

Re: Need Graph Isomorphism Algorithm De-bunked

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-09/msg01017.html>

- *From:* Francois Grieu <fgrieu@xxxxxxxxxxxxx>
 - *Date:* Thu, 28 Sep 2006 23:14:14 +0200
-

In article <[efgqn6\\$dd6@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:efgqn6$dd6@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx)>, Mike Amling <nospam@xxxxxxxxxx> wrote:

François Grieu wrote:

I notice a fun thing: when using any variant of the algorithm to compare two graphs, we can detect with certainty when the algorithm fails, as follow.

We use the algorithm to produce a hash for each vertex.

If these hashes are not identical within order, we have proved the graphs are not isomorphic.

"proved" to the point where I believe it, but I haven't seen a formal proof.

I stand by "proved". The proof, by induction, that the graph hash produced by all variants stated so far is invariant under graph isomorphism, seems quite straightforward; this is all that is needed to prove that different hashes imply non-isomorphism.

Else, we reorder both graph's matrix according to nondecreasing hashes. If the reordered graphs are equal, we have proved the graphs are isomorphic.

Else, the algorithm failed.

I think you have to specify more than "nondecreasing". The reordered graphs are equal iff you have established an isomorphism between the two graphs, and to do that you have to cope with Bill Cox's automorphism

Re: Need Graph Isomorphism Algorithm De-bunked

issue. E.g., two graphs that are each 4 nodes connected in a ring have only 8 isomorphisms, but all the node hashes are same and there are 24 ways to sort them nondecreasing.

You are right. What I stated is strictly speaking true, but the "algorithm failed" box is reached hopelessly often.

François Grien

.