Case study in which the Deutsch-Jozsa algorithm responds with pure states

Eraldo P. Marinho
Univ Estadual Paulista (UNESP/IGCE), Department of Computing, Rio Claro, SP, Brazil
E-mail: pereira.marinho@unesp.br

Abstract. A theoretical essay is presented on a particular type of balanced functions that allow the Deutsch-Jozsa algorithm to produce pure state instead of mixed states. Such results occur if and only if the balanced functions are linear combinations (modulo 2) of a set of balanced clock functions, that is, clock functions with periods that are power of 2.

Key words: quantum circuits, quantum algorithms, Boolean functions

1. Introduction

The Deutsch–Jozsa algorithm was introduced by David Deutsch and Richard Jozsa in 1992 [1], quoted as DJ92 hereafter. The publication was an improvement on an earlier work of David Deutsch [2], which was in turn the first reformulation of the Church–Turing thesis [3] in terms of the principles of quantum mechanics. The DJ92 quantum computing model predicts a never-before-conceived speedup as a consequence of the superposition principle.

To illustrate the exponential power of quantum parallelism, the authors proposed a computationally simple (not to say naive) problem: it is assumed that a Boolean function was intentionally programmed to behave as a constant or balanced function. The simplifying hypothesis omits the possibility that the function is neither constant nor balanced. In these terms, how to computationally decide if this (incognito) function is constant or balanced?

It is easy to see that the brute force version of the classical search expends $O(2^n)$ comparisons. To do so, let $x$ be a for-loop controller variable that runs from 0 to $2^n-1$ and compare $f(x)$ with $f(x+1)$. If $f(0) = f(1)$ and goes on until $f(2^n-1) = f(2^n-1)$, then the search decides that $f$ is constant under the belief in the promise that there is no third behavior for this function. Otherwise, if $f(x) \neq f(x+1)$ for some $x \in [0, 2^n-1]$, the comparison-loop breaks and the function is judged balanced regardless further details in its profile. Thus, there were $2^n-1$ comparisons in the worst case of the naive search.

The authors proposed an algorithm that uses the quantum parallelism to simultaneously explore all possibilities for $f(x)$ and using destructive interference to obtain a quantum state from which one can infer whether $f$ is constant or not. The quantum circuit conceived by the authors use a quantum oracle, $U_f$, according to the following diagram:

\[
\begin{align*}
|0^n\rangle & \xrightarrow{H^\otimes n} |H^\otimes n\rangle \\
|1\rangle & \xrightarrow{H} |H_1\rangle \\
U_f^\otimes n & \xrightarrow{H^\otimes n} |\psi_{out}\rangle \\
\end{align*}
\]
The oracle $U_f$ is a quantum gate that operates on a quantum register comprising $n+1$ qubits whose details are depicted in the following quantum diagram:

$$
\begin{array}{c}
| x \rangle \\
| y \rangle
\end{array}
\xrightarrow{egin{array}{c}
U_f \\
| y \oplus f(x) \rangle
\end{array}}
\begin{array}{c}
| x \rangle \\
| y \rangle
\end{array}
$$

where the upper $n$-qubit bus is named query-register and the bottom qubit wire is called the answer register.

With some algebra [4] one can show that the output state of the quantum circuit (1) can be written as

$$| \psi_{out} \rangle = \sum_{z \in \{0,1\}^n} \psi_z | z \rangle$$

where $\psi_z$ is the probability amplitude of having the $n$-bit string $z$:

$$\psi_z = \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)+x \cdot z}$$

The term $x \cdot z \in \{0,1\}$ in the exponent in the right hand side of equation (4) is defined as the Boolean inner product, namely

$$x \cdot z \equiv \bigoplus_{j=0}^{n-1} x_j z_j = \sum_{j=0}^{n-1} x_j z_j \mod 2$$

where $x = x_{n-1} \ldots x_0$ and $z = z_{n-1} \ldots z_0$, respectively.

Examining Equation (4) one can easily find that in the constant case the probability amplitude becomes

$$\psi_z = \frac{(-1)^c}{2^n} \sum_{x \in \{0,1\}^n} (-1)^x z = \begin{cases} (-1)^c, & \text{iff } z = 0 \\ 0, & \text{iff } z \neq 0 \end{cases}$$

where $c \in \{0,1\}$ is an arbitrary Boolean constant.

As previously remarked, the simplifying hypothesis of the problem proposed by DJ92 rules out the need to know in detail the behavior of the output states for the balanced case, namely, that the quantum number $z$ is nonzero. Still, one may have the curiosity to know these details, especially when the output states for the balanced case correspond to pure states, in addition to $z = 0$, namely $z = 1, 2, \ldots$, as pointed out by [5] and revised in the following section.

2. Pure state solution

We start the study with the most simplified case of balanced function, which certainly output a pure state in the output of the DJ92 algorithm. This is the case of the clock functions whose period is an integer power of 2 (hereafter balanced clock functions) as will be seen below.

This is the case where $f$ oscillates between 0 and 1, along alternating adjacent intervals of length $2^m$ ($0 \leq m \leq n-1$). In this case, $f$ is the discrete form of the clock signal of period $T = 2^{m+1}$. Such periodic function can be written as

$$f_m(x) = c \oplus x_m$$

where $c$ is an arbitrary Boolean constant and $x_m$ is the $m$-th bit right to left counted of the input string $x = x_{n-1} \ldots x_m \ldots x_0$. Such a function is obviously balanced in the domain, since half the points in $\{0,1\}^n$ have the $m$-th bit in the state 0, and the other half in the state 1, so that the constant $c$ is an xor mask as in the right hand side of equation (7).
It immediately follows that the longest possible period in the domain \( \{0, 1\}^n \) is \( T_{\text{max}} = 2^n \), which is the case for \( m = n - 1 \). On the other hand, the smallest permissible period is \( T_{\text{min}} = 2 \), which corresponds to \( m = 0 \). Of course, the exception condition in which \( m = -1 \) would be incurred in the case where \( f \) is constant, i.e. \( T = 2^0 \).

It is easy to verify that Equation (5) is equivalent to

\[
    x_m = 0^{n-m-1}10^m \cdot x = \bigoplus_{j=m+1}^{n-1} 0 \times x_j \oplus 1 \times x_m \oplus \bigoplus_{j=0}^{m-1} 0 \times x_j
\]  

where the \( n \)-bit string \( 0^{n-m-1}10^m \) is a predefined xor mask with all bits zero except the one at position \( m \).

Substituting \( f \) in the exponent on the right hand side of Equation (4) with the balanced clock function \( f_m \), with period \( 2^m + 1 \) as defined in (7), we find

\[
    \psi_m(z) = \begin{cases} 
    (-1)^c & \text{iff } z = 2^m \\
    0 & \text{iff } z \neq 2^m
    \end{cases}
\]  

which is the probability amplitude for the pure \( n \)-qubit state \( |z\rangle \) with the quantum number \( z = 2^m \). Obviously, the constant case would correspond to the particular output \( z = 0^n = 0 \).

The result expressed by Equation (9) will be useful if combined with the following theorem, whose proof is immediate:

**Theorem 2.1.** The modulo 2 sum, \( f_j \oplus f_k \), of two balanced clock functions \( f_j \) and \( f_k \) is either a balanced or a constant function on \( \{0, 1\}^n \).

We can generalize the previous result to the case in which a Boolean function is written as the following linear combination (modulo 2) of balanced clock:

\[
    f(x) = \bigoplus_{j=0}^{n-1} k_j f_j(x),
\]  

where the coefficients, \( k_j \in \{0, 1\}, j = 0, \ldots, n - 1 \), are arbitrary.

It is easy to check that \( f \) in the previous equation is balanced in \( \{0, 1\}^n \). Moreover, each component \( f_j \) in the right hand side of Equation (10) can be written as \( f_j = c_j \oplus x_j \), with \( 0 \leq j \leq n - 1 \). We then conclude that

\[
    f(x) = c \oplus \bigoplus_{j=0}^{n-1} k_j x_j,
\]  

where the arbitrary constant \( c \) is defined as

\[
    c = \bigoplus_{j=0}^{n-1} k_j c_j
\]  

It comes out from Theorem 2.1 and from Equation (10) that the function

\[
    f(x) = c \oplus k \cdot x; \quad \forall x \in \{0, 1\}^n,
\]  

is balanced on the domain \( \{0, 1\}^n \).

As a corollary, we have that the solution of the Deutsch-Jozsa algorithm is a pure state if and only if the function exercised by the quantum oracle is written according to Equation (13).
Figure 1. Left: Pure-state balanced function for 6 qubits. Right: The corresponding probability distribution.

3. Test

In order to visualize the results of the previous section, a program was implemented to load a Boolean array, $f[2^n]$, for all points in the domain $\{0, 1\}^n$, according to Equation (13). For each term in $f[j]$, $j = 0, \ldots, 2^n - 1$ is computed the probability amplitudes $\psi[j]$ through Equation (4). Thus, the probabilities $P[j]$ are computed as $P[j] = |\psi[j]|^2$.

Figure 1 illustrates the simulated behavior of the Deutsch–Jozsa algorithm in the case of $n = 6$ qubits, using the xor-mask $k = 011110 \equiv 30$. Still in the referred figure, the left plot illustrates the values for $f$, and in the right plot are represented the probabilities $P$, which corresponds to a single line, $P = 1$, at position $x = k = 30$. According to the simulation, the output is the pure 6-qubit $|\psi_{out}\rangle = |011110\rangle \equiv |30\rangle$.

4. Conclusion

The present work was devoted to the case study in which the solutions of the Deutsch-Jozsa algorithm are manifested in the form of pure state, which are specific cases of balanced functions.

In general, if we consider the trivial solution $z = 0$ as the special case in which the function is constant, jointly with the balanced cases studied in the previous section, we have that pure-state solutions manifest themselves with functions in the form $f(x) = k \cdot x \oplus c$, with $k$ being the bit-string representation of a non-negative integer in the range $k \equiv 0, 1, \ldots n - 1$. Such a representation is analogous to the spectral decomposition of the queried function as a modulo 2 linear combination of balanced clock functions.

Acknowledgements

The author thanks Geysa de Oliveira Marinho for the critical reading of the manuscript and helpful suggestions.

References

[1] Deutsch D and Jozsa R 1992 Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 439 553–558 ISSN 0962-8444
[2] Deutsch D 1985 Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 400 97–117 ISSN 0080-4630
[3] Turing A M 1937 Proceedings of the London Mathematical Society s2-42 230–265
[4] Nielsen M A and Chuang I L 2000 Quantum Computation and Quantum Information (Cambridge University Press)
[5] Marinho E P 2018 arXiv e-prints arXiv:1812.07844 (Preprint quant-ph/1812.07844)