Abstract. We formally state Skein Problems in Hamiltonian graphs and prove that they are reduced to the Independence Problem in Graph Theory. Skein problems can be widely used in cryptography, particularly, in protocols for message authentication or entities identification. Let $G$ be a Hamiltonian graph. Given a Hamiltonian cycle $H$, let $P$ be a set of pairwise disjoint sub-paths within $H$,

$$P = [v_{11}, \ldots, v_{m1}], \ldots, P_k = [v_{1k}, \ldots, v_{mk}]$$

where $m$ and $k$ are two positive integers, then the pairs of extreme vertices $V = \{(v_{11}, v_{m1}), \ldots, (v_{1k}, v_{mk})\}$ are connected by the paths at $H$ without any crossing. Conversely, let us assume that the following problem is posed: given a collection of pairs $V$ it is required to find a collection of pairwise disjoint paths, without any crossing, connecting each pair at $V$. We reduce this last problem to the Independence Problem in Graph Theory. In particular, for the case of the $n$-dimensional hypercube, we show that the resulting translated instances are not Berge graphs, thus the most common polynomial-time algorithms to solve the translated problem do not apply. We have built a computing system to explicitly generate the resulting graphs of the reduction to the Independence problem. Nevertheless, due to the doubly exponential growth in terms of $n$ of these graphs, the physical computational resources are quickly exhausted.

Keywords. Independence problem in graph theory, Berge graphs, doubly-exponential growth.

1 Introduction

Within a graph, a vertex pair is connectable if there is a path going from a point at the pair to the complementary point. A collection of connectable vertex pair poses the simple problem to find explicitly connecting paths for each vertex pair. Evidently, some supplementary conditions may be imposed, e.g., the located connecting paths should have the shortest possible lengths, or the paths should not cross among themselves, or the collection of connecting paths should allow the extension to a $k$-factor of the graph, for a fixed $k \geq 2$, etc. Let us say that a skein is a set of connecting paths for a collection of connectable vertex pairs.

Let us consider the following problems:

Skein extension Given a collection of equally length paths in a graph which are pairwise non-crossing (no pair has a common vertex which is internal in at least one of the paths) and disjoint (no edge is shared), it is required to add one path with prescribed endpoints in the graph such that the resulting set of paths remains pairwise disjoint and non-crossing.

Skein search Given a collection of vertex pairs, it is required to decide whether there are connecting paths, all of the same length such that they are pairwise non-crossing and disjoint.

2 Preliminaries

For ease of exposition, let us recall some basic notions. A graph is a pair $G = (V, E)$ where $V(G)$ is a finite and non-empty set of vertices,
and the set \( E(G) \) of edges is an unordered subset of \( V \times V \). The cardinalities of \( V(G) \) and \( E(G) \) are, respectively, the order and the size of \( G \). A subgraph \( H \) of \( G \) is a graph such that \( V(H) \subset V(G) \) and \( E(H) \subset E(G) \). If \( V' \subset V(G) \) then the induced subgraph of \( G \) by \( V' \) is the graph having \( V' \) as set of vertices, and two vertices \( u, v \) in \( V' \) are joined by an edge in \( V' \) if and only if \( uv \in E(G) \). If \( e = v_1v_2 \in E(G) \) then \( v_1 \) is adjacent to \( v_2 \) and the vertices \( v_1 \) and \( v_2 \) are incident to the edge \( e \). The complete graph \( K_n \) of order \( n \) is a graph having \( n \) vertices, where each one is adjacent to any other. A clique in \( G \) is a complete induced subgraph of \( G \). A path in \( G \) with initial vertex \( v_0 \) and ending vertex \( v_m \) is a sequence of vertices \( \pi = [v_0, v_1, \ldots, v_m] \). A path can also be written \( \pi = v_0v_1 \ldots v_m \), such that for \( i = 0, \ldots, m - 1 \), \( v_iv_{i+1} \in E(G) \), \( v_0, \ldots, v_{m-1} \) are pairwise different, and \( m \) is a positive integer. The vertices \( v_0 \) and \( v_m \) are the end-vertices or endpoints of \( \pi \). The length \( |\pi| \) of the path \( \pi \) is \( m \), hence \( \pi \) is said to be an \( m \)-path. The internal vertices of \( \pi \) are \( v_1, \ldots, v_{m-1} \). If \( v_0 = v_m \), then \( \pi \) is a cycle.

The distance \( d_G(u, v) \) between two vertices \( u, v \) in \( G \) is the length of a shortest path connecting \( u \) and \( v \). Two paths which are not cycles \( \pi_1, \pi_2 \) are non-crossing if there is no common vertex in \( \pi_1 \) and \( \pi_2 \) which they differ. It is easy to see that the graph \( Q_n \) is the graph containing the \( n \)-dimensional vectors with entries in \( \{0, 1\} \) as vertices, and \( u \) and \( v \) form an edge if and only if they differ in just one entry. The Hamming distance \( \text{Hamming}(u, v) \) holds for every pair of vertices \( u, v \) in \( V(Q_n) \).

A graph \( G \) is a Berge graph, if neither \( G \) nor its complement has an odd-length induced cycle of length \( 5 \) or more. It is well-known that if \( G \) is a Berge graph, then the independence problem on \( G \) can be solved in polynomial time [5].

Any Hamiltonian cycle \( H \) in a graph \( G = (V, E) \) determines, for each pair of distinct vertices \( (u, v) \in V^2 \), two paths, one going, let us say, from \( u \) to \( v \) and the supplementary path from \( v \) to \( u \). Let \( \pi_H(u, v) \) be the path going from \( u \) to \( v \) following the order in which the vertices of \( H \) are listed. Since \( H \) is Hamiltonian, for any two pairs \( (u_0, v_0), (u_1, v_1) \) such that \( u_0, v_0, u_1, v_1 \) appear in the cyclic order of the Hamiltonian cycle, the paths \( \pi_H(u_0, v_0) \) and \( \pi_H(u_1, v_1) \) are non-crossing.

Given a positive integer \( n \), the \( n \)-dimensional hypercube, denoted \( Q_n \), is the graph containing the \( n \)-dimensional vectors with entries in \( \{0, 1\} \) as vertices, and two vertices form an edge if and only if they differ in just one entry. The Hamming distance between two vertices \( u, v \) in \( Q_n \), denoted \( \text{Hamming}(u, v) \) is the number of entries in which they differ. It is easy to see that the graph distance and the Hamming distance coincide, that is, \( d_{Q_n}(u, v) = \text{Hamming}(u, v) \) holds for every pair of vertices \( u, v \) in \( V(Q_n) \).

### 3 Particular Problems

Let us consider the following problem:

**NonCrossingPaths**

**Instance:** A graph \( G = (V, E) \). A positive number \( k \), a set of pairs \( K = \{(i_1, j_1), \ldots, (i_k, j_k)\} \) of \( k \) pairwise different vertex pairs in \( G \), and a positive integer \( m \) satisfying \( m - k \leq |V(G)| \) and \( d_G(i, j) \leq m \) for all \((i, j) \in K \).

**Solution:** A pairwise non-crossing and disjoint collection of \( m \)-length paths \( \Pi = \{\pi_1, \ldots, \pi_k\} \) such that \( \pi_l \) has endpoints \( i_l \) and \( j_l \), for \( l = 1, \ldots, k \).

Given a Hamiltonian cycle \( H \) of \( G \) it is very simple to complete instances of the problem NonCrossingPaths having as solutions non-crossing and disjoint paths taken from \( H \). For
instance, if \( H = v_1v_2\ldots v|V(G)|-1 \), and \( m \cdot k \leq |V(G)| \), then for
\[
K = \{(v_0,v_m), (v_{m+1},v_{2(m+1)-1}), \ldots, (v_{(k-1)(m+1)},v_{k(m+1)-1})\}
\]
the collection of paths
\[
\Pi = \{v_0\ldots v_m; v_{m+1}\ldots v_{2(m+1)-1}; \ldots; v_{(k-1)(m+1)}\ldots v_{k(m+1)-1}\}
\]
is a solution.

Conversely, given the collection \( \Pi \) one may wonder whether it is built from a Hamiltonian cycle.

Let us consider the following problem:

**HamiltonianExtension**

**Instance:** a Hamiltonian graph \( G = (V,E) \). A collection \( \Pi \) of pairwise disjoint and non-crossing \( m \)-paths.

**Solution:** a Hamiltonian cycle \( H \in \mathcal{H}_G \) such that for any \( \pi \in \Pi \), if \( u \) and \( v \) are the initial and the ending points of \( \pi \), respectively, then \( \pi_H(u,v) = \pi \).

For instance, for the \( n \)-dimensional hypercube \( Q_n \) and \( \Pi \) a perfect matching at \( Q_n \) (the paths at \( \Pi \) are just edges), then \( \text{HamiltonianExtension}(Q_n,\Pi) \) always has a solution, although it is not uniquely determined [2, 3].

Thus, \( \text{HamiltonianExtension} \) would allow to recover a Hamiltonian cycle from a solution of the problem \( \text{NonCrossingPaths} \). However, a solution of \( \text{NonCrossingPaths} \) may be obtained without building a whole Hamiltonian cycle containing that solution.

But solving \( \text{NonCrossingPaths} \) can be reduced to finding a maximum independent set in a huge graph as we see now.

**Definition 3.1 (Path Graphs)** Given the instance \( (G, k, K = \{(u_1, v_1), \ldots, (u_k, v_k)\}, m) \) of the problem \( \text{NonCrossingPaths} \), let the path graph \( P_{m,k,K,G} \) be the graph whose vertices are the \( m \)-paths in \( G \) connecting pairs at \( K \):
\[
\pi = [u_j_0 \ldots u_j_m] \in V(P_{m,k,K,G}) \iff (u_j_0, u_j_m) \in K,
\]
and the edges are of two types: for any \( \pi, \mu \in V(P_{m,k,K,G}) \),— if \( \pi, \mu \) are crossing, then \( \pi \mu \in E(P_{m,k,K,G}) \), and— if \( \pi, \mu \) have the same extreme points, then \( \pi \mu \in E(P_{m,k,K,G}) \).

An independent set \( I^* \) of \( P_{m,k,K,G} \) yields a set of non-crossing and disjoint paths with ends in \( K \), with no pair of extreme points connected by two paths.

For any pair \( (u, v) \in K \) let \( R(u,v) \) be the subgraph of \( P_{m,k,K,G} \) induced by the set of vertices at \( V(P_{m,k,K,G}) \) having as extreme points \( u \) and \( v \). Then \( R(u,v) \) is a clique.

Those cliques produce a partition of the vertices in \( P_{m,k,K,G} \) in \( k \) subsets, and any solution of the problem \( \text{NonCrossingPaths} \) should contain exactly one member at each clique, hence it has at most \( k \) paths. Thus, whenever there exists an independent set \( I^* \) reaching the upper bound \( k \), such \( I^* \) is maximum. Hence:

**Proposition 3.1** With the above notation, the parameter \( k \) equals the independence number of \( P_{m,k,K,G} \), \( k = \alpha(P_{m,k,K,G}) \), and an independent set of \( P_{m,k,K,G} \) is maximum if and only if it is a solution of an instance of \( \text{NonCrossingPaths} \) of the form: \((G, k, K = \{(u_1, v_1), \ldots, (u_k, v_k)\}, m)\).

4 Hamiltonian Cycles in the Hypercube

Let us examine some criteria to select instances of \( \text{NonCrossingPaths} \) making it difficult to solve the problem.

The main interest in the stated problem is to find maximum independent sets in the graph \( P_{m,k,K,G} \) for a given instance
\[
(G, k, K = \{(u_1, v_1), \ldots, (u_k, v_k)\}, m)
\]
of NonCrossingPaths.

As we have agreed before, let us consider, in particular, the hypercube \( G = Q_n \) for some positive integer \( n \). The edges in the hypercube \( Q_n \) are pairs of the form \( vu \), where \( v + u = e_i \) is a vector in the canonical basis of \( Q_n \); all its entries are zero, except for the \( i \)-th entry. A Hamiltonian cycle in \( Q_n \) is a sequence \( H = h_0 \cdots h_{2n-1} \) such that its terms form a permutation of \( V(Q_n) \) and each pair of contiguous terms \( h_i, h_{i+1} \) is an edge (the successor map is taken modulus \( 2^n \)). A square, or 4-cycle, in \( Q_n \) is a sequence \( v_0v_1v_2v_3 \) of pairwise different vertices forming a cycle in the hypercube. Necessarily, any square has the form \( v, v + e_i, v + e_i + e_j, v + e_j \) for two distinct indexes \( i, j \in \{0, \ldots, n-1\} \).

The typical Hamiltonian cycle at the hypercube is the binary Gray code. As a sequence, this code is determined recursively by the following recurrence:

\[
g_1 = [0, 1] \quad g_n = \text{join}(0 * g_{n-1}, 1 * \text{rev}(g_{n-1}))
\]

(\text{join} and \text{rev} are, respectively, list concatenation and list reversing, \(* \) is a \text{prepend} map: \( b * \text{list} \) prepends the bit \( b \) to each entry at the list). For instance: \( g_1 = [0, 1] \), \( g_2 = [00, 01, 11, 10] \), \( g_3 = [000, 001, 011, 010, 110, 111, 101, 100] \), and so on.

In order to have an idea about the cardinality of \( V(P_{m,k,K,Q_n}) \) we start by estimating the number of \( m \)-length paths connecting two different vertices at the \( n \)-dimensional hypercube.

**Remark 4.1** Let \( u_0, u_m \in V(Q_n), u_0 \neq u_m \). The number of paths with end vertices \( u_0 \) and \( u_m \) depends exclusively upon the distance \( \text{Hamming}(u_0, u_m) \).

In fact, if \( v_0, v_m \) are other vertices in \( Q_n \) with \n\[
\text{Hamming}(u_0, u_m) = \text{Hamming}(v_0, v_m) = h
\]
then \( u_m = u_0 + \sum_{i=1}^{h} e_{k_i} \) and \( v_m = v_0 + \sum_{i=1}^{h} e_{k_i} \), where the index sets \( \{k_1, \ldots, k_h\} \), \( \{k_1', \ldots, k_h'\} \) are \( h \)-subsets in \( \{1, \ldots, n\} \), i.e. sets with exactly \( h \) elements. For any permutation \( \pi \) of \( \{1, \ldots, n\} \) such that \( \{\pi(k_1), \ldots, \pi(k_h)\} = \{k_1', \ldots, k_h'\} \)
we have that any \( m \)-path \( u_0u_1 \cdots u_m \) with \( u_j = u_0 + \sum_{i=1}^{j} e_{\pi(i)} \), for \( j = 1, \ldots, m \), determines the \( m \)-path \( v_0v_1 \cdots v_m \) where \( v_j = v_0 + \sum_{i=1}^{j} e_{\pi(i)} \) for \( j = 1, \ldots, m \). Hence, the \( m \)-paths connecting \( u_0 \) with \( u_m \) can be put in a bijective correspondence with the \( m \)-paths connecting \( v_0 \) with \( v_m \).

Therefore, without losing any generality, we may assume \( u_0 = 0^{(h)}0^{(n-h)} \) and \( u_m = 1^{(h)}0^{(n-h)} \). Let \( N(n, h, m) \) denote the number of \( m \)-paths connecting \( u_0 \) and \( u_m \). The following remarks are evident:

- If either \( m < h = \text{Hamming}(u_0, u_m) \) or \( m \mod 2 = h \mod 2 \), then \( N(n, h, m) = 0 \).
- If \( m = h \), then \( N(n, h, m) = m! \).
- If \( m > \text{Hamming}(u_0, u_m) \) and \( m > n \), then \( N(n, h, m) > m! \).

The experimental calculations allow to expect that the growth of \( N(n, h, m) \) exceeds the growth of \( m! \):

\[
m \mod 2 = h \mod 2 \implies m! = o(N(n, h, m))
\]

From the simulations explained in the following section, we have checked that no Berge graph appeared in the trajectory graphs. However, this result is sufficient to claim that a general result holds:

**Proposition 4.1** Let \( m \in \mathbb{Z}^+ \) be a fixed length for the connecting paths. If there exists an \( n_0 \in \mathbb{N} \) such that for any set \( K_0 \) of \( k \) pairwise disjoint vertex pairs in the \( n_0 \)-dimensional hypercube \( Q_{n_0} \), the graph \( P_{m,k,K_0,Q_{n_0}} \) is not a Berge graph, then for any \( n \geq n_0 \) and any set \( K \) of \( k \) pairwise disjoint vertex pairs in the \( n \)-dimensional hypercube \( Q_n \), the graph \( P_{m,k,K,Q_n} \) is not a Berge graph.

**Proof.** Let \( n_0 \) and \( k \) be as in the proposition statement. Let \( n \) be an integer such that \( n \geq n_0 \) and let \( K \) be a collection of \( k \) pairwise disjoint vertex pairs in the \( n \)-dimensional hypercube \( Q_n \). Let \( N_0 \subseteq \{1, \ldots, n\} \) be an \( n_0 \)-index subset and let

\[
K_1 = \{(\pi_{N_0}(x_0x_1), \pi_{N_0}^{-1}(x_1x_0)) | (x_0x_1) \in K \}
\]

and let \( K_0 \) be a maximal subset of \( K_1 \) consisting of pairwise disjoint vertex pairs, then \( \text{card}(K_0) = k_0 \leq k \).

Let \( \lambda_{n_0} : Q_{n_0} \to \{0, 1\}^{\mathbb{N}_0} \) be the natural identification consisting of just a renumbering of the
coordinates and let \( \tau_{N_0,n} : \{0, 1\}^N \to Q_n \) be the embedding map consisting of padding with zero values the entries with index out of \( N_0 \).

Then \( \lambda_{n_0} \circ \tau_{N_0,n} \) is an embedding of the \( n_0 \)-dimensional hypercube \( Q_{n_0} \) into the \( n \)-dimensional hypercube \( Q_n \). Via \( \lambda_n \circ \tau_{N_0,n} \), the graph \( P_{m,k,K,Q_{n_0}} \) is identified with a subgraph of \( P_{m,k,K,Q_n} \).

Since \( P_{m,k,K,Q_{n_0}} \) is not a Berge graph, neither can be \( P_{m,k,K,Q_n} \).

On the other hand, it can be observed that neither sparse graphs nor their complements do appear. Evidently, neither claw-free graphs are produced.

Thus the currently known polynomial-time methods \( [4, 7] \) to find maximal independent sets do not apply to the introduced graphs \( P_{m,k,K,Q_n} \).

## 5 Computational Results

In Table 1 we give an exact calculation obtained experimentally for some particular values of \( n, m \) and \( h \).

**Table 1.** Count of the 8-paths \((m = 8)\) connecting a pair of points at distance \( h \) in the hypercube \( Q_n \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>2</th>
<th>4</th>
<th>6</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>10 056</td>
<td>12 552</td>
<td>14 400</td>
<td>-</td>
</tr>
<tr>
<td>7</td>
<td>22 960</td>
<td>26 880</td>
<td>29 520</td>
<td>-</td>
</tr>
<tr>
<td>8</td>
<td>43 740</td>
<td>46 728</td>
<td>44 640</td>
<td>40 320</td>
</tr>
</tbody>
</table>

In our experiments, we have been restricted to \( n = 6, 7, 8 \). And thus, we implemented the vertex counting at \( P_{m,k,K,Q_n} \) for \( k = 8, 16, 32 \) and \( m \) with fixed value 8, where \( k \) is the number of the given connectable pairs, and \( m \) is the length of the required paths. We have performed one hundred simulations for each value of \( n \) in \( \{6, 7, 8\} \) and in all cases, the graph \( P_{8,k,K,Q_n} \) or its complement contained induced cycles with five or more vertices.

### Algorithm 5.1: Path graphs random generation

**Input:** A path graph \( P_{m,k,K,Q_n} \), \( k < 5 \) an odd integer.

**Output:** An odd-hole \( \pi \) if exists.

**Algorithm 5.2: Odd-hole search**

We propose algorithm 5.1 to compute path graphs and algorithm 5.2 to search odd-holes within a given path graph.

Our programs implement a series of basic modules (BM):

1. BM 0: Given a positive integer \( n \) this module generates a Hamiltonian cycle \( h \) in the hypercube \( Q_n \).
This work opens the possibility to carry out many applications, particularly, in cryptography. The stated Skein Problem can be used to design authentication challenge-response protocols or to implement key exchange protocols.

In the same way, based on the Skein Problem, appropriate protocols arise for such different environments as conventional computing, mobile computing, and several communication platforms.

7 Conclusions

Finding maximum independent sets in graphs is a classical NP-hard problem. So, it is possible to profit of it for authentication purposes. In a naive approach, one may use a huge graph as a private key and a maximum independent set as the public one, but several difficulties arise: the first is the manipulation of the graph which may require hundreds of megabytes to offer an acceptable security level, and the second difficulty is to find maximum independent sets to act as the public key.

Skein problems override these difficulties. The path graphs in the hypercube play the role of hard instances, and the corresponding maximum independent sets to be used as public keys can be easily found from Hamiltonian cycles in the hypercube. On the other hand, finding maximum independent sets in path graphs is a very difficult problem due to their size, even for hypercubes of relatively small dimensions.

This is a first intended paper in a series planned to publish the cryptographic protocols and their robustness. Now, we have introduced the skein problems and we discussed their most basic mathematical properties in a purely Graph Theory approach.

6 Contributions and Applications

We introduced a family of problems, globally named “skein problems”. They were posed on general graphs and in particular, on the hypercube. These problems are reduced into the problem of finding independence subsets in graphs, which poses by itself an NP-hard problem and hard even to be approximated (in other words, it is PTAS-hard), and we provide evidence that the obtained reduced graphs are not Berge graphs, thus they are not suitable to be treated by the currently known polynomial-time approaches to solve the independence problem.

In general, from a Hamiltonian cycle in a graph, it is easy to show a family of non-crossing and pairwise disjoint paths connecting, obviously, the extreme vertex pairs. However, the converse of this problem is extremely difficult. This could be used in cryptographic protocols where the public-key corresponds to the path end vertices, and the private key is just the skein, namely, the set of non-crossing paths connecting them pairwisely.

References


Feliú Salgols holds a Ph.D. in Electrical Engineering. He is professor at Center for Research and Advanced Studies of the National Polytechnic Institute of Mexico (CINVESTAV-IPN) in Mexico City, within the Mathematics Department. His areas of interest are computing, combinatorics, graph theory, and topological graph theory. He has developed several computational tools to represent combinatorial maps, producing efficient methods to build GIS.

Guillermo Morales-Luna is researcher at the Computer Science Department at CINVESTAV-IPN in Mexico City. He holds a Bachelor degree in Physics and Mathematics from the National Polytechnic Institute in Mexico, an M.Sc. in Mathematics from CINVESTAV-IPN and a Ph.D. in Mathematics from the Mathematical Institute of the Polish Academy of Sciences in Warsaw, Poland. His areas of interest are the mathematical foundations of computer science, logic and automatic deduction, cryptography and complexity theory. He has taught at the National Polytechnic Institute (IPN) and BUAP and he has spent two sabbatical years at the Mexican Petroleum Institute (IMP).

Israel Buitron-Damaso is a Ph.D. student at the Computer Science Department in CINVESTAV-IPN in Mexico City. He holds a Bachelor degree in Computer Systems Engineering from IPN in Mexico City, and an M.Sc. in Computer Science from CINVESTAV-IPN. His research interests include cryptography, authentication protocols, information security, among others.

Article received on 13/10/2014; accepted on 04/12/2015.
Corresponding author is Israel Buitrón-Damaso.