2B-2

Minimum Certificate Dispersal with Tree Structures

Taisuke Izumi† Tomoko Izumi‡ Hirotaka Ono⋆ Koichi Wada†*
† Graduate School of Engineering, Nagoya Institute of Technology,
‡ College of Information Science and Engineering, Ritsumeikan University,
⋆ Department of Economic Engineering, Kyushu University

Background and Motivation. Let $G = (V, E)$ be a graph and $R \subseteq \{\{x, y\} \mid x, y \in V\}$ be a set of pairs of vertices, which represents requests about reachability between two vertices. For given G and R, we consider an assignment of a set of edges to each vertex in G. The assignment satisfies a request $\{u, v\}$ if the union of the edge sets assigned to u and v contains a path between u and v. The *Minimum Certificate Dispersal Problem (MCD)* is the one to find an assignment satisfying all requests in R that minimizes the sum of the cardinality of the edge set assigned to each vertex.

This problem is motivated by the design of public-key certificate based security systems, which is known as a major technique for supporting secure communication in a distributed system [1, 2, 3, 4, 5, 6, 7, 8]. A public-key certificate contains the public key of a user v encrypted by the private key of another user u. If a user u knows the public key of another user v, user u can issue a certificate from u to v. Any user who knows the public key of u can use it to decrypt the certificate from u to v for obtaining the public key of v. All certificates issued by users in a network can be represented by a certificate graph: Each vertex corresponds to a user and each directed edge corresponds to a certificate. When a user w has communication request to send messages to a user v securely, w needs to know the public key of v to encrypt the messages with it. To satisfy a communication request from a vertex w to v, vertex w needs to get vertex v's public-key. To compute v's public-key, w uses a set of certificates stored in w and v in advance. Therefore, in a certificate graph, if a set of certificates stored in w and v contains a path from w to v, then the communication request from w to v is satisfied. In terms of cost to maintain certificates, the total number of certificates stored in all vertices must be minimized for satisfying all communication requests.

MCD in the most general setting where G is a directed graph has been shown to be LOGAPX-complete, that is, it is $O(\log |V|)$-approximable in polynomial time but has no polynomial time algorithm whose approximation factor is better than $0.2266 \log |V|$ unless P=NP [5]. In this paper, we consider the computational complexity of MCD for more practical topologies of G and R, that is, when G or R forms a tree; a tree structure is frequently adopted to construct an efficient communication network. In fact, many practical applications such as DNS (Domain Name System) adopts bidirectional tree structures, and also physical network structures reflect such tree structures; it is interpreted that G forms an undirected tree. Furthermore, many applications on overlay network utilize tree structures.

Another motivation to focus on tree structures is that observation on tree might give some useful information, since a tree is a minimal connected structure. For example, even if G (resp., R) is not a tree, by solving MCD for G', a spanning tree of G (resp., for a spanning tree R' of R), we can obtain an upper bound on the optimal solution (resp., a lower bound on the optimal solution) of the original MCD problem.

Related Work. The previous work mainly focuses on directed variants of MCD, in which graph G is directed. Jung et al. discussed MCD with a restriction of available paths in [6] and proved that the problem is NP-hard. In their work, to assign edges to each vertex, only the restricted paths that are given for each request is allowed to be used. MCD with no restriction about available paths was first formulated in [8]. This variant is also proved to be

*email:t-izumi@nitech.ac.jp

NP-hard even if the input graph is a strongly connected directed graph. On the other hand, MCD for directed graphs with R forming a clique is polynomially solvable for bidirectional trees and rings, and Cartesian products of graphs such as meshes and hypercubes [8].

After these work, the (in)approximability of MCD for directed graphs has been studied from the viewpoint of the topological structure of R (not G) [5]. the (in)approximability of MCD for directed graphs is investigated for general case and R forming a clique, as a typical community structure. As mentioned above, it was shown that the former case is $O(\log |V|)$-approximable in polynomial time but has no polynomial time algorithm whose approximation factor is better than $0.2266 \log |V|$ unless P=NP. The latter case is 2-approximable but has no polynomial time algorithm whose approximation factor is better than 1.001, unless P=NP. In [5], the undirected variant of MCD is also considered, and 1.5-approximation algorithm for the case when R forming a clique is presented.

Our Contribution. We investigate the complexity of MCD with tree structure. Here, we say "with tree structure" in two senses. One is the case when R forms a tree, and the other is the case when G itself is a tree.

For MCD with tree R, we show that the hardness and approximability depend on the *maximum degree* Δ of tree R: MCD for tree R with constant degree is solvable in polynomial time while that with $\Omega(n)$ degree is APX-hard. As for MCD for tree G, we present a polynomial time algorithm. The followings are summary of our contributions:

R is an arbitrary tree: First we consider MCD for the case when R is a *star*. Even in this simplest setting, MCD is shown to be APX-hard: MCD for undirected graph G with sparse R is still APX-hard. Moreover, the reduction *to* the Steiner tree problem for unweighted graphs(STREE) leads to an upper bound 1.28 on approximation ratio for MCD with star request sets. For arbitrary tree R, it is shown that there is a 2.56-approximate algorithm for MCD by utilizing the approximation algorithm for star R.

R is a tree with $\Delta = O(\log |V|)$: By using a similar analysis to arbitrary tree R, the upper bound of approximation ratio for MCD can be reduced to 2. In particular, if R is a star with $\Delta = O(\log n)$ MCD is polynomially solvable.

R is a tree with constant degree: This case is polynomially solvable. These imply that the hardness of MCD for tree R heavily depends on its maximum degree. A key idea is to define normal solutions. Our dynamic programming based algorithm searches not the whole solution space but (much smaller) normal solution space.

G is an arbitrary tree: In this case also, a positive result is shown. For any request set R (not restricted to a tree), our algorithm outputs an optimal solution in $O(n^{1+\epsilon}|R|)$ time ($\epsilon > 0$) while a naive algorithm takes $O(n^{1.5}|R|)$ time. In the naive algorithm, a polynomial time algorithm for VERTEX-COVER problem on bipartite graphs, which can be solved via the maximum matching algorithm, is applied for each edge in G. Our algorithm realizes the improvement of computation time by exploiting the *reoptimization* of MATCHING problem for bipartite graphs.

References

[1] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE Trans. on Mobile Computing*, 2(1):52–64, March 2003.

[2] M. G. Gouda and E. Jung. Certificate dispersal in ad-hoc networks. In *ICDCS*, pages 616–623, March 2004.

[3] M. G. Gouda and E. Jung. Stabilizing certificate dispersal. In *SSS*, October 2005.

[4] J. Hubaux, L. Buttyan, and S. Capkun. The quest for security in mobile ad hoc networks. In *Mobihoc*, pages 146–155, October 2001.

[5] T. Izumi, T. Izumi, H. Ono, and K. Wada. Approximability and inapproximability of the minimum certificate dispersal problem. *Theoretical Computer Science*, 411(31-33):2773–2783, June 2010.

[6] E. Jung, E. S. Elmallah, and M. G. Gouda. Optimal dispersal of certificate chains. In *DISC*, pages 435–449, October 2004.

[7] H. Zheng, S. Omura, J. Uchida, and K. Wada. An optimal certificate dispersal algorithm for mobile ad hoc networks. *IEICE Trans. on Fundamentals*, E88-A(5):1258–1266, May 2005.

[8] H. Zheng, S. Omura, and K. Wada. An approximation algorithm for minimum certificate dispersal problems. *IEICE Trans. on Fundamentals*, E89-A(2):551–558, February 2006.