

MANY CHEERFUL FACTS

presents

Hash is Hard.

a talk by Ed Carter

12:10 pm - 1:00 on Wednesday, March 16th, in room
1015.

In this talk, I will discuss the problem of constructing a robust graph enumeration or hash. We want a function from the set of directed graphs to the set of natural numbers such that both it and a partial inverse of it can be computed efficiently. The function should also have the property that small changes to the graph leads to a small change in the output of the function. I will show what properties such a function should have for the application of software watermarking, show some basic attempts at producing such a function, why each of those attempts doesn't work all that well, and an NP -completeness result concerning this problem.

o Check out the new(ish) MCF website: <http://math.berkeley.edu/~brownda/cheers/>

*I am the very model of a modern Major General,
I've information vegetable, animal, and mineral,
I know the kings of England, and I quote the fights historical
From Marathon to Waterloo, in order categorical;
I'm very well acquainted, too, with matters mathematical,
I understand equations, both the simple and quadratical,
About binomial theorem I'm teeming with a lot o' news,
With many cheerful facts about the square of the hypotenuse!*

- Gilbert & Sullivan $P \circ P$