Is the Distance Geometry Problem in NP?

Nathanael Beeker, Stéphane Gaubert, Christian Glusa, and Leo Liberti

Abstract Given a weighted undirected graph $G = (V, E, d)$ with $d : E \to \mathbb{Q}_+$ and a positive integer K, the Distance Geometry Problem (DGP) asks to find an embedding $x : V \to \mathbb{R}^K$ of G such that for each edge $\{i, j\}$ we have $\|x_i - x_j\| = d_{ij}$. Saxe proved in 1979 that the DGP is **NP**-complete with $K = 1$ and doubted the applicability of the Turing machine model to the case with $K > 1$, because the certificates for YES instances might involve real numbers. This chapter is an account of an unfortunately failed attempt to prove that the DGP is in **NP** for $K = 2$. We hope that our failure will motivate further work on the question.

1 Introduction

Consider the following decision problem.

DISTANCE GEOMETRY PROBLEM (DGP). Given a weighted undirected graph $G = (V, E, d)$ where $d : E \to \mathbb{F}$, and a positive integer K, establish whether there exists an embedding $x : V \to \mathbb{R}^K$ such that:

$$\forall \{i, j\} \in E \quad \|x_i - x_j\| = d_{ij}, \tag{1}$$

N. Beeker
CMAP, École Polytechnique, 91128 Palaiseau, France
e-mail: `nathanael.beeker@polytechnique.edu`

S. Gaubert
INRIA Rocquencourt, France; e-mail: `stephane.gaubert@inria.fr`

C. Glusa
CMAP, École Polytechnique, 91128 Palaiseau, France
e-mail: `christian.glusa@polytechnique.edu`

L. Liberti
LIX, École Polytechnique, 91128 Palaiseau, France
e-mail: `liberti@lix.polytechnique.fr`

where F is a set of nonnegative numbers, which, for the purposes of this chapter, we assume to be either integers $\mathbb{N}$ or rationals $\mathbb{Q}_+$. We denote explicit dependence of the DGP on K by DGP_K.

The DGP is **NP**-hard, but even when $\mathbb{F} = \mathbb{N}$ it is not known, whenever $K > 1$, whether it is in **NP** or not. Trying to prove that the DGP is in **NP** would involve finding a polynomial size representation for the solutions of a polynomial system of equations of degree two. Disproving the statement would probably be much more difficult. This chapter relates a possible proof technique for showing that DGP∈**NP** and the corresponding failure, in the hope of enticing new efforts on this topic.

1.1 Applications

In the Molecular Distance Geometry Problem (MDGP), G is a molecule graph where the E is the set of known inter-atomic distances, and $K = 3$. Since the function of molecules depends strongly on their spatial configuration, finding an embedding of V in $\mathbb{R}^3$ is of practical interest [11,13]. A distinguishing property is that, because of the experimental techniques involved, most distances are bounded above by 6Å, so that the resulting graph is 3D generalization of a Unit Disk Graph (UDG) [1].

Wireless Sensor Network Localization (WSNL) aims to embed a wireless sensor network in $\mathbb{R}^2$ (so $K = 2$). Pairs of sensors can estimate their distance by measuring the power used for a two-way communication. Since sensor networks always include a wired backbone (allowing the link between the sensor network and the external world), and the position of the wired backbone components is usually known, the distinguising mathematical property of the WSNL is that a *partial embedding* $x' : U \to \mathbb{Q}^2$ is known in advance, where $U \subseteq V$ is the set of wired backbone components, called *anchors* in the WSNL literature [4,21]. Again, because wireless communication can only occur below a certain distance threshold, the resulting graph is a UDG.

Lines of forces acting on static physical structure (such as a building) define a graph. If the forces sum to zero, then the structure stands. Starting from such basic definitions, a theory of bar-and-joint structures has been developed ever since the XVIII century [3,10,15,18,24]. This involves embeddings of the graph where joints are vertices and bars (with their lengths) are weighted edges; the zero sum force requirement holds if a given embedding is an isolated point in embedding space. More recently, the interest was shifted towards graphs whose topology itself guarantees that all (or almost all) embeddings are isolated points. Such graphs are termed *rigid* [6,20].

Graph Drawing (GD) is a discipline studying algorithms for drawing graphs. The embedding might be defined for any $K \geq 1$, but of course only projections in 2D and 3D are actually represented visually. See `www.graphdrawing.org` for more information.

1.2 Complexity

Saxe [19] proved in 1979 that DGP_1 with $\mathbb{F} = \mathbb{N}$ is **NP**-complete by means of a reduction from SUBSET-SUM [5]. It is in **NP** because a given embedding x can be verified to satisfy (1) in polynomial time. Furthermore, an instance $\{a_1, \ldots, a_n\} \in \mathbb{Z}^n$ of SUBSET-SUM can be suitably reduced to the instance $G = (V, E, d)$ with $V = \{v_0, \ldots, v_{n-1}\}$, $E = \{\{v_i, v_{i+1 \mod n}\} \mid i < n\}$, $d_{i,i+1 \mod n} = a_i$ for all $i < n$.

For what concerns $K > 1$, in [19], Sect. 5, Saxe writes,

- **NP**-Completeness is defined for language recognition problems on Turing Machines, which inherently can deal only with integers and not with arbitrary reals.
- Given a "random" embedding of an unweighted graph into a Euclidean space, any two of the edge weights induced by the embedding will be incommensurable with probability 1. Moreover, if the graph is overconstrained and the dimension of the space is at least two, then rounding the induced edge-weights to multiples of some small distance will almost always produce a weighted graph that is not embeddable in space.

The DGP contains the DGP_1, which is **NP**-complete; but as remarked by Saxe, the DGP itself might not be in **NP**. Thus, it is commonly stated in the literature that the DGP (and in particular the MDGP and the WSNL) is **NP**-hard (see e.g. [4, 9]). By definition [5], a problem is **NP**-hard when every problem in **NP** can be reduced to it, independently of whether the problem itself is in **NP** or not.

In order to show that a decision problem is in **NP**, we have to perform the following steps:

1. encoding certificates of YES instances;
2. showing that such certificates can be verified in time which is polynomial in the size of the instance.

In the case of the DGP, the certificates are solutions of the system (1). Squaring every equation of the system yields:

$$\forall \{i, j\} \in E \quad \|x_i - x_j\|^2 = d_{ij}^2. \tag{2}$$

System (2) has the same set of solutions as (1), since d always takes non-negative values. Notice, however, that (2) is a polynomial system: as such, its solutions $x = ((x_{11}, \ldots, x_{1K},), \ldots, (x_{n1}, \ldots, x_{nK}))$ always have algebraic components.

2 Representations of algebraic numbers

It is well known that some algebraic numbers over $\mathbb{Q}$ can be written as mathematical expressions involving integers and elementary operators such as sum, subtraction, product, fraction and k-root. Let us call $\mathscr{O}$ the set of operator symbols $+, \times, \div, \sqrt[k]{}$. The statement $DGP \in \mathbf{NP}$ is equivalent to stating that all components of an embedding solving the instance can always be written as meaningful strings of symbols in $\mathbb{Z}$ and $\mathscr{O}$, the size of which is bound by a polynomial in the instance size. Not all

algebraic numbers, however, can be written this way: specifically, this is the case if and only if the Galois group of the minimal polynomial of the algebraic number in question is soluble [22]. What about those algebraic numbers that do not satisfy this requirement?

If α is a root of a polynomial $p(x)$ over $\mathbb{Q}$ whose Galois group is not soluble, then it can't be expressed using symbols in $\mathbb{Z} \cup \mathscr{O}$ alone. What one can do, however, is to adjoin other algebraic numbers in $B = \{\beta_1, \ldots, \beta_h\}$ to $\mathbb{Q}$, obtaining other fields $F = \mathbb{Q}[\beta_1, \ldots, \beta_h]$, until the minimal polynomial of α over F has a soluble Galois group. This process terminates: it suffices to adjoin all the roots of $p(x)$. Symbolic algebra packages such as Maple [14] attempt to find smallest h such that the Galois group of $p(x)$ over F is soluble. Then α can be expressed by meaningful strings of symbols in $\mathbb{Z} \cup B \cup \mathscr{O}$.

Example 1. Asking Maple to solve:

$$x^5 + y + 1 = 0$$
$$y^2 + y - x = 0$$

yields the solution $x = \alpha^2 + \alpha$, $y = \alpha$, where α is a root of the polynomial $(x + 1)(x^8 + 3x^7 + 3x^6 + x^5 + 1)$. The Galois group of $x^8 + 3x^7 + 3x^6 + x^5 + 1$ is S_8, the full symmetric group over 8 elements, and S_8 is not soluble.

2.1 Polynomial system representation

Each algebraic number $\alpha \in \mathbb{A}$ can be associated with a polynomial $p_\alpha \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$ and a rational $\bar{\alpha} \in \mathbb{Q}$ which is closest to α than to the other roots of p_α.

Example 2. For $\alpha = \sqrt[3]{\frac{1}{2} + \sqrt[4]{3}}$ we might choose its minimal polynomial over $\mathbb{Q}$, $p_\alpha(x) = x^{12} - 2x^9 + \frac{3}{2}x^6 - \frac{1}{2}x^3 - \frac{47}{16}$, and set $\bar{\alpha} = 2$, which is closest to α than to the other real root of p_α.

As mentioned above, embeddings can be seen as sequences of algebraic numbers. Any sequence S of ℓ algebraic numbers can be associated with a multivariate polynomial system $\mathbf{p}_S \in \mathbb{Z}[x_1, \ldots, x_\ell]$ such that $\mathbf{p}_S(S) = 0$, together with a rational vector $q \in \mathbb{Q}^\ell$ such that $\|S - q\|_2$ is smallest.

2.2 Formal grammar representation

The "meaningful strings" mentioned above, used to represent algebraic numbers in a field $F = Q[B]$ where $B = \{\beta_1, \ldots, \beta_h\}$, are generated by the formal grammar:

$$\mathbb{A} \longrightarrow (\mathbb{A} + \mathbb{A}) \vee (\mathbb{A} \times \mathbb{A}) \vee (\mathbb{A} \div \mathbb{A}) \vee (\sqrt[\mathbb{Z}]{\mathbb{A}}) \vee (\mathbb{Z}) \vee (B)$$

where, with a slight abuse of notation, we use $\mathbb{A}, \mathbb{Z}$ to denote the *type* of algebraic and integer numbers. Given a string consisting of symbols in $\mathbb{Z} \cup B \cup \mathcal{O}$, the string is meaningful if it matches the pattern given by the grammar. The algorithm that matches strings to grammars [12] is recursive in nature and is yields a *grammar derivation trees* [16]. Each algebraic number in $\mathbb{A}$ can be represented with respect to B by its corresponding derivation tree.

Example 3. The algebraic number $\alpha = \sqrt[3]{\frac{1}{2} + \sqrt[4]{3}}$ yields the grammar derivation tree shown in Fig. 1.

Fig. 1 The derivation tree for α according to the algebraic grammar.

3 The Gröbner bases strategy

We restrict our attention to $K = 2$, and propose to pursue a line of argument showing that $\text{DGP}_2 \in \mathbf{NP}$. It is well known that any multivariate polynomial system of equations such as (2) can be reduced to a "triangular form" by employing Gröbner bases and the Buchberger algorithm [2] (a clear and short introduction to these concepts can be found in [8]). We represent an embedding $x : V \to \mathbb{R}^2$ solving a DGP_2 instance as the sequence $(x_{11}, x_{12}, x_{21}, x_{22}, \ldots, x_{n1}, x_{n2})$

Example 4. Consider the right-angled triangle with smallest possible integer side lengths $(3, 4, 5)$ in $\mathbb{R}^2$ delimited by $x_1 = (0, 0)$, $x_2 = (3, 0)$, $x_3 = (0, 4)$. System (2) is:

$$(x_{11} - x_{21})^2 + (x_{12} - x_{22})^2 = 9$$
$$(x_{11} - x_{31})^2 + (x_{12} - x_{32})^2 = 16$$
$$(x_{21} - x_{31})^2 + (x_{22} - x_{32})^2 = 25.$$

The above system describe *all* $(3,4,5)$-sided triangles in $\mathbb{R}^2$. We can fix $x_{11} = x_{12} = 0$ and $x_{21} = 3$ to eliminate rotations and translations. This reduces the system to:

$$3^2 + x_{22}^2 = 9$$
$$x_{31}^2 + x_{32}^2 = 16$$
$$(3 - x_{31})^2 + (x_{22} - x_{32})^2 = 25.$$

A Gröbner basis of the above system (provided by Maple 9.5 [14] with the pure lexicographic term ordering) is given by:

$$x_{31}^2 = 0$$
$$x_{32}^2 = 16$$
$$16x_{22} + 3x_{31}x_{32} = 0.$$

It is clear that the Gröbner system has two real solutions given by $x_{22} = x_{31} = 0$, and $x_{32} = \pm 4$, which correspond to two congruent conformations reflected along the 1st coordinate, as shown in Fig. 2.
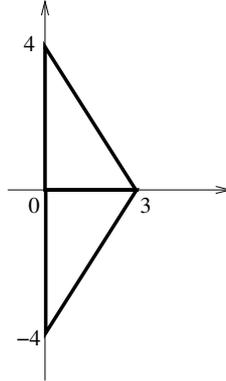
Fig. 2 The two configurations given by the Gröbner system in Example 4.

Let the system (2) have solution set X, and let $x \in X$. According to Sect. 2.1 we can represent x by (2) and a rational vector $q \in \mathbb{Q}^{2n}$ which is closest to x than any other $x' \in X$. Because of Gröbner basis theory, it follows that the very same embedding can be represented by any Gröbner basis system derived from (2) and q. The advantage in reducing the original system (2) to triangular form is that, by

a form of back-substitution, we can easily derive the set B referred to in Sect. 2, together with the string that describes the components of x.

Showing that the size of a Gröbner basis is bounded by a polynomial in the instance size would be a (substantial) first step towards proving that $DGP_2 \in \textbf{NP}$. Unfortunately, this is false in general: the size of a Gröbner basis grows doubly-exponentially. The polynomial system (2), however, has a very special structure, which — one might hope — could provide an exception. The rest of this section will introduce an infinite class of DGP instances which provide empirical evidence to the contrary. This is, of course, not a conclusive statement.

3.1 The empirical evidence against

In this section we construct an infinite class of graphs embedded in $\mathbb{R}^2$ which have a Gröbner basis whose size, obtained computationally for a few cases, indicates an exponential growth in the instance size. The graph class consists of a chain of triangles sharing a side: $V = \{1, \ldots, n\}$ (with $n \geq 3$), and $E = \{\{v-2, v\}, \{v-1, v\} \mid v > 2\}$. The weight function $d : E \to \mathbb{Q}_+$ is such that $d_{uv} = \frac{1}{u}$ for all $\{u, v\}$ such that $u < v$. Examples with $n = 10$ and $n = 20$ are given, respectively, in Fig. 3 and 4.
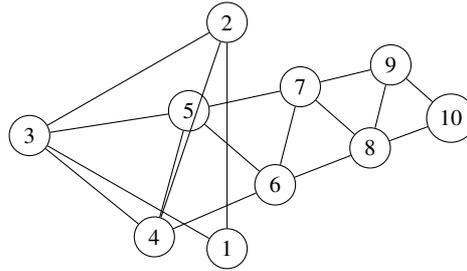
Fig. 3 A triangle chain of size 10 embedded in $\mathbb{R}^2$.

These triangle chains embedded in $\mathbb{R}^2$ provide rigid frameworks [7], and are examples of of Henneberg type I graphs [23] and of DISCRETIZABLE DGP (DDGP) instances [17]. Using Maple [14], we were able to show that the dependency of the Gröbner basis size in terms of the instance size looks exponential over a set of triangle chains with n vertices with $n \in \{3, \ldots, 11\}$. More precisely, the number of equations in the Gröbner basis and the size of each equation both seem to grow exponentially (or worse), whereas the degree seems to grow linearly, as shown in Fig. 5.
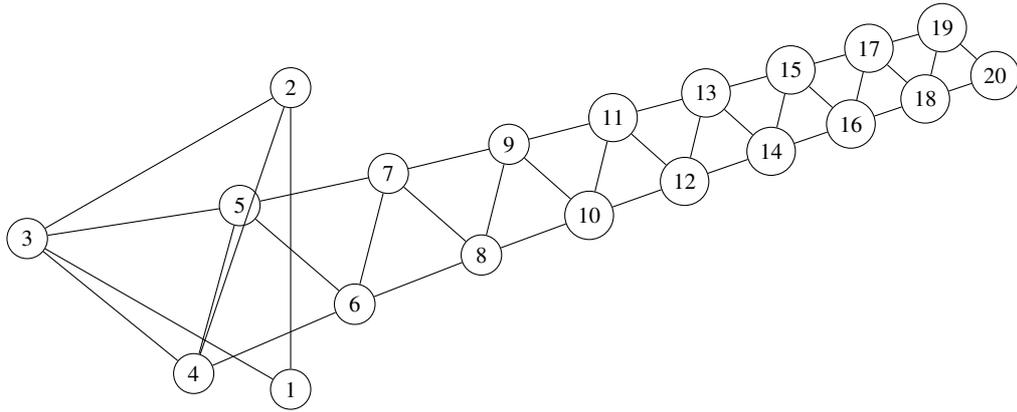
Fig. 4 A triangle chain of size 20 embedded in $\mathbb{R}^2$.
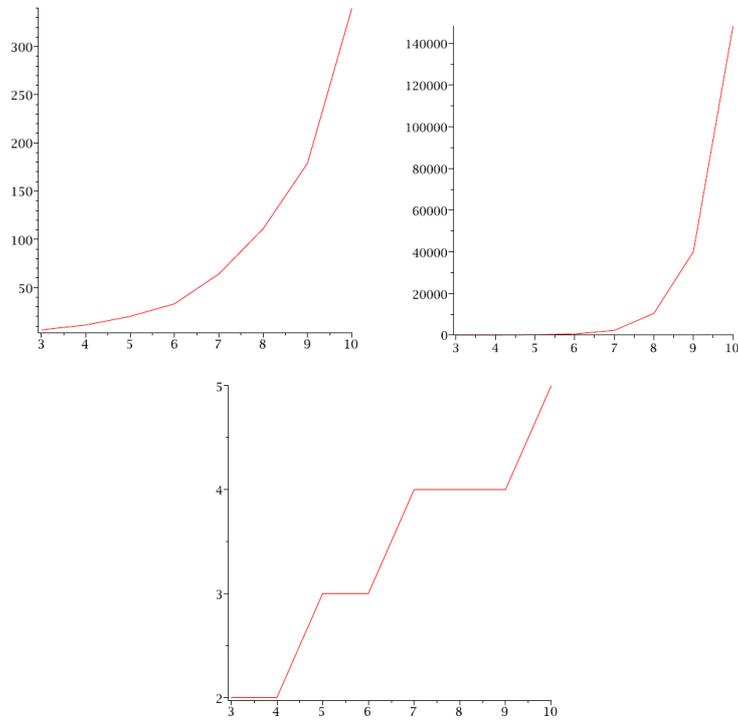
Fig. 5 The growth pattern of the number of equations (left) in the Gröbner basis of triangle chains, the size of each equation (center) and the degree of the system (right).

References

1. Clark, B., Colburn, C., Johnson, D.: Unit disk graph. Discrete Mathematics **86**, 165–177 (1990)

2. Cox, D., Little, J., O'Shea, D.: Ideals, Varieties and Algorithms, second edn. Springer, Berlin (1997)
3. Cremona, L.: Le figure reciproche nella statica grafica. G. Bernardoni, Milano (1872)
4. Eren, T., Goldenberg, D., Whiteley, W., Yang, Y., Morse, A., Anderson, B., Belhumeur, P.: Rigidity, computation, and randomization in network localization. IEEE Infocom Proceedings pp. 2673–2684 (2004)
5. Garey, M., Johnson, D.: Computers and Intractability: a Guide to the Theory of NP-Completeness. Freeman and Company, New York (1979)
6. Graver, J.: Rigidity matroids. SIAM Journal on Discrete Mathematics **4**, 355–368 (1991)
7. Graver, J., Servatius, B., Servatius, H.: Combinatorial Rigidity. American Mathematical Society (1993)
8. Hägglöf, K., Lindberg, P., Svensson, L.: Computing global minima to polynomial optimization problems using gröbner bases. Journal of Global Optimization **7**(2), 115:125 (1995)
9. Hendrickson, B.: The molecule problem: exploiting structure in global optimization. SIAM Journal on Optimization **5**, 835–857 (1995)
10. Henneberg, L.: Die Graphische Statik der starren Systeme. Teubner, Leipzig (1911)
11. Lavor, C., Liberti, L., Maculan, N., Mucherino, A.: Recent advances on the discretizable molecular distance geometry problem. European Journal of Operational Research (accepted / invited survey)
12. Levine, R., Mason, T., Brown, D.: Lex and Yacc, second edn. O'Reilly, Cambridge (1995)
13. Liberti, L., Lavor, C., Mucherino, A., Maculan, N.: Molecular distance geometry methods: from continuous to discrete. International Transactions in Operational Research **18**, 33–51 (2010)
14. Maplesoft, Inc.: Maple 9 Getting Started Guide. Maplesoft, Waterloo (2003). URL `http://www.maplesoft.com/products/maple/manuals/GettingStartedGuide.pdf`
15. Maxwell, J.: On the calculation of the equilibrium and stiffness of frames. Philosophical Magazine **27**(182), 294–299 (1864)
16. Mosses, P.: Denotational semantics. In: J. van Leeuwen (ed.) Handbook of Theoretical Computer Science B: Formal Models and Semantics, pp. 575–631. Elsevier, Amsterdam (1990)
17. Mucherino, A., Lavor, C., Liberti, L.: The discretizable distance geometry problem. Optimization Letters (accepted)
18. Saviotti, C.: Nouvelles méthodes pour le calcul des travures réticulaires. In: Appendix to L. Cremona, "Les figures réciproques en statique graphique", pp. 37–100. Gauthier-Villars, Paris (1885)
19. Saxe, J.: Embeddability of weighted graphs in k-space is strongly NP-hard. Proceedings of 17th Allerton Conference in Communications, Control and Computing pp. 480–489 (1979)
20. Servatius, B., Servatius, H.: Generic and abstract rigidity. In: M. Thorpe, P. Duxbury (eds.) Rigidity Theory and Applications, Fundamental Materials Research, pp. 1–19. Springer, New York (2002). DOI 10.1007/0-306-47089-6_1
21. So, A.M.C., Ye, Y.: Theory of semidefinite programming for sensor network localization. Mathematical Programming B **109**, 367–384 (2007)
22. Stewart, I.: Galois Theory, second edn. Chapman & Hall, London (1989)
23. Tay, T.S., Whiteley, W.: Generating isostatic frameworks. Structural Topology **11**, 21–69 (1985)
24. Varignon, P.: Nouvelle Mecanique. Claude Jombert, Paris (1725)