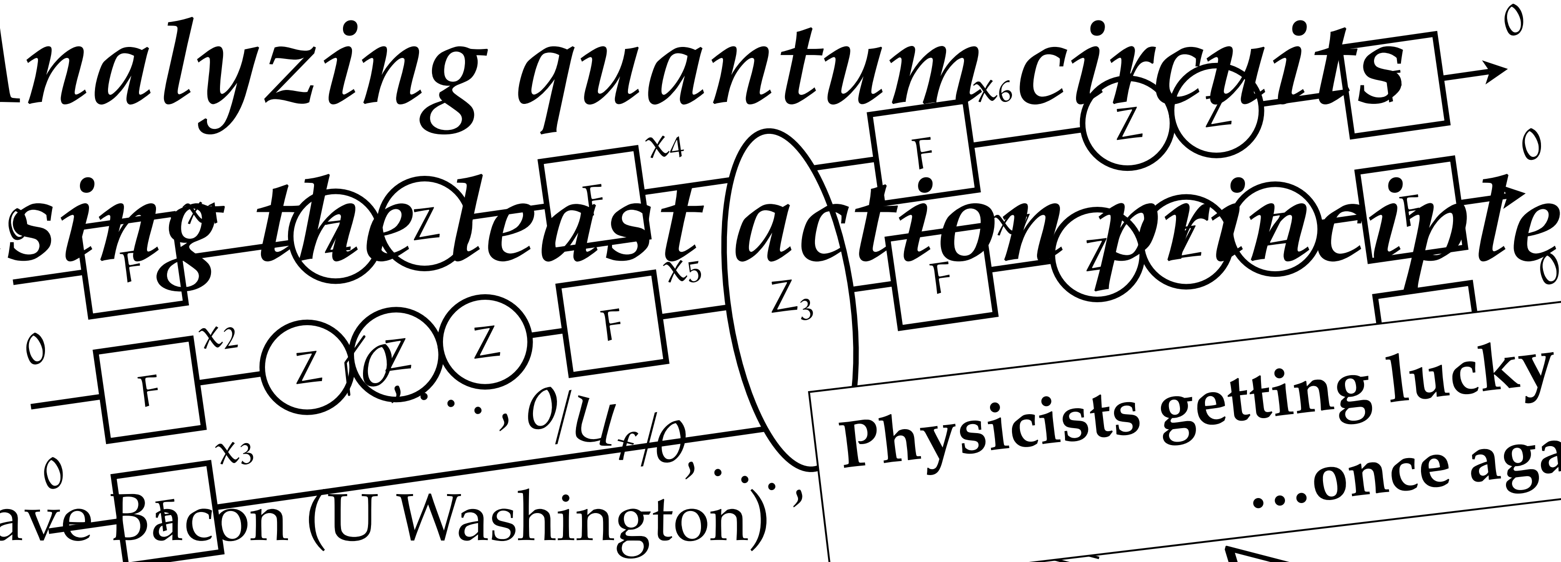
Analyzing quantum circuits using the least action principle



Physicists getting lucky…
…once again

Dave Bacon (U Washington)
Wim van Dam (UC Santa Barbara)
Alexander Russell (U Connecticut)

$$\sum_{x\in(\mathbb{Z}/m\mathbb{Z})^n} e^{2\pi i f(x)/m}$$

$$S(f) = \{ x : \nabla f(x) = (\partial f/\partial x_1,\ldots,\partial f/\partial x_n)(x) = 0 \}$$

The Twelfth Workshop on Quantum Information Processing
January 12, 2009

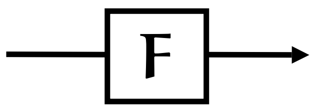
Goal:

To come up with a better understanding of quantum circuits that add, multiply and Fourier transform over arbitrary rings

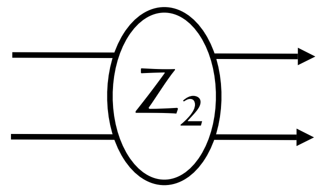
Algebraic Quantum Gates

These quantum gates are defined for any $\mathbb{Z}/m\mathbb{Z}$ ($\zeta_m = e^{2\pi i/m}$):

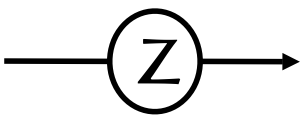
Fourier transform:



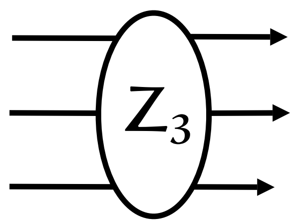
C-Phase Change:



Phase Change:



CC-Phase Change:



$|x,y,z\rangle \mapsto \zeta_m^{xyz}|x,y,z\rangle$

- Inverses are also included.
- For finite fields $\mathbb{F}_q$ we use the trace function Tr: $\mathbb{F}_q \to \mathbb{F}_p$ in the exponents.

Algebraic Quantum Circuits

Algebraic quantum circuits are made with algebraic quantum gates. Like equations such as "$Y^2 = X^3 + 2$", a single circuit can be interpreted over different rings $\mathbb{Z}/m\mathbb{Z}$ or finite fields $\mathbb{F}_q$.

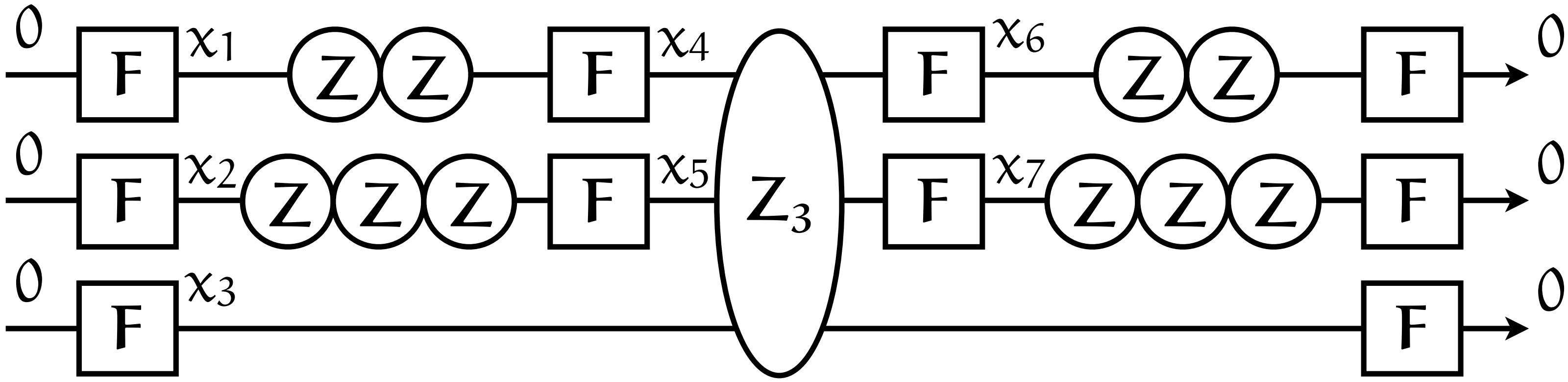
Some questions:

Which properties of the circuit are independent of m?

How does the power of the circuit grow in m or q?

Are algebraic quantum circuits more powerful than classical algebraic circuits?

An Example Algebraic Quantum Circuit



What does it do? On (0,0,0) will it output (0,0,0)?
The amplitude $\langle 000|U|000\rangle$ equals the **exponential sum**

$$\frac{1}{m^5}\sum_{x\in(\mathbb{Z}/m\mathbb{Z})^7}\zeta_m^{2x_1+3x_2+x_1x_4+x_2x_5+x_4x_5x_3+x_4x_6+x_5x_7+2x_6+3x_7}$$

The Action Polynomial

[Dawson et al. and then some]: Each algebraic quantum circuit with w wires and k Fourier transforms has an **action polynomial** $f \in \mathbb{Z}[X_1,\ldots,X_n]$ with $n=k-w$ such that over the modulo m ring $\mathbb{Z}/m\mathbb{Z}$ we have for the 'zeros-in-zeros-out' acceptance amplitude:

$$\langle 0,\ldots,0|U_f|0,\ldots,0\rangle = \frac{1}{\sqrt{m^k}} \sum_{x\in(\mathbb{Z}/m\mathbb{Z})^n} e^{2\pi i f(x)/m}$$

Note that f is independent of m.

Path summations: "The probability is determined by the battle between the interference in the sum over the m^n paths and the $m^{-k/2}$ normalization term."

Some Observations

$$\langle 0,\ldots,0|U_f|0,\ldots,0\rangle = \frac{1}{\sqrt{m^k}} \sum_{x\in(\mathbb{Z}/m\mathbb{Z})^n} e^{2\pi i f(x)/m}$$

- The x are the computational paths from $0\ldots0$ to $0\ldots0$.
- For all paths x, the magnitudes are all the same, all that matters are the phases $e^{2\pi i f(x)/m}$.
- The polynomial f has degree at most 3.
- To get a probability close to 1, the f has to be nonsingular.

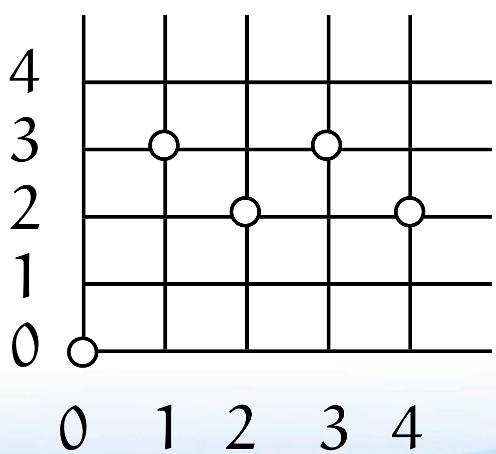
Physics-Inspired Nonsense

Least action principle: **the sum of $e^{2\pi i f(x)/m}$ terms is determined (mostly) by the *singular points***

$$S(f) = \{\, x : \nabla f(x) = (\partial f/\partial X_1,\ldots,\partial f/\partial X_n)(x) = 0 \,\}$$

of $f \in \mathbb{Z}[X_1,\ldots,X_n]$.

It is not obvious that does should make any sense for a summation over $x \in (\mathbb{Z}/m\mathbb{Z})^n$.



For $f = x^3 + 2x \bmod 5$, the points $x=1$ and $x=4$ are singular.

But it does work; crucial is the dimension of $S(f)$.

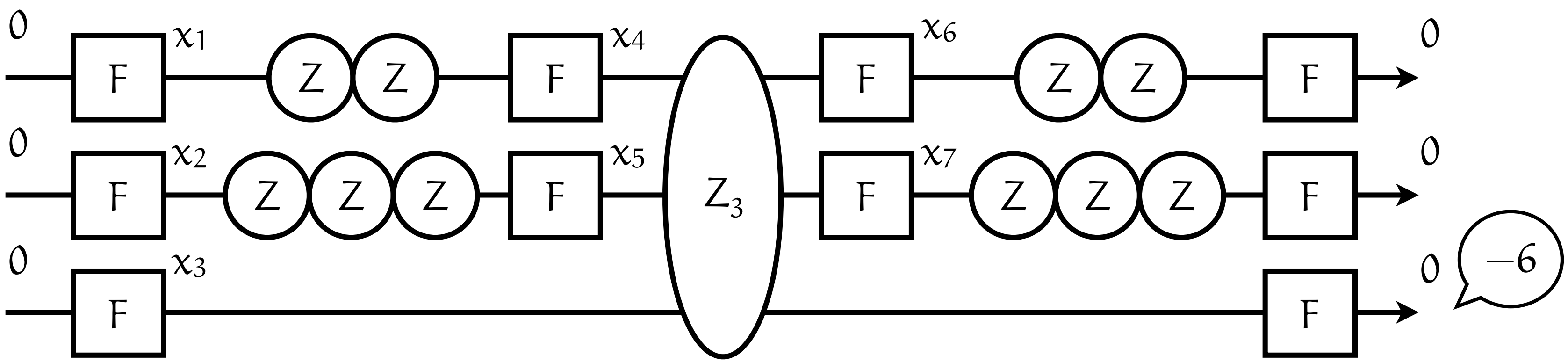
Clifford-like Algebraic Quantum Circuits

The algebraic generalization of Clifford circuits:
Linear algebraic quantum circuits do not use Z_3 gates.

Result:
A linear quantum circuit with w wires over $\mathbb{F}_q$ has acceptance probability $|\langle 0\ldots 0|U|0\ldots 0\rangle|^2 = 1/q^{w-\dim(S(f))}$.

Proof:
Diagonalize the quadratic f, use Gauss sum knowledge and the fact that $S(f)$ is a linear subspace.

Our Earlier Example



$$f = 2x_1+3x_2+x_1x_4+x_2x_5+x_4x_5x_3+x_4x_6+x_5x_7+2x_6+3x_7$$

$$\nabla f(x) = 0 \Leftrightarrow \begin{cases} x_4 = -2 \\ x_5 = -3 \\ 6 = 0 \\ x_6 = 3x_3 - x_1 \\ x_7 = 2x_3 - x_2 \end{cases}$$

If $6=0$, $\dim(S(f)) = 3$,
otherwise $\dim(S(f)) = -\infty$.

This makes perfect sense.

A Conjecture

For general algebraic quantum circuits, in the limit of large $\mathbb{Z}/m\mathbb{Z}$ or $\mathbb{F}_q$, we have

$|\langle 0\ldots 0|U|0\ldots 0\rangle|^2 \rightarrow 1$ if $\dim(S(f)) = \#\text{wires}$

$|\langle 0\ldots 0|U|0\ldots 0\rangle|^2 \rightarrow 0$ if $\dim(S(f)) < \#\text{wires}$

Other results on the large q limit and the limit $m\rightarrow\infty$ confirm that the probability goes to either 0 or 1.

For $m=p^r\rightarrow\infty$ the exponential sum is dominated by the singular points of the action polynomial f.

Parlez-Vous Géométrie Algébrique?

Séminaire BOURBAKI Février 1988
40ème année, 1987-88, n° 691

TRAVAUX DE LAUMON
par Nicholas M. KATZ

To A. Grothendieck, on his 60'th birthday

In this exposé we will try to explain Laumon's "principle of stationary phase" for the ℓ-adic Fourier Transform; where it comes from, what it is, and what it's good for.

Background: The Formalism of Fourier Transform

Let us begin by recalling the classical Fourier Transform in the case of a finite abelian group G, written additively, with Pontryagin dual group $G^\vee$. For a function f on G, its Fourier Transform FT(f) is the

Open Question:

Can algebraic quantum circuits compute non-algebraic functions?