

Re: What is md5sum?

Source: <http://linux.derkeiler.com/Newsgroups/comp.os.linux.setup/2004-07/0013.html>

From: P.T. Breuer (ptb_at_oboe.it.uc3m.es)

Date: 07/01/04

Date: Thu, 1 Jul 2004 00:21:58 +0200

Micha? Kosmulski <M.Kosmulski@nospam.elka.pw.edu.pl> wrote:

> >> *A dramatic misunderstanding ! One doesn't have to show them to prove
> >> they exist.*
> >
> > *Oh, yes one does. What makes you think you don't? (you are supposed to
> > think about how you may convince me).*
> *Well, then let us play by your own rules. If you insist that to prove
> something you have to "show" it, please convince us that no two files
> have the same md5sum, as you claim.*

List all the files you know of and test their md5sums – you'll find they are all different.

> *This ought to be fairly simple: just
> create all possible files and their MD5 sums and send them to this*

No – just the files you already have, thank you. I'm not interested in what you may or may not do (I have quite enough bifurcations of my own in the universe to contend with), just the facts.

> *newsgroup, so we can read through the list and check for ourselves that
> actually no two items in the list share the same MD5 sum. Then I'll agree ;]*

I'm willing to send you any of my files that you are interested in.

> > *Fantastic, so even though you "know" that there "are" two files with
> > the same md5sum, you find yourself curiously unable to CHOOSE a pair to
> > show me!*
> *Have you never seen a proof of a mathematical theorem done by showing
> that if we assume the theorem false, we get a contradiction ?*

Of course – unfortunately proof by contradiction only holds in boolean logics, and even then only over finite domains.

> *If I can
> show that nonexistence of a number with some property X leads to a
> logical contradiction, then a number with property X does exist,*

No it doesn't – that's an axiom only of boolean logics in certain domains. One of the easiest counterexamples is to use what I already suggested – the set of infinite decimal numbers (in the range 0.000...–0.999...) that are not describable. If you assume there aren't any such, then all decimal numbers are describable, and that's in contradiction with the classical proof that the decimals are cardinally superior to the counting numbers (the set of all descriptions can be counted just by ordering them alphabetically and giving each description the index corresponding to where it appears in that ordering).

So now you would have me believe that there is an undecidable decimal number.

Which is the one you had in mind?

- > *even*
- > *though I may be unable to show it to you.*

Tut tut. I don't believe in fairies. You put up or shut up.

- > *Of course, we can change the*
- > *starting set of axioms,*

To a more accurate set?

- > *or perhaps even the logic we use.*

Removing untenable leaps of faith, for example? Belief in the excluded middle for infinite domains, perhaps?

- > *But then we*
- > *have to consider, what value such reasoning would have for learning*
- > *anything about our world.*

Why not ask the quantum logicians, the probabilistic logicians, and so on?

- > *Of course, mathematics is only a model etc etc; but thus far it has*
- > *provided us with quite a lot of good ideas and has found a few uses in*

You seem to think that mathematics is stuck in socrates time. It isn't. In the 1930s Cohen proved the independence of the axiom of choice from the other "axioms" (and the independence of the continuum hypothesis), Goedel provided an example of a true statement of arithmetic that was not provable, and so on. We got rid of a lot of untenable assumptions that at the time of the 1900s attempts to set mathematics on a formal basis, seemed irrefutably self-evident. Wake up to the last century's work.

- > *different branches of science and technology. If someone invents a*
- > *better tool for this job, I'll switch immediately :)*

comp.os.linux.setup: Re: What is md5sum?

- > *Then again, there is one more thing nobody has pointed out so far. All*
- > *our estimations of how probable a collision in MD5 is were based on the*
- > *assumption that MD5 is a really perfect hash function. The sad truth is*

No, they weren't. They were predicated on our lack of knowledge.

Peter