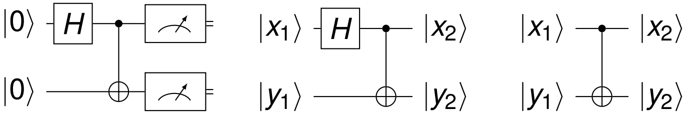
Partial Evaluation of (Quantum) Circuits

Jacques Carette, Amr Sabry, Gerardo Ortiz

WG 2.11, Odense, Denmark

Quantum Circuit



(a) Bell circuit (b) Quantum core (c) Classical core

Legend:

$$|0\rangle = \text{false} = 0$$

$$|1\rangle = \text{true} = 1$$

Examples part I

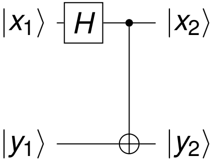


Figure: Quantum core

Examples part II

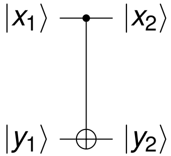


Figure: Classical core

Real Examples

1. Deutsch
2. Deutsch-Jozsa
3. Bernstein-Varizani
4. Simon
5. Grover
6. Shor

Real Examples

1. Deutsch
2. Deutsch-Jozsa
3. Bernstein-Varizani
4. Simon
5. Grover
6. Shor

caveat: Black-Box vs White Box

Deutsch

Problem

Given $f : \mathbb{B} \to \mathbb{B}$*, decide if* f *is constant or balanced.*

Deutsch

Problem

Given $f : \mathbb{B} \to \mathbb{B}$, decide if f is constant or balanced.

Definition

*A boolean function is **balanced** if it outputs the same number of 0/1 outputs.*

Deutsch

Problem

Given $f : \mathbb{B} \to \mathbb{B}$, decide if f is constant or balanced.

Definition

*A boolean function is **balanced** if it outputs the same number of 0/1 outputs.*

$$|x\rangle\,|y\rangle \to |x\rangle\,|f(x) \oplus y\rangle$$

Deutsch-Josza

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$, where f is known to be constant or balanced, decide which one it is.

Deutsch-Josza

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$, where f is known to be constant or balanced, decide which one it is.

Sample outputs:

- $0 = 0$
- $x_0 = 0$,
- $x_0 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 = 0$, and
- $1 \oplus x_3 x_5 \oplus x_2 x_4 \oplus x_1 x_5 \oplus x_0 x_3 \oplus x_0 x_2 \oplus x_3 x_4 x_5 \oplus x_2 x_3 x_5 \oplus x_1 x_3 x_5 \oplus x_0 x_3 x_5 \oplus x_0 x_1 x_4 \oplus x_0 x_1 x_2 \oplus x_2 x_3 x_4 x_5 \oplus x_1 x_3 x_4 x_5 \oplus x_1 x_2 x_4 x_5 \oplus x_1 x_2 x_3 x_5 \oplus x_0 x_3 x_4 x_5 \oplus x_0 x_2 x_4 x_5 \oplus x_0 x_2 x_3 x_5 \oplus x_0 x_1 x_4 x_5 \oplus x_0 x_1 x_3 x_5 \oplus x_0 x_1 x_3 x_4 \oplus x_0 x_1 x_2 x_4 \oplus x_0 x_1 x_2 x_4 x_5 \oplus x_0 x_1 x_2 x_3 x_5 \oplus x_0 x_1 x_2 x_3 x_4 = 0$.

But how to *decide*? Easy: if it mentions a variable, it's balanced.

Introduction

Bernstein-Varizani, Simon

Bernstein-Varizani

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$, *where* f *is known to be of the shape* $\sum_i s_i x_i \mod 2$ *for some* $s \in \mathbb{B}^n$ *and* s_i *is its bit decomposition. Find* s.

Bernstein-Varizani, Simon

Bernstein-Varizani

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$, where f is known to be of the shape $\sum_i s_i x_i \mod 2$ for some $s \in \mathbb{B}^n$ and s_i is its bit decomposition. Find s.

Simon

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$, where it is known that there exist a such that $\forall x. f(x) = f(x + a)$. Find a.

Grover

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$ where there exists a unique x such that $f(x) = 1$. Find x.

Problem

Given $f : \mathbb{B}^n \to \mathbb{B}$ where there exists a unique x such that $f(x) = 1$. Find x.

$n = 4$, w in the range $\{0..15\}$

$u = 0$	$1 \oplus x_3 \oplus x_2 \oplus x_1 \oplus x_0 \oplus x_2x_3 \oplus x_1x_3 \oplus x_1x_2 \oplus x_0x_3 \oplus x_0x_2 \oplus x_0x_1 \oplus x_1x_2x_3 \oplus x_0x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 1$	$x_0 \oplus x_0x_3 \oplus x_0x_2 \oplus x_0x_1 \oplus x_0x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 2$	$x_1 \oplus x_1x_3 \oplus x_1x_2 \oplus x_0x_1 \oplus x_1x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 3$	$x_0x_1 \oplus x_0x_1x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 4$	$x_2 \oplus x_2x_3 \oplus x_1x_2 \oplus x_0x_2 \oplus x_1x_2x_3 \oplus x_0x_2x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 5$	$x_0x_2 \oplus x_0x_2x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 6$	$x_1x_2 \oplus x_1x_2x_3 \oplus x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 7$	$x_0x_1x_2 \oplus x_0x_1x_2x_3$
$u = 8$	$x_3 \oplus x_2x_3 \oplus x_1x_3 \oplus x_0x_3 \oplus x_1x_2x_3 \oplus x_0x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_1x_2x_3$
$u = 9$	$x_0x_3 \oplus x_0x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_1x_2x_3$
$u = 10$	$x_1x_3 \oplus x_1x_2x_3 \oplus x_0x_1x_3 \oplus x_0x_1x_2x_3$
$u = 11$	$x_0x_1x_3 \oplus x_0x_1x_2x_3$
$u = 12$	$x_2x_3 \oplus x_1x_2x_3 \oplus x_0x_2x_3 \oplus x_0x_1x_2x_3$
$u = 13$	$x_0x_2x_3 \oplus x_0x_1x_2x_3$
$u = 14$	$x_1x_2x_3 \oplus x_0x_1x_2x_3$
$u = 15$	$x_0x_1x_2x_3$

Shor

Problem

Factor a given N. Do this by using $f(x) = a^x \mod N$ for suitable a and $f : \mathbb{B}^Q \to \mathbb{B}^Q$ with $Q = \lceil \log_2 (N^2) \rceil$.

Base	Equations				Solution
$a = 11$	$x_0 = 0$				$x_0 = 0$
$a = 4, 14$	$1 \oplus x_0 = 1$	$x_0 = 0$			$x_0 = 0$
$a = 7, 13$	$1 \oplus x_1 \oplus x_0 x_1 = 1$	$x_0 x_1 = 0$	$x_0 \oplus x_1 \oplus x_0 x_1 = 0$	$x_0 \oplus x_0 x_1 = 0$	$x_0 = x_1 = 0$
$a = 2, 8$	$1 \oplus x_0 \oplus x_1 \oplus x_0 x_1 = 1$	$x_0 x_1 = 0$	$x_1 \oplus x_0 x_1 = 0$	$x_0 \oplus x_0 x_1 = 0$	$x_0 = x_1 = 0$

Auto-generated circuits: 56,538 generalized Toffoli gates. For 3*65537=196611 (4,328,778 gates), 16 small equations that refer to just the four variables x_0, x_1, x_2, and x_3 constraining them to be all 0, i.e., asserting that the period is 16.