Law of Sub-Solution-Type Problem Simplification

by Sven Nilsen, 2018

Assume a problem is encoded a function `f` which takes a variable `x` and returns `true` if it is a solution and `false` otherwise. When a such solution exists, one can extract a maximizing sub-type, gradually by investing some work that tends to give high returns on low investments. The sub-type contains the known solution and where every variable satisfying the sub-type is a solution:

$x : [g]\ [f[g \rightarrow id]]\ true$ $\qquad$ $y : [g]\ g(x) \land (\neg= x)$ is used to extract more solutions

$x : [f]\ true$
$f : A \rightarrow bool$
$g : A \rightarrow B$
$f[g \rightarrow id] : B \rightarrow bool$

This formalizes what it means to first create something that works and then polishing it. With other words, finding one solution to the problem is a shortcut to reducing part of the problem to a simpler version to solve, for which every solution to the simpler problem is a solution to the harder problem.

For example, consider a Pythagorean triple in modulus 256 (8 bit unsigned integer):

$a^2 + b^2 = c^2 \qquad \text{mod } 256$

Normally, to solve for `b`, one would find the sub-type of all solutions by solving the equation:

$a^2 + b^2 = c^2$
$b^2 = c^2 - a^2$
$b : [pow\ 2]\ (c^2 - a^2)$

However, in complex problems it is often not possible to find the sub-type of all solutions, or one might want to try properties of old solutions in new situations. Instead of looking for all solutions, one is satisfied with finding a sub-solution-type. With other words, one is not interested in doing the whole work but a quick and lazy of finding more solutions, sometimes not even doing all calculations.

When one solution is found, e.g. `b = 3`, one can look at the expression(s) that depends on it and extract a sub-type which contains at least the solution that has already been found:

$4^2 + b^2 : (= 3^2) = 5^2$	Inject solution and ignore everything that does not depend on `b`
$b^2 = 9$	Extracted as equation
$b : [pow\ 2]\ 9$	Extracted as sub-type

The other numbers in modulus 256 that satisfies this sub-type are: 125, 131 and 253. It turns out that these are all solutions to the equations, because `$5^2 - 4^2 = 9$`. Yet, it was not necessary to solve the whole equation, which demonstrates that this technique tends to give high returns on low investment.