Analyzing Algebraic Quantum Circuits Using Exponential Sums

Dave Bacon[*] Wim van Dam[†] Alexander Russell[‡]

November 18, 2008

Abstract

We introduce and analyze circuits that are the quantum mechanical generalization of classical algebraic circuits. Using the algebraic operations of addition and multiplication, as well as the quantum Fourier transform, such circuits are well-defined for rings $\mathbb{Z}/m\mathbb{Z}$ and finite fields $\mathbb{F}_q$. The acceptance probabilities of such algebraic quantum circuits can be expressed as exponential sums $\sum_x \exp(2\pi \mathrm{i} f(x)/m)$ where the multivariate polynomial f is determined by the circuit, while it is independent of the ring or field over which we interpret the circuit. Dawson et al. [*Quantum Information & Computation,* 5(2), pp. 102–112 (2004)] introduced this "sum over paths" description as a discrete version of the path integral approach of standard quantum mechanics. From this perspective, the polynomial f should be interpreted as the "action" of a specific (classical) computational path between the input and output of the circuit.

In this article we prove several properties of algebraic quantum circuits. Using the theory of exponential sums, we show that in the limit of large m or q, the acceptance probabilities of a circuit converge to zero or to one. Circuits that do not involve the multiplication operation are the algebraic generalization of Clifford circuits and we show how their acceptance probabilities can be calculated exactly in a classical efficient manner. For algebraic circuits that are defined over rings $\mathbb{Z}/p^r\mathbb{Z}$ we derive a "least action principle" that shows how the behaviour of such circuits is determined by those computational paths whose action polynomials are extremal.

1 Introduction

Algebraic circuits are a way of modelling computation with as elementary gates the algebraic operations of addition and multiplication, instead of the Boolean operations (AND, OR, NOT) of Boolean circuits. The wires of such algebraic circuits are allowed to carry elements of an arbitrary ring or field and a single circuit (just as polynomial equations like $x^2 = y^3 + 1$), can thus be interpreted over different domains such as $\mathbb{Z}/m\mathbb{Z}$, $\mathbb{F}_q$ or $\mathbb{C}$. One of the goals of studying algebraic circuits is to determine which properties are inherent to the circuit and independent of the specific ring or field.

Here we introduce the notion of algebraic quantum circuits that are defined over all finite rings $\mathbb{Z}/m\mathbb{Z}$ and finite fields $\mathbb{F}_q$. Just as in the Boolean setting, the classical case is contained in the quantum definition. Our definition is inspired by the analysis of Dawson et al. [5].

[*] Department of Computer Science & Engineering and Department of Physics, University of Washington

[†] Department of Computer Science and Department of Physics, University of California, Santa Barbara

[‡] Department of Computer Science & Engineering, University of Connecticut

2 Algebraic Quantum Circuits

2.1 Defining Algebraic Quantum Circuits

The set of algebraic gates that we will use for our model are: three phase changing gates $Z_{(\cdot)}$ and the Fourier transform F. For a ring $\mathbb{Z}/m\mathbb{Z}$ the Z gates are defined by

$$Z_1 : |x\rangle \mapsto \exp(2\pi i x/m)|x\rangle, \quad Z_2 : |x,y\rangle \mapsto \exp(2\pi i xy/m)|x,y\rangle, \quad Z_3 : |x,y,z\rangle \mapsto \exp(2\pi i xyz/m)|x,y,z\rangle$$

for all $x,y,z \in \mathbb{Z}/m\mathbb{Z}$, while the Fourier transform of course obeys

$$F : |x\rangle \mapsto \frac{1}{\sqrt{m}} \sum_{y\in\mathbb{Z}/m\mathbb{Z}} \exp(2\pi i xy/m)|y\rangle.$$

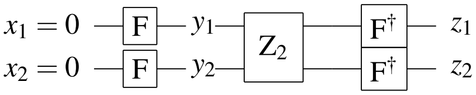
If, instead of the ring $\mathbb{Z}/m\mathbb{Z}$, the algebraic circuit is viewed as acting on a finite field $\mathbb{F}_{p^r}$ the terms $\exp(2\pi i(\cdot)/m)$ in the above definitions are replaced by the phases $\exp(2\pi i \operatorname{Tr}(\cdot)/p)$, which uses the standard trace operation $\operatorname{Tr} : \mathbb{F}_{p^r} \to \mathbb{F}_p$ with $\operatorname{Tr} : x \mapsto x + x^p + x^{p^2} + \cdots + x^{p^{r-1}}$.

With these gates it is not hard to construct circuits that implement the classical algebraic operations of addition and multiplication. Specifically, with F and Z_1 one can implement the addition-by-a-constant operation $|x\rangle \mapsto |x+1\rangle$; with F and Z_2 one can implement general additions $|x,y\rangle \mapsto |x,x+y\rangle$; and with F and Z_3 general multiplication $|x,y,z\rangle \mapsto |x,y,z+xy\rangle$ can be implemented. For this reason we call the algebraic quantum circuits that do not use the multiplicative operation Z_3 *linear quantum circuits,* which are closely related to the generalized Clifford circuits of [3].

2.2 Sum-over-Paths Approach

As the following example shows, the acceptance amplitudes of an algebraic quantum circuit can be expressed as an exponential sum over the computational paths between the input and output of the circuit. This path-summation-approach to calculating the acceptance probabilities of quantum circuits can be viewed as a discrete version of the path integral method of standard (continuous) quantum mechanics.

Example 1 (A Simple Case of the Path Summation Approach)**.** *Consider the following quantum circuit of* 2 *wires over the ring $\mathbb{Z}/m\mathbb{Z}$ with as input the zero values $x = (x_1, x_2) = (0,0)$:*



We want to know the amplitude of the output $z = (z_1, z_2) \in (\mathbb{Z}/m\mathbb{Z})^2$ in this setup. By multiplying the transition amplitudes of the individual gates and by summing over all possible intermediate $y = (y_1, y_2) \in (\mathbb{Z}/m\mathbb{Z})^2$ states, we see that these values can be expressed as the exponential sum

$$\langle (z_1,z_2)|U|(0,0)\rangle = \frac{1}{p^2} \sum_{y\in(\mathbb{Z}/m\mathbb{Z})^2} \exp(2\pi i f(y,z)/m)$$

with the polynomial $f = y_1y_2 - y_1z_1 - y_2z_2$. For this small example it is straightforward to check that the acceptance probability is given by $|\langle (z_1,z_2)|U|(0,0)\rangle|^2 = 1/m^2$ for each possible output z.

It is not hard to see that every algebraic quantum circuit has a unique multivariate polynomial f associated with it that captures the behaviour of the circuit. In general f will be a cubic polynomial but for linear circuits f is only quadratic.

Definition 1 (Action Polynomial of an Algebraic Quantum Circuit)**.** *Let C be an algebraic quantum circuit with w wires, and k Fourier transforms, assume without loss of generality that each wire caries at least one Fourier transform and define $n := k - w$. The action polynomial $f \in \mathbb{Z}[X_1, \dots, X_n]$ of this circuit is the polynomial such that the acceptance amplitude $A_C(\mathbb{Z}/m\mathbb{Z}) = \langle 0, \dots, 0|U_C|0, \dots, 0\rangle$ of the circuit over the ring $\mathbb{Z}/m\mathbb{Z}$, as well as the amplitude $A_C(\mathbb{F}_{p^r}) = \langle 0, \dots, 0|U_C|0, \dots, 0\rangle$ of the same circuit over $\mathbb{F}_{p^r}$ can be expressed by the normalized exponential sums*

$$A_C(\mathbb{Z}/m\mathbb{Z}) = \frac{1}{m^{k/2}} \sum_{x \in (\mathbb{Z}/m\mathbb{Z})^n} \exp(2\pi \mathrm{i} f(x)/m) \text{ and } A_C(\mathbb{F}_{p^r}) = \frac{1}{p^{rk/2}} \sum_{x \in \mathbb{F}_{p^r}^n} \exp(2\pi \mathrm{i}\, \mathrm{Tr}(f(x)/p)). \qquad (1)$$

where the multivariate polynomial determined by the algebraic circuit C, while it is independent of m.

With the prime power factorization $m = p_1^{r_1} \cdots p_s^{r_s}$ one has the multiplicative relation $|A_C(\mathbb{Z}/m\mathbb{Z})| = |A_C(\mathbb{Z}/p_1^{r_1}\mathbb{Z})| \cdots |A_C(\mathbb{Z}/p_s^{r_s}\mathbb{Z})|$ for the norm of the amplitude. As we are ultimately interested in the acceptance probability $|A|^2$, it will be sufficient to focus on the amplitudes of circuits defined over rings $\mathbb{Z}/p^r\mathbb{Z}$.

2.3 Basic Properties of Algebraic Quantum Circuits

2.3.1 Singularity of Action Polynomials

By the fact that the algebraic circuits are unitary it follows that the action polynomials f must be such that $|A_C| \leq 1$ for all rings $\mathbb{Z}/m\mathbb{Z}$ and finite fields $\mathbb{F}_{p^r}$. From the work of Deligne et al. on exponential sums we know that if f is non-singular, then we have the general bound $|A(\mathbb{F}_{p^r})| \leq (\deg(f) - 1)^n p^{r(n-k)/2} = (\deg(f) - 1)^n p^{-rw}$. For a fixed circuit (hence with $\deg(f)$, $n = k - w$ and $w > 0$) this Weil-Deligne bound suggests acceptance amplitudes that will always converge to 0 as p^r grows, contradicting what is possible with algebraic quantum circuits. The conclusion therefore is that, in general, the action polynomial f of a circuit can not be assumed to be non-singular. Here is an example of this crucial singularity of f.

Example 2 (A Singular Action Polynomial)**.** *Consider a single wire with an even number $k \geq 2$ of Fourier transformations such that $n = k - 1$. For all $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{F}_{p^r}$, the acceptance amplitude A_C has unit norm in this case and the action polynomial is the quadratic expression $f(x_1, \dots, x_{k-1}) = x_1x_2 + x_2x_3 + \cdots + x_{k-2}x_{k-1}$. The relevant exponential sum for this circuit is given by (for finite fields)*

$$\sum_{x \in \mathbb{F}_{p^r}^{k-1}} \exp(2\pi \mathrm{i}\, \mathrm{Tr}(f(x))/p) = \pm\sqrt{p^{rk}},$$

whereas a Weil-like bound would give an upper bound of $p^{rn/2} = \sqrt{p^{rk}}/\sqrt{p^r}$ on the norm.

The singular points of f are given by the equations $\partial f/\partial x_1 = \cdots \partial f/\partial x_{k-1} = 0$, which gives the set of solutions $x_2 = x_1 + x_3 = x_2 + x_4 = cdots = x_{k-3} + x_{k-1} = x_{k-2} = 0$. In other words these singular points form the straight line $x_2 = x_4 = \cdots = x_{k-2} = 0$ and $x_1 = -x_3 = x_5 = \cdots = \pm x_{k-1}$ (where the ± sign is determined by whether or not k is divisible by 4).

There is a good reason why the singular points of f deserve our attention. As the name suggests, in many ways the polynomial f can be viewed as expressing the *action* of the circuit taking the path x from the input $|0,\dots,0\rangle$ to the output $|0,\dots,0\rangle$. The *least action principle* from physics thus suggests that the evolution of the circuit is dominated by the paths x that correspond to the singularities of f with $\frac{\partial f}{\partial X_1} = \cdots = \frac{\partial f}{\partial X_n} = 0$. We show that this does indeed seem to be the case, although, given the discrete nature of $\mathbb{Z}/p^r\mathbb{Z}$, this does not make any obvious sense.

For linear quantum circuits the set $S = \{x : \partial f/\partial X_1(x) = \cdots = \partial f/\partial X_n(x) = 0\}$ of singular points of f is determined by n linear equations in $X_1,\dots,X_n$. Using standard techniques from algebraic geometry [4] and the theory of Gauss sums [1] we show in Section 4 that the magnitude $|A|$ is determined exactly by the dimension of S.

For general circuits defined over $\mathbb{Z}/p^r\mathbb{Z}$ with $r > 1$ we show in Section 5, using more advanced techniques such as those of [9], that the amplitude A is again almost completely determined by the singular points of the action polynomial f, while the non-singular points are less and less significant as the size of the rings grows.

First we start by proving the basic property that the acceptance probability of an algebraic quantum circuit over a finite field $\mathbb{F}_q$ converges to a "zero or one probability" in the limit of large q.

3 Algebraic Quantum Circuits in the Limit of Large Fields $\mathbb{F}_{p^r}$

Consider an algebraic quantum circuit with action polynomial over a finite field $\mathbb{F}_{p^r}$. We want to know what we can say about the acceptance amplitude A_C in the limit of large p^r. If we fix the base field $\mathbb{F}_p$ and let r grow, we know through the work of Deligne that there exists finite sets $\{\alpha_i \in \mathbb{C} : 1 \leq i \leq m_\alpha\}$ and $\{\beta_i \in \mathbb{C} : 1 \leq i \leq m_\beta\}$ of complex roots such that for all $r \in \{0,1,2,\dots\}$ we have

$$\sqrt{p^{rk}} \cdot A_C(\mathbb{F}_{p^r}) = \sum_{x\mathbb{F}_{p^r}^n} \exp(2\pi \mathrm{i}\, \mathrm{Tr}(f(x))) = \sum_{i=1}^{m_\alpha} \alpha_i^r - \sum_{i=1}^{m_\beta} \beta_i^r. \tag{2}$$

Furthermore we also know that these roots have integer *weights* $v_i, w_i \in \mathbb{N}$ such that $|\alpha_i| = p^{v_i/2}$ and $|\beta_i| = p^{w_i/2}$ for all i. If two roots α_i, β_j are equal they will always cancel each other in the above sum, making them "ineffective". For the moment we will only deal with the effective sets of roots, i.e. $\alpha_i \neq \beta_j$ for all i, j. Using the unitarity of quantum circuits we can prove the following upper bound on the weights.

Lemma 1. *Let C be an algebraic quantum circuit with k Fourier transforms. For a fixed prime p, define the complex roots α_i, β_i as expressed in Equation 2 for the acceptance amplitudes of the circuit over the finite fields $\mathbb{F}_{p^r}$. By the unitarity of C it follows that the weights $v_i := 2\log|\alpha_i|/\log p$ and $w_i := 2\log|\beta_i|/\log p$ are upper bounded by $v_i, w_i \leq k$. More specifically, there is either one root with weight k, or all roots have weight less than or equal to $k-1$.*

Proof. In the limit $r \to \infty$, the sum 2 will be dominated by the roots with the largest weights, which we will denoted by $w_{\max}$. As pointed out in the proof of Theorem 3 in [2], if there are m such weights, then for arbitrary small $\varepsilon > 0$, there will be an r such that $|\sum_i \alpha_i^r - \sum_i \beta_i^r| > (\sqrt{m} - \varepsilon)p^{rw_{\max}/2}$. By the unitarity of C it follows that at the same time this norm cannot be bigger than $p^{rk/2}$ for any r, hence we have either $m = 1$ and $w_{\max} = k$ or $w_{\max} \leq k-1$. □

The two cases described in the previous lemma completely determine the relevant behaviour of the amplitude A_C in the limit of large r. Moreover, the case can be decided using a polynomial size quantum circuit. This is our main theorem regarding algebraic quantum circuits over finite fields $\mathbb{F}_{p^r}$.

Theorem 1. *Let C be an algebraic circuit. For a fixed prime p, the* $\lim_{r\to\infty}|A_C(\mathbb{F}_{p^r})|^2$ *equals either* 0 *or* 1. *There exists a probabilistic quantum algorithm that decides which is the case in time* $\mathrm{poly}(|C|,\log p)$.

Proof. By Lemma 1 it follows that there is either one root with weight k, or all roots have weight no more than $k-1$. We have $\deg f \leq 3$ and Bombieri showed [2] that, in this setting, the total number of roots is upper bounded by $m_\alpha + m_\beta \leq 17^n$. For the two cases we thus have

$$|A_C(\mathbb{F}_{p^r})| = \begin{cases} \geq 1 - 17^n p^{-r/2} & \text{if } \lim_{r\to\infty}|A_C(\mathbb{F}_{p^r})| = 1 \\ \leq 17^n p^{-r//2} & \text{if } \lim_{r\to\infty}|A_C(\mathbb{F}_{p^r})| = 0. \end{cases} \tag{3}$$

Hence for $\log(p^r) = \Theta(n)$ we have a constant gap between the two probability amplitudes for the two cases. By implementing the algebraic quantum circuit over a field $\mathbb{F}_{p^r}$ with $\log(p^r) = O(n)$ sufficiently big, the decision between the two cases can be made with success rate at least $2/3$. □

3.1 Algebraic quantum circuits in the limit of large base fields

The previous results shows that for fixed p, the probability $|A_C^2|$ converges to either 0 or 1 as $r \longrightarrow \infty$, but what can we say about the limit $p \longrightarrow \infty$? Using a result by Katz [8] the following result is immediate.

Corollary 1. *For every algebraic quantum circuit C there exists a unique limit* $b = 0$ *or* $b = 1$ *such that for all r we have* $\lim_{p\to\infty}|A_C^2(\mathbb{F}_{p^r})| = b$.

Proof. Let f be the action polynomial of the circuit C with k Fourier transforms. In [8, Corollaire 3, p. 95] it is shown that for sufficiently large primes p, the multiset $(v_1,\ldots,w_1,\ldots)$ of the weights of the roots in Equation 2 is independent of p. If the maximum of the multiset equals k, then $\lim_{q\to\infty}|A_C^2(\mathbb{F}_q)| = 1$, while if all weights are $k-1$ or less, then this limit equals 0. (The cited result allows the multiset to contain roots that cancel each other, but as there can only be one root with weight k this does not effect the proof here.) □

Unlike the result in Theorem 1 with its bound "$\log(p^r) = \Theta(n)$", we do not know of any similar bound on p: it is likely a hard open problem to give an explicit expression for what makes p "sufficiently large".

4 Linear Algebraic Quantum Circuits

If the algebraic quantum circuit C does not use the fan 3 gate $|x,y,z\rangle \mapsto \exp(2\pi i xyz/m)|x,y,z\rangle$, the corresponding action polynomial f will be a quadratic function, making it much easier to analyze the exponential sum of A_C. This reduction in the complexity of the circuit corresponds to the fact that such generalized Clifford circuits can be simulated efficiently on a classical computer. [3]

Theorem 2. *Let C be a linear algebraic quantum circuit, i.e. a circuit that does not use the Z_3 gate. The acceptance amplitude $A_C(\mathbb{F}_{p^r})$ can be calculated exactly and classically in time* $\mathrm{poly}(\log(p^r),|C|)$

Proof. (Sketch.) The action polynomial $f \in \mathbb{Z}[X_1,\ldots,X_n]$ of this circuit will be quadratic polynomial. The relevant exponential sum is invariant under $\mathbb{F}_p$-linear transformations of $x \in \mathbb{F}_{p^r}^n$, hence after a suitable sequence of operations, we have

$$A_C(\mathbb{F}_{p^r}) = \frac{1}{p^{rk/2}} \sum_{y \in \mathbb{F}_{p^r}^n} \exp(2\pi\mathrm{i}\,\mathrm{Tr}(g(y))/p) \tag{4}$$

with $g(Y_1,\ldots,Y_n) = \sum_{i=1}^n a_iY_i^2 + b_iY_i$. As a result, the exponential sum can be calculated using the product

$$A_C(\mathbb{F}_{p^r}) = \frac{1}{p^{rk/2}} \prod_{i=1}^n \sum_{y_i \in \mathbb{F}_{p^r}} \exp(2\pi\mathrm{i}\,\mathrm{Tr}(a_iy_i^2 + b_iy_i)/p). \tag{5}$$

For each i, the summation over y_i can be calculated exactly and efficiently: If $a_i \neq 0$, the sum is a quadratic Gauss sum with norm $\sqrt{p^r}$ and a phase $\in \{1,-1,\mathrm{i},-\mathrm{i}\}$ that follows directly from (p^r,a_i,b_i); if $a_i = 0$ and $b_i \neq 0$ then the sum equals 0; and if both $a_i = 0$ and $b_i = 0$, then the sum equals p^r. The total exponential sum is simply the product of these terms. □

Note that the acceptance probability $|A_C^2(\mathbb{F}_{p^r})|$ is especially easy to compute. If g has a non-zero linear term (an i with $a_i = 0$ and $b_i \neq 0$), then $|A_C^2(\mathbb{F}_{p^r}) = 0$; otherwise we have $|A_C^2(\mathbb{F}_{p^r})| = p^{-re}$ where the exponent e equals $k+q-2n$ with q the number of quadratic terms in g. This exponent can also be expressed as a function of the dimension of the linear space of the singular points of g. Defining the set of singular points of g by $S = \{y \in \mathbb{F}_{p^r}^n : \partial g/\partial Y_1(y) = \cdots = \partial g/\partial Y_n(y) = 0\}$, we have that $S = \varnothing$ if g has a non-zero linear term, and otherwise S is a linear space of dimension $n-q$. As the dimension of S is invariant under linear transformations, the same result holds for the singular space of the original action polynomial f.

Corollary 2. *Let C be a linear algebraic quantum circuit with w wires and with quadratic action polynomial $f \in \mathbb{Z}[X_1,\ldots,X_n]$. We have for the acceptance probability $|A_C^2(\mathbb{F}_{p^r})| = p^{-re}$ with $e = w - \dim(S)$, where S is the space $\{x \in \mathbb{F}_{p^r}^n : \partial f/\partial X_1(x) = \cdots = \partial f/\partial X_n(x) = 0\}$ of singular points of f and we define* $\dim(\varnothing) := -\infty$.

The earlier Example 2 is an instance with $w = 1$ and $\dim(S) = 1$, such that $e = 0$ and hence indeed $|A_C^2(\mathbb{F}_{p^r})| = 1$. We conjecture that a similar result holds in the limit of large fields or all algebraic quantum circuits, not just the linear ones.

Conjecture 1. *Let C be an algebraic quantum circuit with w wires and action polynomial $f \in \mathbb{Z}[X_1,\ldots,X_n]$. With* $\dim(\mathrm{Sing}(f))$ *the dimension of the variety of the singular points of f, we conjecture the following convergence of the acceptance probability in the limit of large fields:*

$$\lim_{q\to\infty} |A_C^2(\mathbb{F}_q)| = \begin{cases} 1 & \textit{if}\ \dim(\mathrm{Sing}(f)) = w \\ 0 & \textit{otherwise.} \end{cases} \tag{6}$$

5 Principle of Least Action for Algebraic Quantum Circuits over $\mathbb{Z}/p^r\mathbb{Z}$

If we want to consider algebraic quantum circuits over rings, we have deal with exponential sums over $\mathbb{Z}/p^r\mathbb{Z}$, which are less well understood than those over finite fields. The following result shows however that the role of the singular points of f does again play an important role.

Lemma 2. *Let C be an algebraic quantum circuit with k Fourier transforms and action polynomial $f \in \mathbb{Z}[X_1,\ldots,X_n]$. For a fixed prime p and $r \geq 2$ and integer $1 \leq j \leq r/2$ we have the equality*

$$A_C(\mathbb{Z}/p^r\mathbb{Z}) = \frac{1}{p^{rk/2}} \sum_{x\in(\mathbb{Z}/p^r\mathbb{Z})^n} \exp(2\pi \mathrm{i} f(x)/p^r) = \frac{1}{p^{rk/2}} \sum_{x\in S_{(r,j)}(f)} \exp(2\pi \mathrm{i} f(x)/p^r) \tag{7}$$

where $S_{(r,j)}(f)$ is the set of "approximate singular points" in $(\mathbb{Z}/p^r\mathbb{Z})^n$:

$$S_{(r,j)}(f) := \{x \in (\mathbb{Z}/p^r\mathbb{Z})^n : \partial f/\partial X_1(x) = \cdots = \partial f/\partial X_n(x) = 0 \bmod p^j\}. \tag{8}$$

Proof. This proof uses a standard technique, which we learned from [11]. Define $E = p^{r-j}$ such that $E^2 = 0$ modulo p^r. It is not hard to see that for all $x,y \in (\mathbb{Z}/p^r\mathbb{Z})^n$ the following linear expansion in E holds:

$$f(x+yE) = f(x) + E(\nabla f)_x \cdot y \tag{9}$$

with $(\nabla f)_x$ is the n-dimensional function $(\partial f/\partial X_1,\ldots,\partial f/\partial X_n)$ at the point x. Hence for the exponential sum we have

$$\sum_{x\in(\mathbb{Z}/p^r\mathbb{Z})^n} \exp(2\pi \mathrm{i} f(x)/p^r) = \frac{1}{p^r} \sum_{x,y\in(\mathbb{Z}/p^r\mathbb{Z})^n} \exp(2\pi \mathrm{i} f(x+Ey)/p^r) \tag{10}$$

$$= \frac{1}{p^r} \sum_{x\in(\mathbb{Z}/p^r\mathbb{Z})^n} \exp(2\pi \mathrm{i} f(x)/p^r) \sum_{y\in(\mathbb{Z}/p^r\mathbb{Z})^n} \exp(2\pi \mathrm{i}((\nabla f)_x \cdot y)/p^j) \tag{11}$$

The summation over y will be zero, unless x is such that we have $E(\nabla f)_x = (0,\ldots,0) \bmod p^j$ in which case $\sum_y() = p^r$, which proves the lemma. □

The above result is somewhat unsatisfactory as it involves the "approximate singular points", which in turn depend on the integer j. It is tempting to expect that in the limit $r \longrightarrow \infty$ the right-hand side of above lemma converges into a summation over the singular points of f defined over the p-adic points $x \in \mathbb{Z}_p^n$. Such a result does indeed hold provided that we can apply Hensel's Lemma (see for example [7]) to the solutions of the equations $\nabla f = 0$. We conjecture that for a given circuit C this Lemma does indeed apply except for a finite number of exceptional primes p.

Acknowledgements

We thank Igor Shparlinksi, Scott Aaronson, Steven Sperber, Alan Adolphsen and Nick Katz for helpful conversations and correspondence.

References Cited

[1] Bruce C. Berndt, Ronald J. Evans, and Kenneth S. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 21, John Wiley & Sons, 1998.

[2] Enrico Bombieri, *On exponential sums in finite fields. II*, Inventiones mathematicae, Vol. 47, no. 1, pp. 29–39 (1978).

[3] Sean Clark, Richard Jozsa, and Noah Linden, *Generalised Clifford groups and simulation of associated quantum circuits*, `arXiv:quant-ph/0701103`.

[4] David Cox, John Little, and Donal O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd ed., Undergraduate texts in mathematics, Springer-Verlag, 1997.

[5] Cristopher M. Dawson, Henry L. Haselgrove, Andrew P. Hines, Duncan Mortimer, Michael A. Nielsen, and Tobias J. Osborne, *Quantum computing and polynomial equations over* $\mathbb{Z}_2$, Quantum Information and Computation, Vol. 5, no. 2, pp. 102–112 (2005).

[6] Pierre Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math., no. 43, pp. 273–307 (1974).

[7] Fernando Q. Gouvêa, *p-adic numbers: An Introduction*, Second edition, Universitext, Springer-Verlag, Berlin, 1997.

[8] Nicholas M. Katz, *Sommes exponentielles*, Astérisque, vol. 79, Société Mathématique de France, Paris, 1980. Course taught at the University of Paris, Orsay, Fall 1979, With a preface by Luc Illusie, Notes written by Gérard Laumon, With an English summary.

[9] J. H. Loxton, *Estimates for complete multiple exponential sums*, Acta Arithmetica, Vol. 92, no. 3, pp. 277–290 (2000).

[10] John H. Loxton and Robert A. Smith, *Estimates for multiple exponential sums*, J. Austral. Math. Soc. Ser. A, Vol. 33, no. 1, pp. 125–134 (1982).

[11] Romuald Dąbrowski and Benji Fisher, *A stationary phase formula for exponential sums over* $\mathbb{Z}/p^m\mathbb{Z}$ *and applications to* $\mathrm{GL}(3)$*-Kloosterman sums*, Acta Arithmetica, Vol. 80, no. 1, pp. 1–48 (1997).