Harder Problems are Sometimes Easier

Ohad Asor

January 22, 2016

Abstract

We show a false "information theoretic proof" that factorization is easier than radix change. This is of course not true.

Say I'd like to pass you some information in form of a number X, say $X = 100$. I could represent it as 100 lines or dots, and that'd be called a unary representation. I could also write it in binary representation: 1100100. Or I could simply use decimal representation: 100. I could also give you the prime factors of the numbers: $2, 2, 5, 5$. But the prime representation and the radix representation have some essential difference.

Using n digits in radix b we can express b^n distinct numbers. Observe the simple combinatorial interpretation: we may choose n digits while we may choose every digit more than once, and the order matters. On the other hand, prime factorization does indeed allow using the same prime more than once - but it is agnostic to order.

For the case of binary radix comparing to unary, we therefore get a compressed representation of order $\log X$. For the case of factors comparing to binary we get an asymptotic order of magnitude of $\log X \log\log X$. We then conclude that binary (or higher) radix representation is essentially and inherently stronger and more efficient compression than factoring.

So, "the obvious conclusion" is: integer factorization is harder than radix change! Because it is simply a task that asks for a stronger result, at least when interpreted at some certain sense.

This of course does not reflect reality. In reality, we can change radix very efficiently, but we (still?) cannot factor integers efficiently, and it is widely believed to simply be impossible.