Limitations on continuous variable quantum algorithms with Fourier transforms

Mark R A Adcock\textsuperscript{1,3}, Peter Høyer\textsuperscript{1,2} and Barry C Sanders\textsuperscript{1}

\textsuperscript{1} Institute for Quantum Information Science, University of Calgary, Calgary, AB T2N 1N4 Canada
\textsuperscript{2} Department of Computer Science, University of Calgary, Calgary, AB T2N 1N4 Canada
E-mail: mkadcock@qis.ucalgary.ca and hoyer@ucalgary.ca

New Journal of Physics 11 (2009) 103035 (24pp)
Received 23 December 2008
Published 21 October 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/10/103035

Abstract. We study quantum algorithms implemented within a single harmonic oscillator, or equivalently within a single mode of the electromagnetic field. Logical states correspond to functions of the canonical position, and the Fourier transform to canonical momentum serves as the analogue of the Hadamard transform for this implementation. This continuous variable version of quantum information processing has widespread appeal because of advanced quantum optics technology that can create, manipulate and read Gaussian states of light. We show that, contrary to a previous claim, this implementation of quantum information processing has limitations due to a position–momentum trade-off of the Fourier transform, analogous to the famous time-bandwidth theorem of signal processing.

\textsuperscript{3} Author to whom any correspondence should be addressed.
1. Introduction

Quantum information protocols have been demonstrated experimentally in both the discrete variable (DV) and the so-called continuous-variable (CV) settings. DV quantum information protocols employ qubits [1] and qudits [2], and CV quantum information protocols regard continuously parameterized canonical position states as the logical elements analogous to qubits for the DV case [3]. CV quantum information is experimentally appealing because sophisticated squeezed light experiments have led to claims of successful quantum information protocols such as teleportation [4], key distribution [5], and memory [6, 7], but the theoretical status of CV quantum information is challenged by unresolved issues concerning quantum error correction [8], non-distillability [9], no-go theorems for quantum computation [10, 11], and the absence of full security proofs for key distribution (although significant advances have been made, e.g. [12]). CV information processing has also been studied for classical continuous models, including the now-named Blum–Shub–Smale machine [13] and continuous Turing machines [14].

In this paper, we present a single-mode CV algorithm that implements the early DV quantum algorithm, known as the Deutsch–Jozsa (DJ) algorithm [15]–[17]. The problem solved by DJ algorithm is the following.

**Problem 1.** Given a function \( f : \{0, 1\}^n \rightarrow \{0, 1\} \) that is promised to be either constant (\( f \) takes the same value everywhere) or balanced (\( f \) takes the value 0 on exactly half the inputs), determine whether \( f \) is constant or balanced.
The best classical deterministic algorithm requires \(2^{n-1} + 1\) evaluations in the worst case. If error is tolerated, for any integer \(m \geq 2\), to achieve an error of at most \(2^{-m}\), any probabilistic algorithm requires a number of evaluations that is at least of order \(m^{18}\). If the function is accessible on a quantum computer as a quantum oracle, then the DJ algorithm is exact and requires just one evaluation to solve the problem.

We choose to study the DJ algorithm because two types of quantum algorithms dominate the field, those that implement a version of the hidden subgroup problem and those that use a version of Grover’s search algorithm \([1, 19]\). An early example of the former is the DJ algorithm \([15]\), which is amongst the oracle class of problems \([20]\) that have been important in demonstrations of quantum speed-ups.

Our focus here is on a CV generalization of the DJ algorithm to the case of a single mode of light and a Fourier transform performing the equivalent of the Hadamard transformation. Although other versions of CV DJ are possible, there are three advantages in working with this approach. One is that Braunstein and Pati \([21]\) introduced this CV DJ algorithm, and we can learn from their approach. The second advantage is that the single mode CV DJ algorithm employs standard quantum optics techniques. The third advantage is that we are going to show how the Fourier transform is itself responsible for the limitations of CV schemes, and these limitations can be fully revealed in the case of a single-mode CV DJ with Fourier transforms.

Our paper is presented as follows. In section 2, we review the DJ algorithm. Although this algorithm is well known, our review serves as a foundation for careful construction of the CV version of this algorithm. Our approach emphasizes a recasting of the traditional DJ algorithm from an \((n + 1)\)-qubit algorithm to an \(n\)-qubit algorithm, which does not employ the target qubit. The CV analogue of the \(n\)-qubit algorithm is implemented in the single-mode model.

In section 3, we present a brief review of how CV notation relates to standard quantum information notation. We also motivate the single-mode model and present the key algorithm elements. In section 4, we adapt the DJ problem to the CV case and show that the probabilistic nature of the algorithm is the result of the time-bandwidth uncertainty relation between the continuous representation and its Fourier-transform dual representation.

In section 5, we determine an upper bound on the query complexity of the CV DJ algorithm. We note that because the CV DJ algorithm is shown to be probabilistic, its performance can only logically be compared to the classical probabilistic algorithm and not to the classical deterministic algorithm. We conclude that the formalism presented herein is applicable to a wide range of oracle decision problems in a single-mode CV setting.

2. Background

We cast the DJ problem into the class of oracle decision problems in section 2.1. We then review deterministic algorithms and probabilistic algorithms in section 2.2. In section 2.3, we analyze an alternative representation of the quantum DJ algorithm that uses \(n\) qubits instead of the traditional \(n + 1\) qubits.

2.1. The DJ oracle decision problem

The DJ problem defined in problem 1 is a specific example of a decision problem in which we are given a function from some candidate set \(S = \{f_1, f_2, \ldots, f_M\}\) of functions. The candidate set \(S = S_0 \cup S_1\) is the disjoint union of two collections of functions, and our task is to
determine which of the two collections the function \( f \) is drawn from. We give the definition of a generalized decision problem in the following.

**Problem 2.** Let \( S_0 \) and \( S_1 \) be disjoint subsets of the set \( \{ f | f : \{0, 1\}^n \to \{0, 1\} \} \) of all functions from \( n \) bits to one bit. Given some oracle

\[
f : \{0, 1\}^n \to \{0, 1\}
\]

with the promise that either \( f \in S_0 \) or \( f \in S_1 \), determine which of the two is the case.

For \( N = 2^n \), we impose lexicographic order on the \( N \)-bit strings of \( \{0, 1\}^n \). We can then specify any function \( f_z \) by writing all its \( N \) function values in a list \( z \in \{0, 1\}^N \) of length \( N \). The \( i \)th bit \( z_i \) in the list is 1 if \( f \) takes the value 1 on the \( i \)th bit-string of \( \{0, 1\}^n \). There are \( 2^N \) functions from \( n \) bits to one bit, and thus our candidate set has cardinality upper bounded by \( M \leq 2^N \). In the following, we often write \( f_z \) to denote the function that corresponds to the \( N \)-bit string \( z \).

We are interested in finding an efficient strategy to identify the property of whether \( f \) belongs to set \( S_0 \) or to set \( S_1 \) without necessarily determining \( f \) itself. In the DJ case, given in problem 1, the property we are interested in is whether \( f \) is balanced or constant [15]–[17]. The cost of the algorithm is the number of queries made to the oracle.

2.2. The classical approach

On a classical Turing machine, problem 1 can be solved deterministically using \( N/2 + 1 \) queries to determine whether the given function is balanced or constant, with certainty. The problem cannot be solved with certainty with fewer than \( N/2 + 1 \) queries because \( N/2 \) queries of any balanced function could result in the same value and would thus appear to be a constant function. However, the problem can be solved with much fewer queries by allowing for an incorrect answer with some (small) probability.

A probabilistic algorithm achieves an exponentially small error of \( 2^{-m} \) with a number of queries that is only linear in \( m \) [18]. To understand how a probabilistic algorithm can help, consider that, although a single query with a random input provides no information, two queries with two random inputs can be highly informative. If the output from the second query differs from the first output, then the function is proved not to be constant and therefore must be balanced. If, on the other hand, the second output is the same as the first, then the outcome is not certain, but the more times the outputs are the same, the more confident one can be about the function being constant.

We calculate the success probability of determining whether a given function \( f_z \) is balanced or constant as

\[
\Pr = 1 - \prod_{j=1}^{m} \frac{N/2 - (j - 1)}{N - (j - 1)} \geq 1 - \left( \frac{1}{2} \right)^m . \tag{2.2}
\]

Here the equality is calculated assuming randomized input and sampling without replacement and shows dependency on \( N \), whereas the inequality is based on assuming randomized input and sampling with replacement and is independent of \( N \). We note that the failure probability declines exponentially with the number of queries.
2.3. An n-qubit quantum DJ algorithm

The quantum DJ algorithm has been shown to solve problem 1 in a single query [15]. The quantum DJ algorithm is usually studied via its corresponding quantum circuit. We present a standard circuit version [17] in figure 1. This standard circuit employs $n + 1$ qubits. The extra qubit is referred to as the target qubit and is represented by the lower line in figure 1. In order for easier adaption of this circuit to the CV setting, we choose an alternative, and equivalent, circuit formulation—one without the target state. We take this approach because the $n$-qubit model can be implemented in single a CV mode rather than the two-mode model employed in [21]. The unitary operator associated with the oracle function changes slightly in this alternative circuit.

This simpler algorithm without the target qubit is given in figure 2. The oracle construct originally proposed by DJ is expressed, for $x \in \{0, 1\}^n$ and $y \in \{0, 1\}$, as

$$U_f : \ket{x}\ket{y} \mapsto \ket{x}\ket{y \oplus f(x)}.$$ (2.3)

This construction yields a matrix representation for the $U_f$ as a permutation matrix, hence always unitary [1]. With respect to the ordered basis

$$B = \{\ket{0\cdots0}\ket{0}, \ket{0\cdots0}\ket{1}, \ldots, \ket{1\cdots1}\ket{0}, \ket{1\cdots1}\ket{1}\},$$

the unitary matrix $U_f$ can be expressed in the following insightful form

$$U_f = \begin{pmatrix} X^{f(0\cdots0)} & 0 & \cdots & 0 \\ 0 & X^{f(0\cdots1)} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X^{f(1\cdots1)} \end{pmatrix},$$ (2.4)

with $X$ the $2 \times 2$ NOT operator in this case.

The operator $U_f$ can also be expressed in the alternative ordered basis with $\ket{+} = \frac{1}{\sqrt{2}}(\ket{1} + \ket{0})$, $\ket{-} = \frac{1}{\sqrt{2}}(\ket{1} - \ket{0})$ and

$$B' = \{\ket{0\cdots0}\ket{-}, \ket{0\cdots1}\ket{-}, \ldots, \ket{1\cdots0}\ket{+}, \ket{1\cdots1}\ket{+}\},$$

as

$$U_f = \begin{pmatrix} \hat{U}_f & 0 \\ 0 & \mathbb{I} \end{pmatrix}.$$
Figure 2. Alternative quantum circuit implementing the DV DJ algorithm. Note the absence of the target qubit and the use of the operator $\hat{U}_f$ defined in equation (2.5).

with $\mathbb{1}$ the $2^n \times 2^n$ identity operator. Furthermore the operator $\hat{U}_f$ is expressed as the $2^n \times 2^n$ matrix

$$
\hat{U}_f = \begin{pmatrix}
(-1)^{f(0\cdots 0)} & 0 & \cdots & 0 \\
0 & (-1)^{f(0\cdots 1)} & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & (-1)^{f(1\cdots 1)}
\end{pmatrix},
$$

and thus provides a reduced representation for $U_f$. It is apparent that the operator $\hat{U}_f$ acts non-trivially only on a $2^n$-dimensional subspace of the $2^{n+1}$-dimensional space. This correspondence is clear in the following identity relation

$$
U_f = (\hat{U}_f \otimes |\cdot\rangle\langle\cdot|) + (\mathbb{1}^\otimes_n \otimes |+\rangle\langle+|).
$$

Thus, there is an equivalence between employing the oracle $U_f$, or its counterpart $\hat{U}_f$. We conclude that the construction employing both control and target qubits is not strictly necessary.

We now present a step-by-step analysis of the alternative circuit presented in figure 2. We shall analyze the CV circuit in the same steps for cross reference and comparison. We use the hat notation $|\hat{\Psi}_i\rangle$ in order to emphasize that this analysis is of the algorithm presented in figure 2. The $n$-qubit input state of this circuit is a string of qubits prepared in $|\hat{\Psi}_0\rangle = |0\cdots 0\rangle$. We place this state into an equal superposition of all computational basis states

$$
H^\otimes_n |\hat{\Psi}_0\rangle \mapsto |\hat{\Psi}_1\rangle = 2^{-n/2} \sum_{x \in \{0,1\}^n} |x\rangle
$$

for $H$ the single qubit Hadamard operator.

Given the definition of the reduced operator $\hat{U}_f$ defined in equation (2.5), its effect on the equal superposition of basis states expressed in the state $|\hat{\Psi}_1\rangle$ is to effectively encode the $N$-bit string $z$ unitarily into the state $|\hat{\Psi}_2\rangle$. We express this as

$$
\hat{U}_f |\hat{\Psi}_1\rangle \mapsto |\hat{\Psi}_2\rangle = 2^{-n/2} \begin{pmatrix}
(-1)^{f(0\cdots 0)} \\
(-1)^{f(0\cdots 1)} \\
\vdots \\
(-1)^{f(1\cdots 1)}
\end{pmatrix},
$$

New Journal of Physics 11 (2009) 103035 (http://www.njp.org/)
which is a convenient representation. We shall show that this representation naturally extends to the CV setting.

Measurement proceeds by first undoing the superposition created during the state preparation step. The resultant state may be expressed as follows

$$|\hat{\Psi}_3\rangle = \frac{1}{2^n} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & -1 & \cdots & -1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & -1 & \cdots & -1 \end{pmatrix} \begin{pmatrix} (-1)^{f(0\cdots 0)} \\ (-1)^{f(0\cdots 1)} \\ \vdots \\ (-1)^{f(1\cdots 1)} \end{pmatrix}. \quad (2.7)$$

Equation (2.7) allows us to see that all of the rows (and columns) of the operator $H \otimes n$ have an equal number of positive and negative ones except for the first row, which consists entirely of plus ones. It is this feature that permits the constant and balanced functions to be distinguished in a single measurement.

For the two constant cases, equation (2.7) results in the state $|\hat{\Psi}_{3C}\rangle = \pm (0 \cdots 0)'$ as only the first row does not result in amplitude cancellation of the $2^n$ constant amplitude components of the state $|\hat{\Psi}_2\rangle$. Each of the balanced functions result in the amplitudes of the state $|\hat{\Psi}_2\rangle$ having an equal number of positive and negative ones. This feature results in the first component of the state $|\hat{\Psi}_3\rangle$ having zero amplitude for all the balanced functions. We express this result as $|\hat{\Psi}_{3B}\rangle = \pm (0 \cdots x)'$, where we use the symbol $x$ to represent the nonzero value(s) that land on the other $N - 1$ components depending on which of the $\binom{N}{N/2}$ balanced functions the oracle is set to.

For the final measurement step, we employ the projection operator $[1]$ defined for $m \in \{0, 1\}^N$ as follows

$$M_m = |m\rangle \langle m|.$$

We are only concerned with the first component as discussed above, so for the constant cases we have

$$\Pr[m = (0 \cdots 0)] = \langle \hat{\Psi}_{3C} | M_{(0 \cdots 0)} | \hat{\Psi}_{3C} \rangle = 1,$$

and for all balanced cases we have

$$\Pr[m = (0 \cdots 0)] = \langle \hat{\Psi}_{3B} | M_{(0 \cdots 0)} | \hat{\Psi}_{3B} \rangle = 0$$

as required.

We have established that the $n$-qubit discrete DJ algorithm gives the same result as the standard implementation. In the next section we formulate how to adapt the $n$-qubit model to the CV setting.

3. CV representation of the DJ problem

There are many potential models representing CV DJ algorithms. Both single-mode and multiple-mode models can be analyzed; each model can be studied using input states represented by different $L^2(\mathbb{R})$ functions; also different oracle encoding schemes can be envisaged. In this section, we present the arguments for studying a particular one-mode model that offers insight into the key features of all CV models.

In section 3.1, we provide background material on how the study of CV systems relates to standard quantum information discourse. In section 3.2, we motivate the study of a single-mode
model of the CV DJ algorithm. We relate the model states to the position and momentum states of a particle or equivalently to those of an electro-magnetic oscillator. In section 3.3, we discuss the model elements used in the algorithm.

3.1. CV background

Typically in CV quantum information discourse, the position states $|x\rangle$ are introduced as a basis set of the Hilbert space with each $|x\rangle$ an eigenstate of a position operator $\hat{x}$, with $x \in \mathbb{R}$. These states are tied to standard quantum information by associating the position states with the discrete computational basis states. Unfortunately the state $|x\rangle$ does not exist in the Hilbert space; this problem is evident in the standard inner product

$$\langle x| x' \rangle = \delta(x - x'). \quad (3.1)$$

As $\delta$ is not a proper function, position states are not proper states. Fortunately the position states are correct as a representation; for example $f(x) = \langle x| f \rangle$ is the wavefunction in position space for the state $|f\rangle$ [22].

We review this concept in the following. Suppose we have a complete set of orthonormal wavefunctions $\{\varphi_n\}$; then an arbitrary wavefunction may be written

$$\Psi = \sum c_n \varphi_n. \quad (3.2)$$

Extending this expression to a continuous spectrum, we expect an expression of the form

$$\Psi(q) = \int_{-\infty}^{\infty} c(p) u(p; q) dp, \quad (3.3)$$

where the coefficients $c(p) = \langle u(p; q), \Psi(q) \rangle$ are the inner products between the function of interest and the basis functions. Substituting the function given by equation (3.3) into the inner product expression allows us to write

$$c(p) = \langle u(p; q), \int_{-\infty}^{\infty} c(p) u(p; q) dp \rangle$$

$$= \int_{-\infty}^{\infty} c(p') (u_{p}, u_{p'}) dp'$$

$$= \int_{-\infty}^{\infty} \delta(p - p') c(p') dp', \quad (3.4)$$

where we have used the linearity of the inner product.

Viewing the CV position kets $|x\rangle$ as equivalent to the basis functions, permits us to write

$$\langle x| \Psi \rangle = \int_{-\infty}^{\infty} \delta(x - x') \Psi(x') dx'. \quad (3.5)$$

This allows us to consider the wavefunctions in terms of Dirac notation, and a wavefunction in position space for a state $|\Psi\rangle$ can thus be written as

$$\Psi(x) = \langle x| \Psi \rangle. \quad (3.6)$$
We use this function representation throughout our analysis of the CV DJ algorithm. In particular we view encoded wave functions of the form \( f_i(x) = \langle x | f_i \rangle \), with the index \( i \) representing an encoded string carrying the information imparted by the oracle. Furthermore, we view measurement as being over finite intervals of the probability density function \( |f_i(x)|^2 \) rather than being precise measurements of real numbers.

For \( n \) the size of problem 1, the target-less quantum DJ algorithm requires \( n \) qubits. This requires a Hilbert space of size \( N = 2^n \) [23, 24]. The Hilbert space for CV problems seems quite generous in this respect as it is infinite-dimensional. This is part of the motivation for studying CV systems. In fact the CV Hilbert space is equivalent to the space of square-integrable complex functions over the real field \( L^2(\mathbb{R}) \) [22]. A function \( f: [a, b] \to \mathbb{C} \), for \( [a, b] \subset \mathbb{R} \), is in \( L^2(\mathbb{R}) \) if
\[
\int_a^b |f(x)|^2 \, dx < \infty.
\] (3.7)

The inner product of two functions \( f \) and \( f' \) is
\[
(f'|f) = \int_a^b f'^*(x)f(x) \, dx,
\] (3.8)
with positive definite norm and distance metric defined by
\[
\|f\| = \sqrt{(f|f)}, \quad d(f, f') = \|f - f'\|,
\] (3.9)
respectively.

The adaptation of the DV DJ algorithm to the CV regime needs to be done in the context of a computational problem. Here the relevant problem is still problem 1, and the notion of the oracle remains unchanged. Thus, in the CV case, our task is still to determine whether the function \( f_z \) belongs to the set of constant functions or to the set of balanced functions. We motivate and select the CV model in the next subsection.

### 3.2. CV model selection

Our strategy is to create a model of the CV DJ algorithm that naturally relates to the discrete case, employs reasonable resources, is generally applicable and is independent of particular basis functions. Discrete quantum information algorithms solving oracle decision problems follow a pattern: prepare the input state in one of \( n \) computational basis states \( \in \mathbb{C}^n \); apply the Hadamard transformation to place the input state in an equal superposition of basis states; apply a unitary operator representing the oracle; undo the superposition by again applying the Hadamard operator, and perform a projective measurement of a particular basis state. The probability of the desired outcome is the square of the magnitude of the amplitude of the particular basis state.

In order for our CV model to relate naturally to the discrete case, we mimic this pattern using the position and momentum states of a single particle. We choose a single-mode CV model for the following reasons. Firstly, we can apply the necessary algorithm features with minimal resources using the tools of quantum optics. Secondly, this single mode has infinite dimension, which is intrinsically more than sufficient to solve the problem. If it cannot be solved in a single-mode model, it is highly desirable to gain insight into the fundamental reasons why not. Thirdly, Braunstein and Pati’s techniques [21] employ a similar model for which, although it is a two-mode model employing a CV target state, the results of our single-mode model are directly applicable to it.
Figure 3. Quantum circuit implementing the CV DJ algorithm without the use of the target state.

Our algorithm is the CV analogue of the alternative formulation of the discrete DJ algorithm presented in figure 2. We present the CV version of this algorithm in figure 3. In our model, we also choose to encode the functions into an orthonormal basis of square-integrable complex-valued functions over the reals, namely $L^2(\mathbb{R})$. The orthonormal encoding ensures in-principle exact readout of bit strings. Since information is of finite length and can be represented by $N$-bits, it is desirable that the encoded functions form a compact basis with $p \in [-P, P]$. We have not selected the non-orthogonal Gaussian states for reason of their non-compactness.

We select $x, p \in \mathbb{R}$ and use the particle’s position wavefunction, $\phi(x)$ to describe both the input and output states. The information representing the oracle is encoded into the momentum wavefunction $\tilde{\phi}(p)$. The position and momentum wavefunctions are Fourier transform pairs, and the relationship between the particle’s position and its momentum is governed by Heisenberg’s uncertainty principle. We selected $x$ and $p$ for illustrative purposes and use it throughout for convenience. We note, however, that it is unimportant, in principle, whether information is encoded in $x$ or $p$—or indeed anything in between.

Regarding the use of the continuous Fourier transform we note that in the oracle setting, any mathematically allowed transformation is indeed permitted for the oracle, but the non-oracle operations should be described in an implementable way. Thus, we choose a transformation that is amenable to current or planned technology. It is germane to our scheme that the canonical position and momentum bases are dual to each other in the sense that the Fourier transform is the analogue of the Hadamard transformation for qubit-based quantum computation. We thus exclude the use of the discrete Fourier or Hadamard transformations in this model.

Our approach to the creation of a single-mode CV DJ algorithm differs from that of Braunstein and Pati [21] in two key areas. Firstly, our approach relies only on states that are elements in the Hilbert space congruent to $L^2(\mathbb{R})$. Secondly, our approach does not require the use of the target state. Although their model employs the target state, it only serves to ‘kick back’ the phase of the oracle function and the conclusions from both models should be identical.

3.3. Algorithm elements

The basic algorithm elements required to implement the single-mode CV model are input state preparation; Fourier transform; oracle application and measurement. Our model requires that the momentum wavefunction be compact and the encoding be unambiguous. We define the following function, along with its Fourier dual, to help us achieve this end. For $P > 0$, the
'top hat' function

\[ \tophat(p; P, P_0) = \langle p | \tophat(P, P_0) \rangle \]

\[
= \frac{1}{\sqrt{2P}} \begin{cases} 
1, & \text{if } p \in [P_0 - P, P_0 + P] \\
0, & \text{if } p \notin [P_0 - P, P_0 + P] 
\end{cases},
\]

has the compact feature. We also note that

\[
\lim_{P \to 0} |\tophat(p; P, P_0)|^2 = \delta(p - P_0),
\]

so the state |\tophat⟩ is, in some sense, a momentum eigenstate |p⟩ in the limit |P⟩ → 0.

The state given by equation (3.10) is the Fourier transform of the desired input state. Here the Fourier transform acts as the continuous version of the discrete Hadamard transform (extending the Hadamard transformation to the CV case is not unique [2, 25]). For |x⟩ the canonical position and \( p \) the canonical momentum, the Fourier transform maps a function \( \phi(x) \) to its dual \( \tilde{\phi}(p) \) according to [26]

\[
F : \phi(x) \mapsto \tilde{\phi}(p),
\]

such that

\[
\tilde{\phi}(p) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dx \ e^{-ipx} \phi(x),
\]

and

\[
\phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} dp \ e^{ipx} \tilde{\phi}(p).
\]

Note that \( \phi(x) = \langle x | \phi \rangle \); the momentum state |p⟩ is the Fourier transform of |x⟩, and \( \tilde{\phi}(p) = \langle p | \phi \rangle \).

The inverse Fourier transform of the function \( e^{ix_0} \tophat(p; P, P_0) \) gives the input state, which is described by the sinc function

\[
\phi(x) = \langle x | \phi \rangle = \frac{e^{ip_0} \sin(P(x - x_0))}{\sqrt{\pi}P(x - x_0)}
\]

centered at \( x_0 \). The limit of \(|\phi(x)|^2\) as \( P \) goes to \( \infty \) yields \( \delta(x - x_0) \). The position eigenstate |x = x_0⟩ is likewise formed in the limit |P⟩ → \( \infty \).

Our model of the oracle encodes the N-bit string \( z \) into the compact domain \([-P, P]\). Since each of the \( N \)-bits comprising the string is represented unambiguously, the contiguous momentum pulses within \([-P, P]\) have width \( \delta_p = 2P/N \), and for \( j \in \{0, N - 1\} \), the \( j \)th momentum pulse is centered at position \(-P + (j + 1/2)\delta_p\) and takes on value \((-1)^{j/2}\). The oracle can be repressed in Dirac notation as

\[
U_{CV} : |p_j⟩ \mapsto (-1)^{j/2} |p_j⟩.
\]

We illustrate this oracle behavior in figure 4 for a particular \( N = 4 \) balanced case. Note that each of the unique balanced and constant strings form a set of orthonormal functions \( \in \mathcal{L}^2(\mathbb{R}) \) when encoded in this manner.

The final quantum element of our algorithm is measurement. We measure finite intervals of the probability density function \(|\phi_i(x)|^2\), with the index \( i \) representing the encoded function.
Figure 4. Illustration of the concept for encoding an $N$-bit string in a region of momentum extending from $-P$ to $+P$ using the $N = 4, z = 0101$ example. Note that each of the bits $z_j$ are uniquely represented by individual pulses of height $\pm \frac{1}{\sqrt{2P}}$, width $\delta_p = 2P/N$ centered at $-P + (j + 1/2)\delta_p$.

This is preferable to making precise measurements of real numbers. The CV analogue of the projection operator given in equation (2.8) is defined as

$$E^b_a = \int_b^a |x\rangle\langle x| dx,$$

and thus the probability of detecting the wavefunction $\phi_i(x)$ in the interval $[a, b]$ is

$$Pr[\phi_i] = \int_b^a |\phi_i(x)|^2 dx.$$  \hspace{1cm} (3.16)

With these concepts in order, we illustrate the four stages of our algorithm in figure 5.

We begin with the position wavefunction centered at $x_0 = 0$ and illustrated in figure 5(a). In figure 5(b), we present the momentum wave function, which acts as the ‘substrate’ into which the $N$-bit strings are encoded. In figure 5(c), the compact pulse function is encoded with the particular $N$-bit string $z = \{0 \cdots 01 \cdots 1\}$. Finally, the inverse Fourier transform of this ‘square wave’ is presented in figure 5(d). Since the inverse Fourier transforms of finite pulses in the momentum domain have infinite extent in the position domain, we need to limit the extent of our measurement to $\pm \delta$.

We briefly summarize the key features of our single-mode model of the DJ algorithm. Our CV DJ algorithm requires the parameters $N$, which represents the size of the problem, the momentum ‘length’ $P$ over which the information is encoded, and the extent of the measurement window, $\delta$. Since the Fourier transform maps compact states into non-compact states, we expect to determine relationships between these parameters.

4. A single-mode CV DJ algorithm

In this section, we analyze the one-mode CV DJ algorithm presented in figure 3. This algorithm employs position states represented by sinc functions; employs the continuous Fourier transform; has oracle-encoded states represented by modulated top-hat functions, and employs the CV projection operator. We show that this model results in an uncertainty principle between
Figure 5. Overview of the four stages of our continuous DJ algorithm. (a) The probability distribution of the input state. (b) The Fourier transform of the position state acts as the encoding ‘substrate’. (c) The \( N \)-bit string \( z = \{0 \cdots 01 \cdots 1\} \) modulates this ‘substrate’. (d) The inverse Fourier transform of the encoded ‘square wave’ necessitates an optimal measurement ‘window’ parameterized by \( \pm \delta \).

the momentum ‘length’ \( P \) over which the \( N \)-bit string is encoded and the position ‘length’ \( \delta \) corresponding to the optimum measurement window. This uncertainty implies that this model results in an algorithm that is necessarily probabilistic.

In section 4.1, we define the input state and its Fourier transform. In section 4.2, we apply the oracle and perform the inverse Fourier transform of the encoded state. In section 4.3, we first determine which of the balanced function dominates the measurement window, and we use this result to establish the fundamental uncertainty relationship.

4.1. State preparation

We argued in the previous section that we need the Fourier transform of the input state to be the top hat function defined in equation (3.10). We add several conditions that do not take away from the generality of the solution. Firstly, we want the top hat to have zero phase, which gives \( x_0 = 0 \) and to be centered at \( P_0 = 0 \). Secondly, we want the pulse to have extent \( \pm P \). This gives us the simplest form of the sinc function for the initial state

\[
\phi_0(x) = \frac{\sin(Px)}{\sqrt{\pi Px}}.
\]  

The final step in state preparation is to perform the Fourier transform, which yields the top hat function with extent \( \pm P \)

\[
\tilde{\phi}(p) = \frac{1}{\sqrt{2P}} \begin{cases} 
1, & \text{if } p \in [-P, P] \\
0, & \text{if } p \notin [-P, P]. 
\end{cases}
\]  

This function forms the raw substrate, which is ‘modulated’ by the individual \( N \)-bit strings \( z \).
4.2. Oracle application

We perform encoding by partitioning the real numbers representing momentum into non-overlapping, contiguous and equal-sized bins. In this digital-to-analogue strategy, the width of each $p$-bin is $\frac{2P}{N}$, and

$$\Gamma_i^{(N)}(p) = \begin{cases} 1, & \frac{p}{P} \in \left[ -\left(1 - \frac{2N - 1 - i}{N}\right), -\left(1 - \frac{2N - i}{N}\right) \right] \\ 0, & \text{otherwise.} \end{cases}$$ \hspace{1cm} (4.3)

The oracle encodes the index $z$ into the function $f_z$ as follows:

$$f_z^{(N)}(p) = \sum_{i=0}^{N-1} (-1)^z_i \Gamma_i^{(N)}(p),$$ \hspace{1cm} (4.4)

where the factor $(-1)^z_i$ serves to modulate the phase of the top hat function according to the bit value.

**Example 1.** Consider the case $n = 2$; hence $N = 2^2 = 4$. As one case, the function corresponding to the four-bit string 0011 is

$$f_{0011}^{(N)}(p) = \Gamma_0^{(N)}(p) + \Gamma_1^{(N)}(p) - \Gamma_2^{(N)}(p) - \Gamma_3^{(N)}(p).$$ \hspace{1cm} (4.5)

The only two four-bit strings yielding constant functions would be 0000, for which the function is identically unity over the whole domain $[-P, P]$, and 1111, for which the function is identically $-1$ over $[-P, P]$. Four cases are presented in figure 6.

In the limit that $N \to \infty$ with $P$ fixed, $|\Gamma_i(p)|^2 \mapsto \delta(p - p_i)$ for $p_i$ the midpoint of the $i$th bin. The limit $N \to \infty$ thus gives a prescription for approaching a CV representation where the $z$ index seems to approach a continuum; however this limit yields a countable, rather than uncountable, set $\{z\}$, and the finite domain $[-P, P]$ has important ramifications on the nature of the functions corresponding to Fourier transforms of $\Gamma_i(p)$. We express the state after encoding as

$$\tilde{\phi}_z^{(N)}(p) = f_z^{(N)}(p)\tilde{\phi}(p),$$ \hspace{1cm} (4.6)
where we observe the ‘modulating’ effect of the encoded string $f_z$ on the momentum ‘substrate’ $\hat{\phi}(p)$.

We have the strings $z \in \{0, 1\}^N$ encoded into the momentum state (4.6). The next step is to take the inverse Fourier transform of this pulse train. For $z_j$, the $j$th bit of $z$, this is expressed as

$$\phi_z^{(N)}(x) = \frac{\sin(Px/N)}{\sqrt{P\pi}x} \sum_{j=1}^{N} (-1)^{z_j} e^{i\varphi_j(x)}, \quad (4.7)$$

where we have set $\varphi_j(x) = (\frac{2j-1-N}{N})Px$. We see that the magnitude of an individual generalized sinc function, $\phi_z^{(N)}(x)$, is determined by a vector sum of $N$ phasors, which is modulated by a particular $N$-bit string $z$.

The phasors, $e^{i\varphi_j(x)}$, are equiangular divisions of the angular interval

$$[-(N-1)Px/N, (N-1)Px/N],$$

and they exhibit the pairwise complex conjugate property $\varphi_j(x) = -\varphi_{N+1-j}(x)$. In figure 7, we present the phasors for $N = 8$ with $Px = \pi/2$ and $Px = \pi/4$ to illustrate these features.

We note that the only functions with $\phi_z^{(N)}(0) \neq 0$ are the two constant sinc functions. This is clear given that $\sum_{j=1}^{N} (-1)^{z_j} = \pm N$ for the two constant cases, and $\sum_{j=1}^{N} (-1)^{z_j} = 0$ for all balanced cases. This feature of the set of $\binom{N}{N/2} + 2$ sinc functions represented by $\phi_z^{(N)}(x)$ implies that the strategy for measurement that distinguishes between the constant and balanced cases is to measure about $x_0 = 0$.

4.3. Measurement

We measure the probability distribution in a small band around the position $x_0 = 0$. Due to the symmetry of the sinc functions about $x_0$, we employ the CV projection operator given in
equation (3.15) and set $a = \delta$ and $b = -\delta$. The probability of detecting a particular wavefunction in the interval $\pm \delta$ is thus expressed as

$$
\Pr \left[ \phi_z^{(N)}(x) \right] = \int_{-\delta}^{\delta} \left| \phi_z^{(N)}(x) \right|^2 \, dx.
$$

We now need to determine the optimal value of $\delta$ that maximizes our ability to distinguish between the constant and balanced cases.

In order to proceed, we must first determine which of the balanced functions dominates the region $\pm \delta$ and set bounds on the value of $\delta$. We hypothesize that the dominant balanced functions are the balanced functions having the lowest 'frequency' content. This occurs when the first $N/2$ bits and the last $N/2$ bits have opposite values. For this pair of balanced functions, which we call the antisymmetric balanced (ASB) functions, we have

$$
\text{ASB} \in \left\{ \begin{array}{c}
0 \cdots 01 \cdots 1 \\
N/2 \\
N/2 \\
N/2 \\
N/2
\end{array} \right\}.
$$

Note that of the $\binom{N}{N/2}$ balanced functions, there are many that are also antisymmetric about the midpoint. However, we reserve the term ASB for these two lowest-order ASB functions. Before proving the ASB function dominates all other balanced functions in the region $\pm \delta$, we illustrate the concept of frequency in the following example.

**Example 2.** Again consider the case $P = 1$, $n = 2$; hence $N = 2^2 = 4$. As one case, the function corresponding to the four-bit string 0011 is

$$
\phi_{0011}^{(4)}(x) = \frac{\sin(x/4)}{\sqrt{\pi x}} \left( e^{-i(3x/4)} + e^{-i(x/4)} - e^{i(x/4)} - e^{i(3x/4)} \right) = \frac{i (\cos x - 1)}{\sqrt{\pi x}}
$$

This function corresponds to the $N = 4$ ASB function. The probability distributions for the four distinct $N = 4$ cases are presented in figure 8. We clearly see that of the three balanced cases, the $N = 4$ ASB function has probability peaks closest to $x_0 = 0$ and thus has the lowest frequency content.

In order to proceed with the proof, we set $2m = N$ and define the quantity

$$
S = \sum_{j=1}^{2m} g(j)e^{i\varphi_j},
$$

where $g: [2m] \mapsto \pm 1$ subject to the balanced condition $\sum_j g(j) = 0$. The sum defined in equation (4.11) is a convenient re-expression of the vector sum portion of equation (4.7). Here we have incorporated $x$ into the definition of $\varphi_j = \left( \frac{(2j-1)-N}{N} \right)Px$. We seek to prove that, for all $N$, $|S|$ is maximized by the ASB balanced function given in equation (4.9).

**Lemma 1.** For the region $|Px| < \pi$, $\text{Max} \, |S|$ occurs under the specific balanced conditions

$$
g(j) = \begin{cases}
1 & \text{if} \quad 1 \leq j \leq m, \\
-1 & \text{if} \quad m + 1 \leq j \leq 2m,
\end{cases}
$$

New Journal of Physics 11 (2009) 103035 (http://www.njp.org/)
Figure 8. The probability distributions $|\phi_z^{(4)}(x)|^2$ for (a) $z = 0000$, (b) $z = 0011$, (c) $z = 0101$, and (d) $z = 0110$. We clearly see that of the three balanced cases (b) through (d), the ASB function (b) has probability peaks closest to $x_0 = 0$.

and

$$g(j) = \begin{cases} -1 & \text{if } 1 \leq j \leq m, \\ 1 & \text{if } m + 1 \leq j \leq 2m, \end{cases}$$

which we refer to as the asymmetric balanced functions (ASB) defined in equation (4.9).

Proof. Proof is done by induction on $N$. We require two base cases for $N = 2$ and $N = 4$. The base case for $N = 2$ is trivial since the only balanced cases are the two ASB cases represented by the strings $\{01, 10\}$. The base case for $N = 4$ is a little more involved. We begin by labeling the angles and phasors as shown in figure 9. There are $\binom{4}{2} = 6$ balanced cases, and we have to consider the strings $\{0011, 0101, 0110, 1100, 1010, 1001\}$. Since the latter three are complements of the first three, we have to consider only three vector sums.

With reference to figure 9, we have $S_{\{0011\}} = e^{-i\varphi_1} + e^{-i\varphi_2} - e^{i\varphi_1} - e^{i\varphi_2}$. We simplify and express the result along with the three other cases as

- $S_1 = S_{\{0011\}} = \pm 2i (\sin \varphi_1 + \sin \varphi_2)$,
- $S_2 = S_{\{0110\}} = \pm 2 (\cos \varphi_1 - \cos \varphi_2)$,
- $S_3 = S_{\{0101\}} = \pm 2i (\sin \varphi_1 - \sin \varphi_2)$,

where $\varphi_1 = -\frac{3\pi}{4}$ and $\varphi_2 = -\frac{\pi}{4}$. Clearly $|S_1| > |S_3|$. We use the trigonometric identities,

$$|S_1| = 2 \sin \left( \frac{\varphi_1 + \varphi_2}{2} \right) \cos \left( \frac{\varphi_1 - \varphi_2}{2} \right),$$

$$|S_2| = 2 \sin \left( \frac{\varphi_1 + \varphi_2}{2} \right) \sin \left( \frac{\varphi_1 - \varphi_2}{2} \right).$$
Figure 9. Definition of the phasor angles for the \( N = 4 \) base case for \( P = 1 \).

Note that the effect of varying \( x \) over \([-\pi/2, \pi/2]\) simply focuses or expands the double angles \( 2\varphi_1 \) and \( 2\varphi_2 \) proportionally.

to establish the relationship between \( |S_1| \) and \( |S_2| \). For \( 0 \leq P_x < \pi \), \( \cos(\frac{P_x}{4}) > \sin(\frac{P_x}{4}) \), and therefore \( |S_1| > |S_2| \). This proves that the theorem is true for the \( N = 4 \) base case.

For the inductive step for \( N > 4 \), we assume that \( |S| \) is maximized for both the \( N - 2 \) and the \( N - 4 \) balanced strings. For an arbitrary balanced string of size \( N \), we consider two cases. Case (i) assumes every pair is antisymmetric. By this we mean that \( g(j) = -g(2m + 1 - j) \). If we remove any antisymmetric pair, we recover the \( N - 2 \) base case only if the string itself is the ASB string. This part of the inductive step is expressed as \( |S| \leq |S([l, 2m + 1 - l])| + |S_2(w)| \), where \( |S_2(w)| \) is maximized per the \( N = 4 \) base case.

Case (ii) assumes that Case (i) is false and therefore the arbitrary string must have two symmetric pairs for which \( g(l) = g(2m + 1 - l) = +1 \) and \( g(k) = g(2m + 1 - k) = -1 \). If we remove any two symmetric pairs, we recover the \( N - 4 \) base case only if the string itself is the ASB string. This part of the inductive step is expressed as \( |S| \leq |S([l, 2m + 1 - l, k, 2m + 1 - k])| + |S_4(w)| \) where \( |S_4(w)| \) is maximized per the \( N = 4 \) base case. Only when \( |S([l, 2m + 1 - l, k, 2m + 1 - k])| \) itself is maximized is equality achieved and the total sum maximized. This occurs for the ASB strings.

We have established that the ASB functions dominate all other balanced function in the region \( |P_x| < \pi \). We use this result to determine the optimum value of \( \delta \). We first define the constant and ASB probability distributions. The two constant functions are defined by the strings

\[
C \in \left\{ \underbrace{0 \cdots 0}_{N}, \underbrace{1 \cdots 1}_{N} \right\}.
\]
Taking the square of the magnitude of equation (4.7) given the constant functions defined above gives the constant probability distribution
\[ P_C(x) = |\phi_C^{(N)}(x)|^2 = \frac{\sin^2(Px)}{P\pi x^2}. \]  (4.15)

Similarly for the ASB functions defined by equation (4.9), the ASB probability distribution is expressed as
\[ P_{\text{ASB}}(x) = |\phi_{\text{ASB}}^{(N)}(x)|^2 = \frac{(\cos(Px) - 1)^2}{P\pi x^2}. \]  (4.16)

Next we note that the ability to effectively distinguish between two random events is proportional to the separation of the individual probabilities of occurrence. Thus we need to select \( \delta \) such that we get as much separation between the constant distribution and the ASB distribution as possible. When we make a measurement we are distinguishing between two events, the probabilities for which we define as follows
\[ \Pr_{\text{Const}}(\delta) = \Pr\left[ |\phi_C^{(N)}| = P_C(x) \right] = E_{-\delta}^\delta P_C(x), \]  (4.17)
and
\[ \Pr_{\text{ASB}}(\delta) = \Pr\left[ |\phi_{\text{ASB}}^{(N)}| = P_{\text{ASB}}(x) \right] = E_{-\delta}^\delta P_{\text{ASB}}(x). \]  (4.18)

We determine the optimum value of \( \delta \) by maximizing the expression \(|\Pr_{\text{Const}}(\delta) - \Pr_{\text{ASB}}(\delta)|\). It suffices to find the value of \( \delta \) for which \( \frac{d}{d\delta} |\Pr_{\text{Const}}(\delta) - \Pr_{\text{ASB}}(\delta)| = 0 \), which may be expressed as
\[ \frac{d}{d\delta} |\Pr_{\text{Const}}(\delta) - \Pr_{\text{ASB}}(\delta)| \bigg|_{\delta = 0} = \frac{\sin^2(P\delta)}{P\pi \delta^2} - \frac{(\cos(P\delta) - 1)^2}{P\pi \delta^2} = 0. \]  (4.19)

This occurs where \( \cos(P\delta) = \cos^2(P\delta) \) for \( \delta \neq 0 \), which gives a global maximum at \( \delta = \frac{\pi}{2P} \). It is interesting to think of this result as an uncertainty relationship
\[ P\delta = \frac{\pi}{2}. \]  (4.20)

For \( P = 1 \) and \( N = 4 \), the optimal measurement window of \( \delta = \frac{\pi}{2} \) is plotted along with the four distinct probability distributions in figure 10.

The probability distributions \( P_C(x) \) and \( P_{\text{ASB}}(x) \) defined by equations (4.15) and (4.16) respectively, are in \( H_2 \), the Hilbert space of \( L^2((\mathbb{R}) \) functions over the interval \((-\infty, \infty)\). This implies that since we are measuring over a finite interval, the CV DJ algorithm is necessarily probabilistic. Furthermore, we noted that \( P \) and \( \delta \) are related by the uncertainty relation given in equation (4.20). This leads to the conclusion that even in the limit of the improper delta function \( \delta(x - x_0) \), the CV DJ algorithm remains probabilistic.

This conclusion contradicts Braunstein and Pati’s speed-up claim [21]. Their algorithmic improvement relies on unboundedness of the canonical momentum to provide perfect resolution for canonical position. As both domains must be bounded, our quantum-information Fourier limit applies, and their claimed speed-up is forbidden by the probabilistic nature of the protocol due to the position–momentum (equivalently time-bandwidth) tradeoff.

New Journal of Physics 11 (2009) 103035 (http://www.njp.org/)
Figure 10. For $P = 1$, the optimal value of $\delta = \frac{\pi}{2}$. This graph shows that only the constant and the ASB functions significantly contribute to probability between $\pm \delta$.

5. Bounding the query complexity of the CV DJ algorithm

In this section, we first determine the single query success probability. We then provide an upper bound on the success probability after multiple repetitions. We make no attempt to make a tight bound because a meaningful tight bound would require investigating different $L^2(\mathbb{R})$ functions as input states. The sinc-pulse Fourier pair is sufficient to establish that the single-mode CV model is necessarily probabilistic.

5.1. Single measurement success probability

We now determine numerical values of the probabilities determined in equations (4.17) and (4.18). We can readily calculate the probability of detecting if the function is constant

$$\Pr_{\text{const}} = \int_{-\delta}^{\delta} \frac{\sin^2(Px)}{P \pi x^2} \, dx$$

$$= \frac{\cos(2\delta P) + 2\delta P \text{Si}(2\delta P) - 1}{\delta P \pi}, \tag{5.1}$$

where the sine integral is given by

$$\text{Si}(z) = \int_{0}^{z} \frac{\sin t}{t} \, dt. \tag{5.2}$$

Note this probability depends only on the product $P \delta$. If the function is the lowest-order ASB, we have

$$\Pr_{\text{ASB}} = \int_{-\delta}^{\delta} \frac{(\cos(Px) - 1)^2}{P \pi x^2} \, dx$$

$$= \frac{-8 \sin^4(\delta P/2) + 4\delta P \text{Si}(\delta P) - 2\delta P \text{Si}(2\delta P)}{\delta P \pi}. \tag{5.3}$$
For $P\delta = \pi/2$, the numerical values of these two probabilities are

$$\Pr_{\text{Const}} = \frac{2(\pi \, \text{Si}(\pi) - 2)}{\pi^2} \approx 0.77,$$

and

$$\Pr_{\text{ASB}} = \frac{4\pi \, \text{Si}(\pi/2) - 2\pi \, \text{Si}(\pi) - 4}{\pi^2} \approx 0.16.$$

Given this probabilistic nature of the CV DJ algorithm, we need to develop a strategy to bound the error probability. We employ the technique sometimes called probability amplification [27, 28].

### 5.2. Success probability after multiple repetitions

Our strategy is to make $m$ repetitions of the CV DJ algorithm where we assume that the oracle is set to the same function for each of the repetitions. Each repetition ends with a measurement. From this sequence of measurements we want to determine whether the unknown function is balanced or constant with high probability.

**Lemma 2.** An error of $O(e^{-m})$ can be achieved by making $O(m)$ repetitions of the CV DJ algorithm.

**Proof.** We adopt the convention that when we make a query to the CV DJ algorithm we either detect something (algorithm returns a 1), or we do not (algorithm returns a 0). We can thus treat multiple queries as a sequence of Bernoulli trials [29]. We assume that we have set our measurement limits to the optimal $\pm \delta$. The two events we are trying to uncover are the constant cases where, for ease of calculation we set the probability of detecting something is $Pr_C \geq 3/4$, and the balanced cases where the probability detecting something is $Pr_B \leq 1/4$. Note that we have set the probabilities to these rational numbers for illustrative purposes and to simplify the calculation. We can make this arbitrary setting, and we obtain the same result as long as the probabilities are bound from $1/2$ by a constant.

If each measurement is based on an independent preparation of the state $\phi_0(x)$, then each of the queries are independent. After a series of $m$ queries, we can use the Chernoff bounds of the binomial distribution to amplify the success probability [28, 29]. The simplest (but somewhat weak) Chernoff bound on the lower tail is given by [28] as

$$\Pr[X < (1 - \epsilon)\mu] < e^{-\mu \epsilon^2/2},$$

and on the upper tail as

$$\Pr[X > (1 + \epsilon)\mu] < e^{-\mu \epsilon^7/4},$$

where $\mu$ is the expected mean of the resulting binomial distributions after $m$ queries, and $\epsilon$ is the relative distance from the respective means.

First, we bound the lower tail corresponding to the distribution of the constant case for which we have $\mu = m \, \frac{P_C}{2}$. Here we set $\epsilon = \frac{1}{3}$, which expresses the probability for the value being less than halfway between the two means as $Pr[X < (m/2)] < e^{-m/24}$. Similarly, we bound the upper tail for the balanced case for which we have $\mu = m \, \frac{P_B}{2}$. Here we set $\epsilon = 1$, which expresses the probability for the value being greater than half way between the two means as...
Pr[\(X > (m/2)\)] < \(e^{-m/16}\). Clearly the success is worse for the lower tail allowing us to bound the success probability of the CV DJ algorithm after \(m\) queries as

\[
\Pr[\text{Success}] \geq 1 - e^{-m/24}.
\]

This gives an error probability that is \(O(e^{-m})\) as required. \(\square\)

We note that this is of the same order as the exponentially good success probability we have for the classical probabilistic approach given by equation (2.2). Also note that this query complexity is independent of the value of \(N\). We have made no attempt to obtain a tighter bound preferring to show only that we can achieve the same exponentially small error probability using the CV DJ algorithm as the classical probabilistic approach to solving the DJ problem using a number of queries that is of the same order as the classical probabilistic approach. The CV DJ algorithm is in this sense no worse than the classical probabilistic approach.

6. Conclusions

In this paper we have presented a single-mode CV model of the DJ algorithm. Our model employs logical states that are in the Hilbert space congruent to the space of \(L^2(\mathbb{R})\) functions. Our analysis shows that this algorithm is necessarily probabilistic, and cannot provide the exponential speed-up of its discrete quantum counterpart. This is contrary to results published in the literature.

The probabilistic nature of this single-mode CV quantum algorithm derives from the nature of the continuous Fourier transform. The lack of speed-up results from an uncertainty principle between the ability to encode perfectly in a continuous representation and the subsequent inability to measure perfectly in the Fourier-dual representation. This uncertainty relationship is manifest in equation (4.20), which relates \(P\), the encoding extent, to \(\delta\), the measurement extent.

Our result is directly analogueous to the time-bandwidth uncertainty theorem of signal processing. Furthermore our result does not have to be limited to the DJ algorithm. We argue that our model is generally applicable and that the algorithm relies only on the orthonormality of basis functions, compactness of encoding requirements, and the time-bandwidth uncertainty relation.

In our analysis, we intentionally did not employ the Gaussian states so readily created in quantum optics experiments. We chose to select the sinc–pulse Fourier transform pair for our model because of our interest in unambiguous encoding of the unknown function. Since the Fourier transform of a Gaussian state is itself a Gaussian state and both span infinite domains, the encoding strategy may be different, but we can see that the result is also probabilistic. This is again due to the necessity of finite measurement extent.

A natural extension of this work would be prove a lower bound perhaps exploring the techniques along the lines of [30] from the perspective of different Fourier transform pairs. The analysis provided in here provides intuition on how to proceed—particularly the technique of finding which of the balanced functions is the limiting function. In our model the limiting balanced function is the ASB function given by expression (4.9).

Acknowledgments

We thank Loïck Magnin for his helpful comments and for sharing his insight into CV quantum computing. We appreciate financial support from the Alberta Ingenuity Fund (AIF),
Alberta’s Informatics Circle of Research Excellence (iCORE), Canada’s Natural Sciences and Engineering Research Council (NSERC), the Canadian Network Centres of Excellence for Mathematics of Information Technology and Complex Systems (MITACS), and General Dynamics Canada. PH is a Scholar and BCS is an Associate of the Canadian Institute for Advanced Research (CIFAR).

References

[1] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge: Cambridge University Press)
[2] Gottesman D, Kitaev A and Preskill J 2001 Encoding a qubit in an oscillator Phys. Rev. A 64 012310
[3] Braunstein S L and Pati A K (ed) 2003 Quantum Information with Continuous Variables (Dordrecht: Kluwer) (arXiv:quant-ph/0207108)
[4] Furusawa A, Sørensen J L, Braunstein S L, Fuchs C A, Kimble H J and Polzik E S 1998 Unconditional quantum teleportation Science 282 706–9
[5] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states Phys. Rev. Lett. 88 057902
[6] Appel J, Figueroa E, Korystov D, Lobino M and Lvovsky A I 2008 Quantum memory for squeezed light Phys. Rev. Lett. 100 093602
[7] Akamatsu D, Yokoi Y, Arikawa M, Nagatsuka S, Tanimura T, Furusawa A and Kozuma M 2007 Ultraslow propagation of squeezed vacuum pulses with electromagnetically induced transparency Phys. Rev. Lett. 99 153602
[8] Braunstein S L 1998 Error correction for continuous quantum variables Phys. Rev. Lett. 80 137903
[9] Bartlett S D and Sanders B C 2002 Efficient classical simulation of optical quantum information circuits Phys. Rev. Lett. 89 207903
[10] Bartlett S D, Sanders B C, Braunstein S L and Nemoto K 2002 Efficient classical simulation of continuous variable quantum information processes Phys. Rev. Lett. 88 097904
[11] Renner R and Cirac J I 2009 A de Finetti representation theorem for infinite dimensional quantum systems and applications to quantum cryptography Phys. Rev. Lett. 102 110504
[12] Blum L, Shub M and Smale S 1989 On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines Bull. Am. Math. Soc. 21 1
[13] Continuous Turing machines Manuscript, not dated (available at http://www.mathpages.com/home/kmath135.htm Accessed on 3 December 2008)
[14] Deutsch D and Jozsa R 1992 Rapid solution of problems by quantum computation Proc. R. Soc. A 439 553
[15] Deutsch D 1985 Quantum theory, the Church–Turing principle and the universal quantum computer Proc. R. Soc. A 400 97
[16] Cleve R, Ekert A, Macchiavello C and Mosca M 1998 Quantum algorithms revisited Proc. R. Soc. A 454 339–54
[17] Bacon D 2005 Lecture 4: Quantum Algorithms from Summer School in Siena, Italy. 30 August–2 September, 2005. Manuscript (available at http://www.cs.washington.edu/homes/dabacon/teaching/siena. Reference downloaded 20 October 2008)
[18] Grover L K 1996 A fast quantum mechanical algorithm for database search Proc. 28th Annu. ACM Symp. on Theory of Computing (STOC ’96) pp 212–9
[19] Ambainis A, Iwama K, Kowachi A, Raymond R and Yamashita S 2004 Robust quantum algorithms for oracle identification arXiv:quant-ph/0411204
[20] Braunstein S L and Pati A K Deutsch–Jozsa algorithm for continuous variables Quantum Information with Continuous Variables (Dordrecht: Kluwer) (arXiv:quant-ph/0207108)
[22] Tan C I 2008 Notes on Hilbert Space Manuscript, not dated (available at http://jcbmac.chem.brown.edu/baird/QuantumPDF. Reference downloaded 20 October 2008)

[23] Blume-Kohout R, Caves C M and Deutsch I H 2002 Climbing mount scalable: physical resource requirements for a scalable quantum computer Found. Phys. 32 1641

[24] Caves C M 2008 Physical resources, entanglement and the power of quantum computation. Lecture given in SQuInT Summer Retreat University of Southern California, July 7 2005. Accessed on 3 December 2008

[25] Bartlett S D, de Guise H and Sanders B C 2002 Quantum encodings in spin systems and harmonic oscillators Phys. Rev. A 65 052316

[26] Bracewell R N 1986 The Fourier Transform and Its Applications 2nd edn (New York: McGraw-Hill)

[27] Adcock M 2004 The classical and quantum complexity of the Goldreich–Levin problem with applications to bit commitment MSc Thesis Department of Computer Science, University of Calgary

[28] Canny J F 2001 Chernoff bounds Manuscript (available at http://www.cs.berkeley.edu/jfc/cs174/lecs/lec10/lec10.pdf. Accessed on 20 October 2008)

[29] Cormen T H, Leiserson C E and Rivest R L 1990 Introduction to Algorithms (Cambridge, MA: MIT Press)

[30] Høyer P and Špalek R 2005 Lower Bounds on quantum query complexity Bull. Eur. Assoc. Theoret. Comput. Sci. 87 87–103