, x_M$ such that the associated quiver representation is not absolutely indecomposable.

The Kac-Li quiver representation $R_\Theta(x_1, \dots, x_M)$ associated to the 3-CNF Boolean formula Θ lead us to an easy proof of the fact that the inverse quiver problem is NP-complete. The quiver representation $R_{\neg\Theta}(x_1, \dots, x_M)$ is not absolutely indecomposable if and only if $\neg\Theta(x_1, \dots, x_M) = 0$ so if and only if $\Theta(x_1, \dots, x_M) = 1$, where $\neg\Theta$ is the boolean negation of the formula Θ . We present here an other proof, more elementary of the two problems. To prove that the inverse quiver problem is NP-complete, we construct a quiver representation over a finite field $\mathbb{F}$ that is not absolutely indecomposable if and only if the variables $x_1, \dots, x_M$ satisfy $P(x_1, \dots, x_M) = 0$ for a chosen polynomial $P \in \mathbb{F}[X_1, \dots, X_M]$.

2. CONSTRUCTION OF THE QUIVER REPRESENTATION

$\text{Root}_P(x_1, \dots, x_M)$

Let $P \in \mathbb{F}[X_1, \dots, X_M]$ be a nonzero polynomial. In this section, we construct $\text{Root}_P(X_1, \dots, X_M)$, a quiver representation over $\mathbb{F}$ such that $\text{Root}_P(x_1, \dots, x_M)$ is not absolutely indecomposable if and only if $P(x_1, \dots, x_M) = 0$. For clarity, we construct the quiver representation in several parts. The vertices of the quiver are labelled by the vector space of the representation.

2.1. The lock part. Let L be the following quiver representation:

$$\begin{array}{ccccc} \mathbb{F} & & \mathbb{F} & & \mathbb{F} \\ & \searrow^{(1)} & \downarrow^{(1)} & \swarrow_{(0)} & \\ & & \mathbb{F}^2 & & \end{array}$$

Lemma 1 (L is indecomposable). *The quiver representation L is indecomposable.*

Proof. Suppose there exists a non-trivial decomposition. Then the vertex $\mathbb{F}^2$ decomposes as a direct sum of two one-dimensional vector spaces. It follows that two of the three arrows have their images in one of these subspaces, which is a contradiction. $\square$

2.2. The coefficient part. Let $C(a, k_1, \dots, k_M)$ be the following quiver representation, where $a \in \mathbb{F}$ and $k_1, \dots, k_M \in \mathbb{Z}_{\geq 0}$:

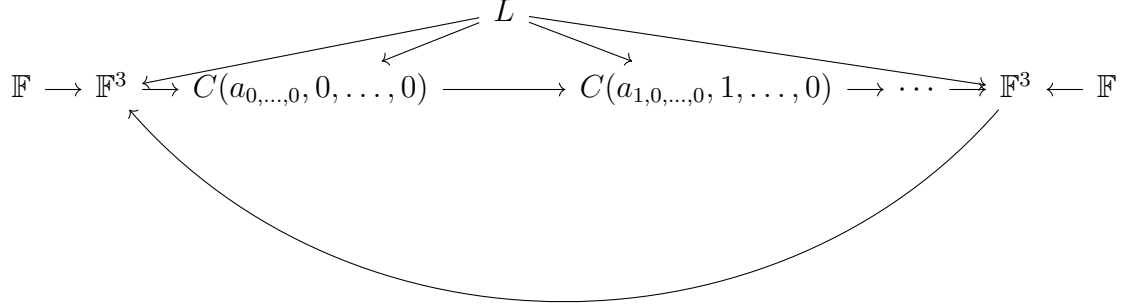
$$\mathbb{F}^3 \xrightarrow{f_a} \mathbb{F}^3 \xrightarrow{f_1} \dots \xrightarrow{f_1} \mathbb{F}^3 \xrightarrow{f_2} \mathbb{F}^3 \xrightarrow{f_2} \dots \xrightarrow{f_M} \mathbb{F}^3$$

where

$$f_a = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ a & 0 & 1 \end{pmatrix}, \quad f_i = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & x_i \end{pmatrix},$$

and the map f_i appears k_i times.

2.3. The quiver representation $\text{Root}_P(x_1, \dots, x_M)$. We write $P = \sum_{k_1, \dots, k_M} a_{k_1, \dots, k_M} X_1^{k_1} \dots X_M^{k_M}$. The quiver representation $\text{Root}_P(x_1, \dots, x_M)$ is the following:



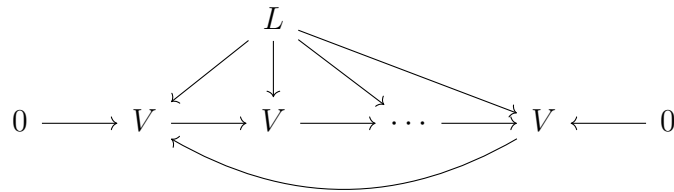
There is an arrow from L to each $\mathbb{F}^3$ vertex, originating at the vertex $\mathbb{F}^2$ of L . The corresponding linear map is always $\begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$.

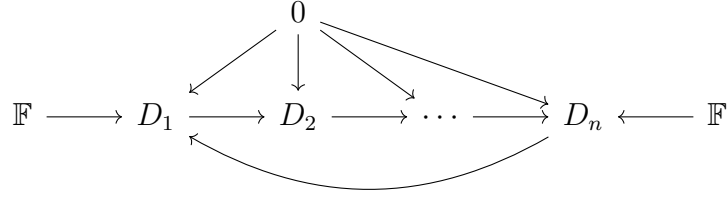
Between two consecutive C parts, the connecting map is $s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}$.

The same map connects the last C part to the last $\mathbb{F}^3$ vertex. The arrows from $\mathbb{F}$ to $\mathbb{F}^3$ are given by $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. The arrow between the two extremal $\mathbb{F}^3$ vertices is the identity.

Theorem 1. *The quiver representation $\text{Root}_P(x_1, \dots, x_M)$ is absolutely indecomposable if and only if $P(x_1, \dots, x_M) \neq 0$.*

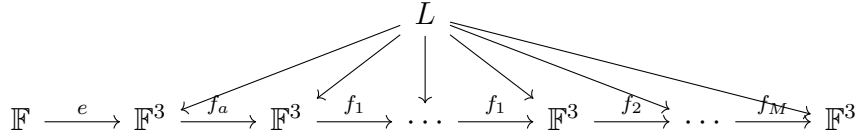
Lemma 2. *If $\text{Root}_P(x_1, \dots, x_M)$ admits a decomposition, then every $\mathbb{F}^3$ vertex must decompose as a direct sum of V , the subspace spanned by $\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$, and a one-dimensional subspace D_k . The decomposition must then take the following form:*



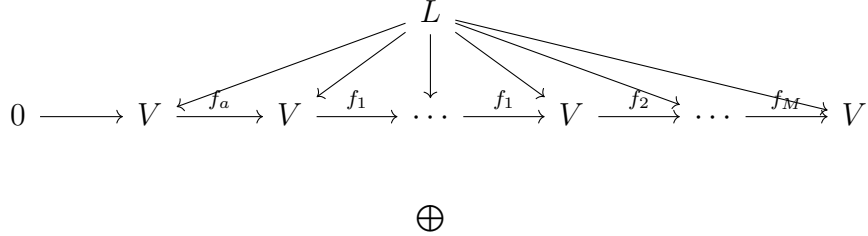


Proof. By Lemma 1, the L part is indecomposable. Hence, each $\mathbb{F}^3$ vertex must decompose as a direct sum of two subspaces. The arrow from L into each $\mathbb{F}^3$ vertex forces one of these subspaces to be V . Moreover, the maps f_a, f_i, s , and Id all stabilize V and map any complementary subspace into another one, and they are nonzero on each such complement. Since there is an incoming arrow into each decomposed $\mathbb{F}^3$ vertex, the source space must decompose in the same way. Therefore, all $\mathbb{F}^3$ spaces decompose identically. $\square$

Lemma 3. *The following quiver representation, with $e = \begin{pmatrix} 1 \\ Q \\ 0 \end{pmatrix}$,*



admits a decomposition where the last $\mathbb{F}^3$ is decomposed; it is unique, namely:



$$\mathbb{F} \xrightarrow{e} A_1 \xrightarrow{f_a} A_2 \xrightarrow{f_1} \dots \xrightarrow{f_1} A_k \xrightarrow{f_2} \dots \xrightarrow{f_M} A_n$$

where A_2 is spanned by $\begin{pmatrix} 1 \\ Q \\ a \end{pmatrix}$, A_3 by $\begin{pmatrix} 1 \\ Q \\ ax_1 \end{pmatrix}$, $\dots$, and A_n by $\begin{pmatrix} 1 \\ Q \\ ax_1^{k_1} \dots x_M^{k_M} \end{pmatrix}$.

Lemma 4. *By the same argument as in the proof of Lemma 2, if the last $\mathbb{F}^3$ is decomposed, all the $\mathbb{F}^3$ vertices are decomposed. Moreover, A_1 is spanned by $\begin{pmatrix} 1 \\ Q \\ 0 \end{pmatrix}$ because of e . Then, the actions of f_a and f_i show that this decomposition is necessarily the one above. One can verify that this decomposition is valid.*

Proof of Theorem 1. Suppose that $\text{Root}_P(x_1, \dots, x_M)$ is decomposable. By Lemma 2, we know the form of this decomposition. By Lemma 3, and using the identity

$$s \begin{pmatrix} 1 \\ Q \\ ax_1^{k_1} \cdots x_M^{k_M} \end{pmatrix} = \begin{pmatrix} 1 \\ Q + ax_1^{k_1} \cdots x_M^{k_M} \\ 0 \end{pmatrix},$$

we conclude that D_n (from Lemma 2) is spanned by $\begin{pmatrix} 1 \\ P(x_1, \dots, x_M) \\ 0 \end{pmatrix}$.

However, due to the incoming arrow from $\mathbb{F}$, we must have $P(x_1, \dots, x_M) = 0$. Conversely, if this condition holds, the decomposition described above is valid. Therefore, $\text{Root}_P(x_1, \dots, x_M)$ is decomposable (equivalently, not absolutely indecomposable) if and only if $P(x_1, \dots, x_M) = 0$. $\square$

Corollary 1. *The inverse quiver problem is NP-complete.*

Proof. The problem lies in NP by [4]. The construction of the quiver representation $\text{Root}_P(x_1, \dots, x_M)$ is polynomial in the number of monomials of P , which is the size of the input. What matters here is the number of coefficients, not the number of variables. Furthermore, the problem of determining whether there exist $x_1, \dots, x_M$ such that $P(x_1, \dots, x_M) = 0$ is NP-complete (see [1]). Consequently, the inverse quiver problem is NP-complete. $\square$

Corollary 2. *The quiver problem is NP-complete.*

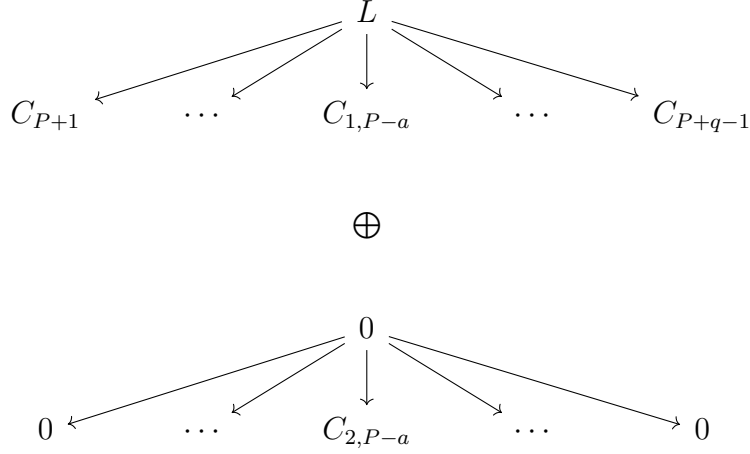
Proof. Let $P \in \mathbb{F}[X_1, \dots, X_M]$. The quiver representation $\text{Root}_P(x_1, \dots, x_M)$ has the form

$$\begin{array}{c} L \\ \downarrow \\ C_P \end{array}$$

We can then build the following quiver representation, where $q = |\mathbb{F}|$:

$$\begin{array}{ccccc} & & L & & \\ & \swarrow & \downarrow & \searrow & \\ C_{P+1} & & \cdots & & C_{P+q-1} \end{array}$$

This representation is absolutely indecomposable if and only if $P(x_1, \dots, x_M) \neq 0$. Indeed, if there is a decomposition, by the same argument as before, one of the C_{P+a} parts must be decomposed, so $P(x_1, \dots, x_M) = -a$. Conversely, if $P(x_1, \dots, x_M) = a \neq 0$, we have the following decomposition:



where $C_{1,P-a}$ and $C_{2,P-a}$ are the two parts of the decomposition of $\text{Root}_{P-a}(x_1, \dots, x_M)$. Therefore, by the same reasoning as above, the quiver problem is NP-complete. $\square$

2.4. Dimension of the representation. In this section, we show that the dimension of the representation $\text{Root}_P(X_1, \dots, X_M)$ is an imaginary root. Further details can be found in [3].

Recall that if $\{u\}$ is the set of vertices of a quiver, $\Gamma = \bigoplus_{\{u\}} \alpha_u \mathbb{Z}$ and R is a quiver representation, with V_u the vector space associated with vertex u in R , then the dimension of R is $\dim R = \sum_u \dim V_u \alpha_u \in \Gamma$.

The Cartan matrix A of the quiver is an $n \times n$ matrix, where n is the number of vertices, $u_1, \dots, u_n$ being a numbering of the vertices, and $A_{i,j} = 2$ if $i = j$, otherwise $-A_{i,j}$ is the number of edges connecting u_i and u_j . Let $(\cdot, \cdot)$ denote the associated symmetric bilinear form. Thus $(\alpha_{u_i}, \alpha_{u_j}) = A_{i,j}$. Let $s_i : x \mapsto x - (x, \alpha_{u_i}) \alpha_{u_i}$. The group W generated by $\{s_i\}$ is the Weyl group. A root α of the associated Kac-Moody Lie algebra is real if it exists $w \in W$ such that $w(\alpha)$ is a simple root, i.e $\alpha = u_i$. Otherwise, α is imaginary. Let $C = \{\alpha, (\alpha, \alpha_{u_i}) \leq 0, \forall i\}$ the fundamental domain. α is imaginary root if and only if $w(\alpha) \in K$ for a $w \in W$. Let α_0 denote the canonical basis element of Γ associated with the vertex $\mathbb{F}^2$ of the part L . Let $\alpha_1, \alpha_2, \alpha_3$ be the elements associated with the other vertices of the part L . Let β_0, β_1 be the two elements associated with $\mathbb{F}$ in the representation. Let $\delta_1, \dots, \delta_n$ be associated with all vertices of $\mathbb{F}^3$. Let $\alpha = \dim \text{Root}_P(x_1, \dots, x_M) = 2\alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 + \beta_0 + \beta_1 + 3\delta_1 + \dots + 3\delta_n$

We have then

$$\begin{aligned}
(\alpha, \alpha_0) &= (2\alpha_0, \alpha_0) + \sum_{k=1}^3 (\alpha_k, \alpha_0) + \sum_{k=1}^n (3\delta_k, \alpha_0) = 1 - 3n \\
(\alpha, \alpha_{1,2,3}) &= (\alpha_{1,2,3}, \alpha_{1,2,3}) - (2\alpha_0, \alpha_{1,2,3}) = 0 \\
(\alpha, \beta_{0,1}) &= (\beta_{0,1}, \beta_{0,1}) + (\beta_{0,1}, 3\delta_{1,n}) = -1 \\
(\alpha, \delta_{1,n}) &= 6 - 1 - 3 - 3 - 2 = -3 \\
(\alpha, \delta_{2,\dots,n-1}) &= 6 - 3 - 3 - 2 = -2
\end{aligned}$$

So α is in the fundamental domain C , and so α is an imaginary root. Based on a similar calculation, one can proof that the dimension of the representation of Corollary 2 is also an imaginary root. [3]

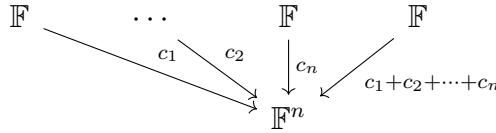
3. A GENERALIZATION

Here we generalize the construction of the quiver representation $\text{Root}_P(x_1, \dots, x_M)$ to a finite family of polynomials.

3.1. The construction of the quiver representation. Let $P_1, \dots, P_r \in \mathbb{F}[X_1, \dots, X_M]$, with

$$\begin{aligned}
P_1 &= \sum_{k_1, \dots, k_M} a_{1,k_1, \dots, k_M} X_1^{k_1} \cdots X_M^{k_M}, \\
&\vdots \\
P_r &= \sum_{k_1, \dots, k_M} a_{r,k_1, \dots, k_M} X_1^{k_1} \cdots X_M^{k_M}.
\end{aligned}$$

3.1.1. The n -lock part. We denote by L_n the following quiver representation:



Lemma 5. *For every $n \geq 2$, the representation L_n is absolutely indecomposable.*

Proof. Suppose there is a non-trivial decomposition. Then $\mathbb{F}^n$ must decompose into two non-trivial subspaces. Since there are $n+1$ incoming arrows and the sum of the dimensions of the two subspaces is n , one of the two subspaces receives more incoming arrows than its dimension. However, every subfamily of n vectors from $\{c_1, \dots, c_n, c_1 + \dots + c_n\}$ is linearly independent, giving a contradiction. $\square$

3.1.2. *The coefficient part.* Let $C(a_1, \dots, a_r, k_1, \dots, k_M)$ be the following quiver representation, where $a_1, \dots, a_r \in \mathbb{F}$ and $k_1, \dots, k_M \in \mathbb{Z}_{\geq 0}$:

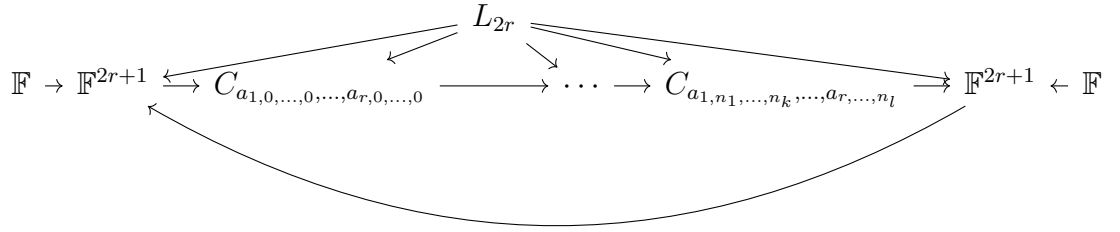
$$\mathbb{F}^{2r+1} \xrightarrow{f_{a_1, \dots, a_r}} \mathbb{F}^{2r+1} \xrightarrow{f_{1,r}} \dots \xrightarrow{f_{1,r}} \mathbb{F}^{2r+1} \xrightarrow{f_{2,r}} \mathbb{F}^{2r+1} \xrightarrow{f_{2,r}} \dots \xrightarrow{f_{M,r}} \mathbb{F}^{2r+1}$$

where, denoting by $v_1, \dots, v_{2r+1}$ the canonical basis of $\mathbb{F}^{2r+1}$:

$$f_{a_1, \dots, a_r}(v_1) = v_1 + a_1 v_3 + a_2 v_5 + \dots + a_r v_{2r+1},$$

$f_{a_1, \dots, a_r}(v_j) = v_j$ for $j \neq 1$, while $f_{i,r}(v_j) = x_i v_j$ for $j \geq 3$ an odd number and $f_{i,r}(v_j) = v_j$ else.

3.1.3. *The quiver representation.* We denote by $\text{Root}_{P_1, \dots, P_r}(x_1, \dots, x_M)$ the following quiver representation:



The arrows from $\mathbb{F}$ to $\mathbb{F}^{2r+1}$ are given by v_1 . The connection map between the $\mathbb{F}^{2r+1}$ and the C parts, and between the C parts is

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & 0 \end{pmatrix}.$$

The connection map from the rightmost $\mathbb{F}^{2r+1}$ to the leftmost $\mathbb{F}^{2r+1}$ is the identity. By a similar argument, one can show that $\text{Root}_{P_1, \dots, P_r}(x_1, \dots, x_M)$ is decomposable if and only if $P_1(x_1, \dots, x_M) = \dots = P_r(x_1, \dots, x_M) = 0$.

3.2. Dimension of the representation. As before, let $\alpha = 2r\alpha_0 + \alpha_1 + \dots + \alpha_{2r+1} + \beta_0 + \beta_1 + (2r+1)\delta_1 + \dots + (2r+1)\delta_n$ the dimension of $\text{Root}_{P_1, \dots, P_r}(X_1, \dots, X_M)$. Then :

$$(\alpha, \alpha_0) = 4r - (2r+1) - (2r+1)(n) = 4r - (2r+1)(n+1)$$

$$(\alpha, \alpha_{1, \dots, 2r+1}) = 2 - 2r$$

$$(\alpha, \beta_{0,1}) = 2 - (2r+1) = 1 - 2r$$

$$(\alpha, \delta_{1,n}) = 2(2r+1) - 1 - 2r - 2(2r+1) = -1 - 2r$$

$$(\alpha, \delta_{2, \dots, n-1}) = 2(2r+1) - 2r - 2(2r+1) = -2r$$

And, then α is an imaginary root.

4. THE QUIVER PROBLEM CATEGORY

As we saw earlier, many “polynomial problems” can be reformulated in terms of “quiver problems.” Let’s examine the following two arithmetic examples. The first is the famous Fermat’s Last Theorem, proven by Wiles [5].

Theorem 2 (Fermat-Wiles). *The answer to the inverse quiver problem for $\text{Root}_{X^p+Y^p-1}(X, Y)$ over $\mathbb{Q}$, where $X, Y \neq 0$, is always NO.*

We can easily rephrase the problem to determine whether a number is prime.

Lemma 6. *The answer to the inverse quiver problem for $\text{Root}_{XY-p}(X, Y)$ is NO with X, Y two positives integers greater than 1 if and only if p is a prime number.*

This results can be generalized.

Lemma 7. *The answer to the inverse quiver problem of $\text{Root}_{(X_1Y_1-p_1)\dots(X_nY_n-p_n)}(X_1, Y_1, \dots, X_n, Y_n)$ is NO with $X_1, Y_1, \dots, X_n, Y_n$ positives integers greater than 1 if and only if $p_1, \dots, p_n$ are prime numbers.*

One can also translate the famous Goldbach’s conjecture.

Conjecture 1 (Goldbach’s conjecture). *Let $n \geq 2$ an integer. The answer to the inverse quiver problem of $\text{Root}_{X+Y-2n}(X, Y)$ is YES with X, Y prime numbers.*

In both of these problems, we wish to determine the solution to an (inverted) quiver problem, with a restriction on the elements of the matrix. To reformulate these problems, let us construct the category $QP_{\mathbb{F}}(\Gamma, \Omega)$, where $\mathbb{F}$ is a field and (Γ, Ω) is a quiver (Γ being a graph and Ω the orientation). The objects of $QP_{\mathbb{F}}(\Gamma, \Omega)$ are the quiver representations over $\mathbb{F}$ of (Γ, Ω) such that the elements of the matrix belong to $\mathbb{F} \cup \{X_1, \dots, X_n\}$, where n is an integer. Arrows are quiver representation morphisms compatible with these quiver representations (i.e., a collection of matrices whose entries are rational fractions that behave well with the matrices of the representations). Note that this category has the direct sum, but the concept of indecomposition in this category does not correspond to the quiver problem. Let $R \subset \mathbb{F}$ be a subset, the “restriction” set. We define two functors, C_R and I_R . These two functors act on the following category.

$$\begin{array}{ccc} T & \xrightleftharpoons{\quad} & F \\ \curvearrowright & & \curvearrowright \end{array}$$

If A is an object in $QP_{\mathbb{F}}(\Gamma, \Omega)$, then $C_R(A) = T$ if and only if the answer to the quiver problem for A , with inputs restricted to R , is “YES.” $I_R(A)$ equals T if and only if the answer to the inverse quiver problem for A , with inputs restricted to R , is “YES.” One can reformulate the examples.

Theorem 3 (Fermat-Wiles). *One has*

$$I_{\mathbb{Q} \setminus \{0\}}(\text{Root}_{X^p+Y^p-1}(X, Y)) = F$$

Lemma 8. *One has*

$$I_{\mathbb{N} \setminus \{0,1\}}(\text{Root}_{(X_1Y_1-p_1)\dots(X_nY_n-p_n)}(X, Y)) = F$$

if and only if $p_1, \dots, p_n$ are prime numbers.

Let’s denote by $\mathcal{P}$ the set of prime numbers

Conjecture 2 (Goldbach). *One has*

$$I_{\mathcal{P}}(\text{Root}_{X+Y-2n}(X, Y)) = T$$

for all $n \geq 2$

REFERENCES

- [1] Emanuele Bellini, Rusydi H. Makarim, Carlo Sanna, and Javier Verbel. *An Estimator for the Hardness of the MQ Problem*, pages 323–347. 10 2022.
- [2] Victor Kac and Bangzheng Li. The quiver problem is NP-complete. *Journal of Algebra*, 697:145–156, 2026.
- [3] Victor G Kac. Infinite root systems, representations of graphs and invariant theory. *Inventiones mathematicae*, 56(1):57–92, 1980.
- [4] Victor G. Kac. On complexity of representations of quivers. *Comptes Rendus. Mathématique*, 357(11-12):841–845, 2019.
- [5] Andrew Wiles. Modular Elliptic Curves and Fermat’s Last Theorem. *Annals of Mathematics*, 141(3):443–551, 1995.