Supplementary to Lecture 8

Richard Cleve

There is a broader generalization of the Simon property than the one given on slide 6 of Lecture 8.

The ℓ-to-1 Simon mod m property

Let d, m, and ℓ be positive integers, where ℓ is a divisor of m. Let $f : (\mathbb{Z}_m)^d \to T$ be an ℓ-to-1 function.

Definition: *An ℓ-to-1 function $f : (\mathbb{Z}_m)^d \to T$ satisfies the **ℓ-to-1 Simon mod m property** provided that there exists an $r \in (\mathbb{Z}_m)^d$ such that, for all $a, b \in (\mathbb{Z}_m)^d$, it holds that $f(a) = f(b)$ if and only if $a - b$ is a multiple of r.*

This is equivalent to the colliding sets of f being of the form $\{a, a+r, a+2r, \ldots, a+(\ell-1)r\}$.

Running the quantum circuit given in the lecture with queries for such a function yields a uniformly generated element of the set $\{b \in (\mathbb{Z}_m)^d \,:\, b \cdot r = 0\}$, where each such b occurs with probability ℓ/m^d.

Simon mod m property in Lecture 8

This is the special case where $\ell = m$. This special case is what arises from the function constructed for the discrete log problem.