More Graph Drawing in the Cloud: Data-Oblivious st-Numbering, Visibility Representations, and Orthogonal Drawing of Biconnected Planar Graphs

Michael T. Goodrich and Joseph A. Simons

Department of Computer Science, University of California, Irvine, USA
{goodrich,jsimons}@uci.edu

Abstract. We give a new efficient data-oblivious PRAM simulation and several new data-oblivious graph-drawing algorithms with application to privacy-preserving graph-drawing in a cloud computing context.

Keywords: Data-Oblivious, Cloud Computing, st-Numbering, Visibility Representation, Orthogonal Drawing.

1 Introduction

Cloud computing is a work-flow paradigm where a client outsources her data to external servers administered by a third party so that she can reliably access her data from anywhere using any computational device. Moreover, the client gains these features of reliability and availability often at very low cost (sometimes they are even free). Still, there are some drawbacks, with one of the most significant being the loss of privacy that can occur from outsourcing one's data to a third party. Indeed, some cloud computing companies have based their business models on their ability to mine client data for useful information. Thus, it is useful to design methods that allow for privacy-preserving access to data in the cloud.

In this paper, we are interested in a privacy-preserving data access technique that is based on the use of data-oblivious algorithms, that is, algorithms where the sequence of data accesses is independent of the data values. Such algorithms are useful for cloud computing, since combining them with a semantically-secure encryption scheme will not reveal data values nor data access patterns.

We are particularly interested in methods that avoid the use of constant-time random oracles, since the existence of such functions is considered a strong assumption in the cryptographic literature. We only consider algorithms that only require storage on the client that is logarithmic in the number of data items stored on the server.

The best existing data-oblivious RAM simulation which does not require random oracles [1] increases the running time by $O(\log^3 n)$ factor. Thus, it is desired for us to design data-oblivious graph drawing methods that have running times that are factors of at most $o(\log^3 n)$ from the asymptotically fastest existing methods.

W. Didimo and M. Patrignani (Eds.): GD 2012, LNCS 7704, pp. 569–570, 2013.
© Springer-Verlag Berlin Heidelberg 2013

2 Results

Motivated by graph drawing in a cloud-computing context, we give a new efficient method for simulating parallel algorithms in the data-oblivious model. Our method is significantly simpler and asyptotically more efficient than existing data-oblivious RAM simulations. As applications we give new data-oblivious graph drawing algorithms for classic graph drawing problems including st-numbering, visibility representations, upward grid drawings, and orthogonal grid drawings of planar graphs.

Theorem 1. *Suppose A is a CRCW PRAM algorithm that runs in T steps using a memory of size N and $P \leq N$ processors. Then one can simulate A sequentially in a data-oblivious fashion in $O(TN \log N)$ time without the use of random oracles.*

Proof: (sketch). At each time step each parallel processor either reads memory, writes to memory, or performs a small computation. We obliviously sort read, write, and compute requests and simulate them sequentially and data-obliviously building on the compressed-scanning model given in [3]. Details omitted from this short abstract. □

Note that this theorem applies to one of the most powerful versions of the CRCW PRAM model. Thus, it also applies to any weaker model, including the CREW and EREW PRAM models.

We apply our simulation result to achieve data-oblivious algorithms for classic PRAM graph drawing algorithms such as those given in [2, 4].

Corollary 1. *Given a biconnected planar graph G with n vertices, in $O(n \log^2 n)$ time we can data-obliviously compute the following: an st-numbering of G; an orientation of G as an st-graph; a visibility representation for G; an upward polyline grid drawing of G with $O(n)$ bends; a planar orthogonal grid drawing of G with $O(n)$ bends. All drawings are in an integer grid of $O(n^2)$ area.*

Acknowledgements. This work was supported in part by NSF grant 0830403 and by the Office of Naval Research under grant N00014-08-1-1015.

References

1. Damgård, I., Meldgaard, S., Nielsen, J.B.: Perfectly Secure Oblivious RAM without Random Oracles. In: Ishai, Y. (ed.) TCC 2011. LNCS, vol. 6597, pp. 144–163. Springer, Heidelberg (2011)
2. Gazit, H.: Optimal EREW parallel algorithms for connectivity, ear decomposition and st-numbering of planar graphs. In: IPPS, pp. 84–91 (1991)
3. Goodrich, M.T., Ohrimenko, O., Tamassia, R.: Graph Drawing in the Cloud: Privately Visualizing Relational Data Using Small Working Storage. In: Didimo, W., Patrignani, M. (eds.) GD 2012. LNCS, vol. 7704, pp. 43–54. Springer, Heidelberg (2013)
4. Tamassia, R., Vitter, J.S.: Optimal parallel algorithms for transitive closure and point location in planar structures. In: SPAA, pp. 399–408 (1989)