

1046-12-1953

Gregory V Bard* (bard@fordham.edu), Department of Mathematics, John Mulcahey Hall
Room 421, Fordham University, The Bronx, NY 10458. *Solving an Intellectual Property Problem
via A System of Polynomial Equations over $GF(2)$* . Preliminary report.

Suppose there is some circuit which is believed to be functionally identical to some other circuit, i.e. equal to it for all possible inputs. All digital circuits can be represented as systems of polynomial equations, and searching for a solution to $p(x) + q(x) = 1$ is logically equivalent to the question $\exists x$ st $p(x) \neq q(x)$.

However, if one does not know which inputs of one represent which inputs of the other then the problem becomes much harder. For n inputs, there are $n!$ possible permutations, e.g. $n!$ instantiations of the problem in the previous paragraph would have be solved. However, I will present a technique that will solve the system with $\log n$ additional variables in the system of equations, and only 1 instantiation. (Received September 16, 2008)