Determining Parity

We consider ways of determinig the parity by quantum means. Parity serves as a *Rosetta stone* for quantum computational (in-)capacities.

PACS numbers: 03.65.Aa, 03.67.Ac
Keywords: quantum algorithms, parity

I. PARITY OF STATES

A. Parity of two-partite binary states

Consider the four two-partite binary basis states $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$. Suppose we are interested in the even parity of these states. Then we could construct a *even parity operator* P *via* a spectral decomposition; that is,

$$\begin{aligned}\mathsf{P} &= 1\cdot\mathsf{P}_- + 0\cdot\mathsf{P}_+, \text{ with}\\ \mathsf{P}_- &= |01\rangle\langle 01| + |10\rangle\langle 10|,\\ \mathsf{P}_+ &= |00\rangle\langle 00| + |11\rangle\langle 11|,\end{aligned} \tag{1}$$

which yields even parity "0" on $|00\rangle$ as well as $|11\rangle$, and even parity "1" on $|01\rangle$ as well as $|10\rangle$, respectively. Note that P_- as well as P_+ are projection operators, since they are idempotent; that is, $\mathsf{P}_-^2 = \mathsf{P}_-$ and $\mathsf{P}_+^2 = \mathsf{P}_+$.

Thereby, the basis of the two-partite binary states has been effectively equipartitioned into two groups of even parity "0" and "1;" that is,

$$\big\{\{|00\rangle, |11\rangle\}, \{|01\rangle, |10\rangle\}\big\}. \tag{2}$$

The states associated with the propositions corresponding to the projection operators P_- for even parity one and P_+ for even parity zero of the two bits are entangled; that is, this information is only expressed in terms of a *relational property* – in this case parity – of the two quanta between each other [1, 2].

B. Parity of multi-partite binary states

This equipartinioning stategy [3, 4] to determine parity with a single query can be generalized to determine the parity of multi-partite binary states. Take, for example, the even parity of three-partite binary states definable by

$$\begin{aligned}\mathsf{P} &= 1\cdot\mathsf{P}_- + 0\cdot\mathsf{P}_+, \text{ with}\\ \mathsf{P}_- &= |001\rangle\langle 001| + |010\rangle\langle 010| + |100\rangle\langle 100| + |111\rangle\langle 111|,\\ \mathsf{P}_+ &= |000\rangle\langle 000| + |011\rangle\langle 011| + |101\rangle\langle 101| + |110\rangle\langle 110|.\end{aligned} \tag{3}$$

Again, the states associated with the propositions corresponding to the projection operators P_- for even parity one and P_+ for even parity zero of the three bits are entangled. The basis of the three-partite binary states has been equipartitioned into two groups of even parity "0" and "1;" that is,

$$\begin{aligned}&\big\{\{|000\rangle, |011\rangle, |101\rangle, |110\rangle\},\\ &\quad\{|001\rangle, |010\rangle, |100\rangle, |111\rangle\}\big\}.\end{aligned} \tag{4}$$

II. PARITY OF BOOLEAN FUNCTIONS

It is well known that Deutsch's problem – to find out whether the output of a binary function of one bit is constant or not; that is, that whether the two outputs have even parity zero or one – can be solved with one quantum query [5, 6]. Therefore it might not appear totally unreasonable to speculate that the parity of some Boolean function – a binary function of an arbitrary number of bits – can be determined by a single quantum query. Even though we know that the answer is negative [7] it is interesting to analize the reason why this parity problem is "difficult" even for quantum resources, in particular, quantum parallelism. Because an answer to this question might provide us with insights about the (in)capacities of quantum computations in general.

Suppose we define the functional parity $P(f_i)$ of an n-ary function $f_i = (g_i + 1)/2$ *via* a function $g_i(x_1, \ldots, x_n) \in \{-1, +1\}$ and

$$P(g_i) = \prod_{x_1,\ldots,x_n\in\{0,1\}} g_i(x_1, \ldots, x_n). \tag{5}$$

Let us, for the sake of a direct approach of functional parity, consider all the 2^{2^n} Boolean functions $f_i(x_1, \ldots, x_n)$, $0 \le i \le 2^{2^n} - 1$ of n bits, and suppose that we can represent them by the standard quantum oracle

$$\begin{aligned}U_i(|x_1, \ldots, x_n\rangle|y\rangle) &=\\ |x_1, \ldots, x_n\rangle|y \oplus f_i(x_1, \ldots, x_n)\rangle&\end{aligned} \tag{6}$$

as a means to cope with possible irreversibilities of the functions f_i. Because $f_i \oplus f_i = 0$, we obtain $U_i^2 = \mathbb{I}$ and thus reversibility of the quantum oracle. Note that all the resulting $n+1$-dimensional vectors are not necessarily mutually orthogonal.

For each particular $0 \le i \le 2^{2^n} - 1$, we can consider the set

$$F_i = \{f_i(0, \ldots, 0), \ldots, f_i(1, \ldots, 1)\} \tag{7}$$

of all the values of f_i as a function of all the 2^n arguments. The set

$$\begin{aligned}V &= \{F_i \mid 0 \le i \le 2^{2^n} - 1\}\\ &= \big\{\{f_i(0, \ldots, 0), \ldots, f_i(1, \ldots, 1)\} \mid 0 \le i \le 2^{2^n} - 1\big\}\end{aligned} \tag{8}$$

is formed by all the 2^{2^n+n} Boolean functional values $f_i(x_1, \ldots, x_n)$. Moreover, for every one of the 2^{2^n} different Boolean functions of n bits the 2^n functional output values characterize the behavior of this function completely.

In the next step, suppose we equipartition the set of all these functions into two groups: those with even parity "0" and "1," respectively. The question now is this: can we somehow construct or find two mutually orthogonal subspaces (orthogonal projection operators) such that all the parity "0" functions are represented in one subspace, and all the parity "1" are in the other, orthogonal one? Because if this would be the case, then the corresponding (equi-)partition of basis vectors spanning those two subspaces could be coded into a quantum query [3] yielding the parity of f_i in a single step.

We conjecture that involvement of one or more additional auxiliary bits (e.g., to restore reveribility for non-reversible f_i's) cannot the improve the situation, as any uniform (over all the functions f_i) and non-adaptive procedure will not be able to generate proper orthogonality relations.

We know that for $n = 1$ this task is feasible, since (we recoded the functional value "0" to "-1")

f_i	$P(f_i)$	$f_i(0)$	$f_i(1)$
f_0	0	-1	-1
f_1	0	$+1$	$+1$
f_2	1	-1	$+1$
f_3	1	$+1$	-1

(9)

and the two parity cases "0" and "1," are coded into rthogonal subspaces spanned by $(1, 1)$ and $(-1, 1)$, respectively.

This is no longer true for $n = 2$; due to an overabundance of functions, the vectors corresponding to both parity cases "0" and "1" span the entire Hilbert space:

f_i	$P(f_i)$	$f_i(00)$	$f_i(01)$	$f_i(10)$	$f_i(11)$
f_0	0	-1	-1	-1	-1
f_1	0	-1	-1	$+1$	$+1$
f_2	0	-1	$+1$	-1	$+1$
f_3	0	-1	$+1$	$+1$	-1
f_4	0	$+1$	-1	-1	$+1$
f_5	0	$+1$	-1	$+1$	-1
f_6	0	$+1$	$+1$	-1	-1
f_7	0	$+1$	$+1$	$+1$	$+1$
f_8	1	-1	-1	-1	$+1$
f_9	1	-1	-1	$+1$	-1
f_{10}	1	-1	$+1$	-1	-1
f_{11}	1	-1	$+1$	$+1$	$+1$
f_{12}	1	$+1$	-1	-1	-1
f_{13}	1	$+1$	-1	$+1$	$+1$
f_{14}	1	$+1$	$+1$	-1	$+1$
f_{15}	1	$+1$	$+1$	$+1$	-1

(10)

The results of this section are also relevant for making precise Zeilinger's *foundational principle* [1, 2] claiming that an n-partite system can be specified by exactly n bits (dits in general). The issue is what exactly is a "specification?"

ACKNOWLEDGMENTS

This research has been partly supported by FP7-PEOPLE-2010-IRSES-269151-RANPHYS.

[1] Anton Zeilinger, "Quantum teleportation and the non-locality of information," Philosophical Transactions of the Royal Society of London A **355**, 2401–2404 (1997).

[2] Anton Zeilinger, "A foundational principle for quantum mechanics," Foundations of Physics **29**, 631–643 (1999).

[3] Niko Donath and Karl Svozil, "Finding a state among a complete set of orthogonal ones," Physical Review A **65**, 044302 (2002), arXiv:quant-ph/0105046.

[4] Karl Svozil, "Quantum information in base n defined by state partitions," Physical Review A **66**, 044306 (2002), arXiv:quant-ph/0205031.

[5] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[6] David N. Mermin, *Quantum Computer Science* (Cambridge University Press, Cambridge, 2007).

[7] Edward Farhi, Jeffrey Goldstone, Sam Gutmann, and Michael Sipser, "Limit on the speed of quantum computation in determining parity," Physical Review Letters **81**, 5442–5444 (1998), arXiv:quant-ph/9802045.