Electronic Colloquium on Computational Complexity - Reports Series 1996 - available via:

Comment 01 on
ECCC TR96-054

FTP: ftp.eccc.uni-trier.de:/pub/eccc/
WWW: http://www.eccc.uni-trier.de/eccc/
Email: ftpmail@ftp.eccc.uni-trier.de with subject 'help eccc'

The Graph Clustering Problem has a Perfect Zero-Knowledge Proof

Alfredo De Santis * Giovanni Di Crescenzo † Oded Goldreich ‡
Giuseppe Persiano §

January 28, 1998

We have posted, as TR98-006, an improvement over TR96-054. Whereas TR96-054 considers the parametrized (by sequence of integers) problem, the new posting refers to the non-parametrized version where these integers are part of the input. Follwing are the two formulations.

TR96-054 The Graph Clustering Problem is parameterized by a sequence of positive integers, $m_1, ..., m_t$. The input is a sequence of $\sum_{i=1}^{t} m_i$ graphs, and the question is whether the equivalence classes under the graph isomorphism relation have sizes which match the sequence of parameters.

TR98-006 The input to the *Graph Clustering Problem* consists of a sequence of integers $m_1, ..., m_t$ and a sequence of $\sum_{i=1}^{t} m_i$ graphs. The question is whether the equivalence classes, under the graph isomorphism relation, of the input graphs have sizes which match the input sequence of integers.

Each of the TRs shows that the corresponding formulation of the problem has a (perfect) zero-knowledge interactive proof system.

*Dipartimento di Informatica ed Appl., Università di Salerno, 84081 Baronissi (SA), Italy. E-mail: ads@dia.unisa.it.

†Computer Science and Engineering Department, University of California San Diego, 92093 La Jolla, CA, USA. E-mail: giovanni@cs.ucsd.edu.

‡Work done while visiting MIT. E-mail: oded@lcs.mit.edu.

§Dipartimento di Informatica ed Appl., Università di Salerno, 84081 Baronissi (SA), Italy. E-mail: giuper@dia.unisa.it.