

From Goldwasser's talk:

A very simple example of a σ -knowledge proof.

A: I claim that y is a square mod N .

Indeed, I've chosen a random r & set $z = r^2 \bmod N$. I'll show you z . on your request I'll show either

a. z is a square mod N .

b. yz is a square mod N .

IF both are true, clearly y is a square mod N . Which do you want me to show?

From Lott's talk: IF M is a compact metric space, so is $P(M)$ (prob. measures on M) in the optimal transport metric. To what extent is $P(M)$ an ∞ -dim manifold?