An inverter for an algorithm $A$ is another algorithm $I$ such that for any $y \in \text{ran } A$, the value $x = I(y)$ is a preimage of $y$ s.t. $A(x) = y$. An inverter for $A$ is optimal if the combined run-time of computing $I(y)$ and verifying $A(I(y)) = y$ is minimal up to a polynomial among all algorithms for this task.

The existence of optimal inverters for all algorithms was shown by Levin [1]. This paper surveys applications of this result, in particular several recent ones by the authors.

The classic application of optimal inverters is the existence of an algorithm $A$ for the NP-complete problem SAT, the satisfiability problem for classical propositional logic, such that $A$ runs in polynomial time if and only if $P = NP$.

Among the applications presented are some results concerning the (conditional) existence or non-existence of algorithms satisfying other notions of optimality, notably optimal acceptors and optimal proof systems. There are also other applications that are on the surface not related to optimal algorithms, like a new proof of Gödel’s incompleteness theorem, or a result relating different versions of the Exponential Time Hypothesis and the Clique problem.

References