On the solution of trivalent decision problems by quantum state identification

Karl Svozil*
Institut für Theoretische Physik, University of Technology Vienna,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria

and

Josef Tkadlec†
Department of Mathematics, Faculty of Electrical Engineering,
Czech Technical University,
166 27 Praha, Czech Republic

January 29, 2009

Abstract

The trivalent functions of a trit can be grouped into equipartitions of three elements. We discuss the separation of the corresponding functional classes by quantum state identifications.

1 Quantum computation by state identification

One of the advantages of quantum computation [1, 2, 3, 4, 5, 6, 7, 8] over classical algorithms [9, 10] is due to the fact that throughout a quantum computation, some classically useful information can be encoded by distributing it over different particles or quanta, such that [11, 12]

- measurements of *single* quanta are irrelevant, yield "random" results, and even destroy the original information (by asking complementary questions);
- well defined correlations exist and can be defined among different particles or quanta — even to the extend that a state is solely defined by propositions about *collective* (or *relative*) properties of the particles or quanta involved; and

*email: svozil@tuwien.ac.at
†email: tkadlec@fel.cvut.cz

- identifying a given state of a quantized system can yield information about *collective* (or *relative*) properties of the particles or quanta involved.

That is, unlike classical physical states, quantum states can also be characterized with respect to propositions and properties not encoded into a *single* quantum, but "spread among" quanta in an entangled multi-partite state [13, 14, 15, 16, 17, 18, 19]. Stated differently, according to Brukner, Zukowski and Zeilinger [20], the essence of entanglement can be identified by two observations: the finiteness of the amount of information per participating quantum, and the possibility that *"the information in a composite system resides more in the correlations than in properties of individuals."* This is also evident from the fact that entangled states cannot be represented as the product of the individual states of the participating quanta (cf. Ref. [3], Sect. 1.5).

Suppose one is interested in a decision problem which could be associated with some *"collective"* property or behaviour; related to or involving, for instance,

- a function over a wide range of its arguments,
- which is of "comparative" nature; that is, only the relative functional values count;
- for which the single functional values are irrelevant; e.g., are of no interest, "annoying" or are otherwise unnecessary.

Then it is not completely unreasonable to speculate that one could use the kind of distributive information capacity encountered in the quantum physics of multipartite states for a more effective (encryption of the) solution.

The potentiality to quantum mechanically solve decision problems by quantum computing an appropriate multipartite state is not only present in binary decision problems of the usual type, such as Deutsch's algorithm [21, 22, 23, 2, 3]. It can be extended to d-ary decision problems on dits. (For the related state determination problem, see Ref. [13], footnote 6, and Ref. [18].)

In what follows we shall consider as the simplest of such problems the trivalent functions of one trit. We shall group them in three functional classes corresponding to an equipartition of the set of functions into three elements. We then investigate the possibility to separate each of these classes by quantum state identifications [17, 18].

A strategy to identify an observable associated with the solution of a decision problem can be implemented via the method of general state identification [17, 18, 19] as follows [12]:

1. Re-encode the behaviour of the algorithm or function involved in the decision problem into an orthogonal set of states, such that every distinct function results in a *single* distinct state orthogonal to all the other ones. Suppose that this is impossible because the number of functions exceeds the number of orthogonal states, then

(a) one could attempt to find a suitable representation of the functions in terms of the base states; e.g., the generalized Deutsch algorithm in Ref. [12].

(b) Alternatively, the dimension of the Hilbert space could be increased by the addition of auxiliary Qbits. The latter method is hardly feasible for general q-ary functions of n dits, since the number of possible functions increases with q^{d^n}, as compared to the dimension d^n of the Hilbert space of the input states.

In our case of trivalent ($q = 3$) functions of a single ($n = 1$) trit ($d = 3$), there are 27 such functions on three-dimensional Hilbert space. [For the original Deutsch algorithm computing the parity (constancy or nonconstancy) of the four binary functions of one bit, there are $2^{2^1} = 4$ such functions.] For a one-to-one correspondence between functions and orthogonal states, trivalent decision problems among the 27 trivalent functions of a single trit require three three-state quanta associated with the set of $3^3 = 27$ states corresponding to some orthogonal base in $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$.

2. Create three *equipartitions* containing three elements per partition — thus, every such partition element contains nine orthogonal states — such that

   (a) *one of the partitions* corresponds to the solution of the decision problem.

   (b) The other two partitions "complete" the system of partitions such that the set theoretic intersection of any three arbitrarily chosen elements of the three partition with *one element per partition* always yields a *single* base state.

3. Formally, the three partitions correspond to a system of three co-measurable *filter operators* F_i, $i = 1, 2, 3$ with the following properties:

   (F1) Every filter F_i corresponds to an operator (or a set of operators) which generates one of the three equipartitions. (A filter is said to separate two eigenstates if their eigenvalues are different.)

   (F2) From each one of the three partitions of (F1), take an arbitrary element. The intersection of these elements of all different partitions (one element per partition) results in a *single* one of the 27 different states.

   (F3) The union of all those single states generated by the intersections of (F2) is the entire set of states.

4. As the first partition corresponds to the solution of the decision problem, the corresponding first filter operator corresponds to the "quantum oracle" operator solving the decision problem on the set of states corresponding to the different cases or branches involved — one state per case or branch.

$f_0: \ (---)$	$f_9: \ (0--)$	$f_{18}: \ (+--)$
$f_1: \ (--0)$	$f_{10}: \ (0-0)$	$f_{19}: \ (+-0)$
$f_2: \ (--+)$	$f_{11}: \ (0-+)$	$f_{20}: \ (+-+)$
$f_3: \ (-0-)$	$f_{12}: \ (00-)$	$f_{21}: \ (+0-)$
$f_4: \ (-00)$	$f_{13}: \ (000)$	$f_{22}: \ (+00)$
$f_5: \ (-0+)$	$f_{14}: \ (00+)$	$f_{23}: \ (+0+)$
$f_6: \ (-+-)$	$f_{15}: \ (0+-)$	$f_{24}: \ (++-)$
$f_7: \ (-+0)$	$f_{16}: \ (0+0)$	$f_{25}: \ (++0)$
$f_8: \ (-++)$	$f_{17}: \ (0++)$	$f_{26}: \ (+++)$

Table 1: Enumeration of all trivalent functions of a single trit in lexicographic order "$- < 0 < +$."

Ideally, in order for the above strategy to work in three-dimensional Hilbert space of a single Qtrit, one should find a function g on the set of trivalent functions of a trit "folding" the decision problem into a *single* triple of orthogonal vectors. However, as has been already pointed out, because the number of functions may exceed the dimension of the Hilbert space, this task might be impossible. For some decision problem, it might still be possible to find a suitable vector representation for the functional values. Another possibility might be the enlargement of Hilbert space by the inclusion of more auxiliary Qbits.

2 Options for "folding" the decision problem into a single Qtrit

For the sake of demonstration, let us again consider our example of trivalent functions of a single trit. Formally, we shall consider the functions

$$f\colon \{-,0,+\} \to \{-,0,+\}$$

which will be denoted as triples

$$\big(f(-), f(0), f(+)\big)\ .$$

There are $3^{3^1} = 27$ such functions. They can be enumerated in lexicographic order "$- < 0 < +$" as in Table 2.

The trits will be coded by elements of some orthogonal base in $\mathbb{C}^3$. Without loss of generality we may take $(1,0,0) = |-\rangle$, $(0,1,0) = |0\rangle$, $(0,0,1) = |+\rangle$.

For a given "quantum oracle" function

$$g\colon \{-,0,+\} \to \mathbb{C}$$

we represent a function $f\colon \{-,0,+\} \to \{-,0,+\}$ by a linear subspace of $\mathbb{C}^3$ generated by the vector

$$g\big(f(-)\big)\,|-\rangle + g\big(f(0)\big)\,|0\rangle + g\big(f(+)\big)\,|+\rangle\,,$$

i.e., by the vector

$$\big(g(f(-)), g(f(0)), g(f(+))\big).$$

In order to be able to implement the first, re-encoding, step of the above strategy, we will be searching for a function g such that the subspaces representing functions $\{-,0,+\} \to \{-,0,+\}$ are nonzero and form the smallest possible number — ideally only one — of orthogonal triples.

First, let us show that we may find a function g such that we obtain three orthogonal triples of orthogonal vectors, each one of the three triples containing nine triples of the form $\big(f(-), f(0), f(+)\big)$ associated with cases of the functions f which can grouped into three partitions of three triples of the form $\big(f(-), f(0), f(+)\big)$. Let the values of g be the $\sqrt[3]{1}$ (in the set of complex numbers). Let us, for the sake of simplicity and briefness of notation, denote $\alpha = \mathrm{e}^{2\pi \mathrm{i}/3} = -\frac{1}{2}(1 - i\sqrt{3})$. Then the values of g are α, $\alpha^2 = \alpha^* = \mathrm{e}^{-2\pi \mathrm{i}/3} = -\frac{1}{2}(1 + i\sqrt{3})$ and $\alpha^3 = 1$. Moreover, $\alpha\alpha^* = 1$ and $\alpha + \alpha^* = -1$. Then, the "quantum oracle" function g might be given by the following table:

x	$-$	0	$+$
$g(x)$	α^*	1	α

and (if we identify '$-$' with '-1' and '$+$' with '$+1$') might be expressed by

$$g(x) = \alpha^x = \mathrm{e}^{2\pi \mathrm{i} x/3}\,.$$

g maps the 27 triples of functions $\big(f(-), f(0), f(+)\big)$ into nine groups of three triples of functions, such that triples within the nine groups are assigned the same vector (except a nonzero multiple) by the scheme enumerated in Table 2. In every column we obtain an orthogonal triple of vectors

$$\begin{aligned} t_1 &= \{(1,1,1), (1,1,\alpha), (1,1,\alpha^*)\}\,, \\ t_2 &= \{(1,\alpha,\alpha^*), (1,\alpha,1), (1,\alpha^*,1)\}\,, \\ t_3 &= \{(1,\alpha^*,\alpha), (\alpha,1,1), (\alpha^*,1,1)\}\,. \end{aligned}$$

Moreover, vectors from different orthogonal triples are apart by the same angle ϕ, for which $\cos\phi = \sqrt{3}/3$.

Now, let us prove by contradiction that in general the function g cannot be defined in such a way that we obtain at most two orthogonal triples of subspaces. This implies that g cannot "generate" a *single* triple of orthogonal vectors or subspaces, — with nine different functions $\big(f(-), f(0), f(+)\big)$ per element element of that triple — required for the method of computation by state identification in three-dimensional Hilbert space.

For the sake of contradiction, let us suppose that this proposition is false, e.g., that there is a function g such that we obtain at most two orthogonal triples of subspaces.

$\left.\begin{matrix}(-,-,-)\\(0,0,0)\\(+,+,+)\end{matrix}\right\}\mapsto(1,1,1)$	$\left.\begin{matrix}(-,-,0)\\(0,0,+)\\(+,+,-)\end{matrix}\right\}\mapsto(1,1,\alpha)$	$\left.\begin{matrix}(-,-,+)\\(0,0,-)\\(+,+,0)\end{matrix}\right\}\mapsto(1,1,\alpha^*)$
$\left.\begin{matrix}(-,0,+)\\(0,+,-)\\(+,-,0)\end{matrix}\right\}\mapsto(1,\alpha,\alpha^*)$	$\left.\begin{matrix}(-,0,-)\\(0,+,0)\\(+,-,+)\end{matrix}\right\}\mapsto(1,\alpha,1)$	$\left.\begin{matrix}(-,+,-)\\(0,-,0)\\(+,0,+)\end{matrix}\right\}\mapsto(1,\alpha^*,1)$
$\left.\begin{matrix}(-,+,0)\\(+,0,-)\\(0,-,+)\end{matrix}\right\}\mapsto(1,\alpha^*,\alpha)$	$\left.\begin{matrix}(0,-,-)\\(+,0,0)\\(-,+,+)\end{matrix}\right\}\mapsto(\alpha,1,1)$	$\left.\begin{matrix}(+,-,-)\\(-,0,0)\\(0,+,+)\end{matrix}\right\}\mapsto(\alpha^*,1,1)$

Table 2: Enumeration of the map g of all trivalent functions $\big(f(-),f(0),f(+)\big)$ into nine groups of three triples of functions, such that triples within the nine groups are assigned the same vector (except a nonzero multiple).

First, all values $g(-),g(0),g(+)$ are nonzero [if, e.g., $g(-)=0$ then the vector $\big(g(-),g(-),g(-)\big)$ assigned to the function $(-,-,-)$ is a zero vector]. Hence, we obtain a vector $\big(g(-),g(-),g(-)\big)$ that is a nonzero multiple of the vector $(1,1,1)$.

Second, $g(-),g(0),g(+)$ cannot have the same value (in this case we obtain only one subspace generated by the vector $(1,1,1)$).

Let us show that the vectors assigned to the functions $(-,-,0)$ and $(-,0,0)$ are not orthogonal. Indeed, if $\big(g(-),g(-),g(0)\big)$ and $\big(g(-),g(0),g(0)\big)$ are orthogonal, then they have a zero scalar product $0=g(-)\,g(-)^*+g(-)\,g(0)^*+g(0)\,g(0)^*=|g(-)|^2+g(-)\,g(0)^*+|g(0)|^2$ and therefore $g(-)\,g(0)^*$ is a negative real number. Hence $0=|g(-)|^2-|g(-)|\cdot|g(0)|+|g(0)|^2=\big(|g(-)|-\frac{1}{2}\,|g(0)|\big)^2+\frac{3}{4}\,|g(0)|^2$ and therefore $g(0)=0$ that is impossible.

Let us show that all values $g(-),g(0),g(+)$ are different. Indeed, let, e.g., $g(-)=g(0)$. Since $g(-),g(0),g(+)$ cannot have the same value, we obtain $g(+)\neq g(-)$ and therefore the vectors $\big(g(-),g(-),g(+)\big)$ and $\big(g(-),g(+),g(+)\big)$ are not multiples of the vector $(1,1,1)$ and do not generate the same subspace. Analogously as in the previous paragraph we can show that the vectors $\big(g(-),g(-),g(+)\big)$ and $\big(g(-),g(+),g(+)\big)$ are not orthogonal, hence they do not belong to one orthogonal triple and therefore at least one of these vectors is orthogonal to $(1,1,1)$. Let, e.g., $\big(g(-),g(-),g(+)\big)$ is orthogonal to $(1,1,1)$. Then we obtain a zero scalar product $0=2\,g(-)+g(+)$ and therefore the vector $\big(g(-),g(-),g(+)\big)$ is a multiple of $(1,1,-2)$. The subspace making an orthogonal triple with subspaces generated by vectors $(1,1,1)$ and $(1,1,-2)$ is generated by $(1,-1,0)$. But, since all values $g(-),g(0),g(+)$ are nonzero, this subspace is not obtained.

We have shown that the subspaces assigned to functions $(-,-,0)$ and $(-,0,0)$ are not orthogonal and do not coincide (otherwise $g(-) = g(0)$). Hence they do not belong to one orthogonal triple and at least one of them should belong to an orthogonal triple with the space generated by the vector $(1,1,1)$. Let, e.g., $\big(g(-), g(-), g(0)\big)$ is orthogonal to the vector $(1,1,1)$. Then we obtain a zero scalar product $0 = 2\,g(-) + g(0)$. Analogously (using the transformations $(-,0) \to (-,+)$ and $(-,0) \to (0,+)$) we can show that one of the vectors $\big(g(-), g(-), g(+)\big)$ and $\big(g(-), g(+), g(+)\big)$ ($\big(g(0), g(0), g(+)\big)$ and $\big(g(0), g(+), g(+)\big)$, resp.) is orthogonal to the vector $(1,1,1)$ and therefore $0 = 2\,g(-) + g(+)$ or $0 = g(-) + 2\,g(+)$ ($0 = 2\,g(0) + g(+)$ or $0 = g(0) + 2\,g(+)$, resp.). Since all values $g(-), g(0), g(+)$ are different and $0 = 2\,g(-) + g(0)$, we obtain that $0 \neq 2\,g(-)+g(+)$ and $0 \neq g(0)+2\,g(+)$. Hence $0 = g(-)+2\,g(+)$ and $0 = 2\,g(0)+g(+)$. The system of equations $0 = 2\,g(-)+g(0)$, $0 = g(-)+2\,g(+)$ and $0 = 2\,g(0) + g(+)$ has the only solution $g(-) = g(0) = g(+) = 0$, which results in a complete contradiction.

3 Increasing the dimension of state space by additional quanta

The geometric constraints obtained in the last section can be interpreted as the impossibility to "fold" a decision problem into an appropriate quantum state identification in low-dimensional Hilbert space. As has been mentioned already, this can be circumvented by the introduction of additional quanta, thereby increasing the dimension of Hilbert space. In that way, the functions of a small number of bits can be mapped one-to-one onto orthogonal quantum states. However, this strategy fails for a large number of arguments, since the ratio of the number of q-ary functions of n dits to the dimension of the Hilbert space of n dits $d^{-n}q^{d^n}$ increases fast with growing n.

One possibility of mapping the 27 trivalent functions of one trit into the 27 orthogonal base states of the Hilbert space spanned by three Qtrits is

$$|h\big(f(-)\big)\rangle \otimes |h\big(f(0)\big)\rangle \otimes |h\big(f(+)\big)\rangle\,,$$

with $h = id$ being the identity function. A reversible implementation of this function can be given by

$$\begin{aligned} h:\ &\textstyle\prod_{x\in\{-,0,+\}} |x\rangle|0\rangle \to \\ &\to \textstyle\prod_{x\in\{-,0,+\}} |x\rangle|0 \oplus h(f(x))\rangle = \\ &\qquad \textstyle\prod_{x\in\{-,0,+\}} |x\rangle|h(f(x))\rangle\,, \end{aligned}$$

where "$\oplus$" stands for modulo-two addition.

For the sake of demonstration, consider the following trivalent decision problem associated with the three triples of vectors t_1, t_2, and t_3 as follows:

> *Given some trivalent function of a single trit $f_i(x)$, $i \in \{0,\ldots,26\}$, $x \in \{-,0,+\}$. Find the triple of vectors t among the three triples t_1, t_2 and t_3, such that $g(f_i) \in t$.*

4 Summary

In summary we find that, in three-dimensional Hilbert space, we cannot solve the type of trivalent decision problems discussed above by a single query. Such a behavior has already been observed for the problem to find the parity of an unknown binary function $f : \{0,1\}^k \to \{0,1\}$ of k bits, which turned out to be quantum computationally hard [24, 6, 25, 26, 27]. We conjecture that this hardness increases with the number d of possible states of a single bit.

We have also explicitly discussed a trivalent decision problem which can be interpreted as the solution of a quantum state identification problem.

Acknowledgements

The work was supported by the research plan of the Ministry of Education of the Czech Republic no. 6840770010 and by the grant of the Grant Agency of the Czech republic no. 201/07/1051 and by the exchange agreement of both of our universities.

References

[1] J. Gruska, *Quantum Computing* (McGraw-Hill, London, 1999).

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

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

[4] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and Weaknesses of Quantum Computing," SIAM Journal on Computing **26**, 1510–1523 (1997).
http://dx.doi.org/10.1137/S0097539796300933

[5] Y. Ozhigov, "Quantum Computer Can Not Speed Up Iterated Applications of a Black Box," Lecture Notes In Computer Science **1509**, 152–159 (1998).
http://dx.doi.org/10.1007/3-540-49208-9

[6] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf, "Quantum Lower Bounds by Polynomials," Journal of the ACM **48**, 778–797 (2001).
http://dx.doi.org/10.1145/502090.502097

[7] R. Cleve, "An Introduction to Quantum Complexity Theory," in *Collected Papers on Quantum Computation and Quantum Information Theory*, C. Macchiavello, G. Palma, and A. Zeilinger, eds., pp. 103–127 (2000).

[8] L. Fortnow, "One complexity theorist's view of quantum computing," Theoretical Computer Science **292**, 597–610 (2003).
http://dx.doi.org/10.1016/S0304-3975(01)00377-2

[9] H. Rogers, Jr., *Theory of Recursive Functions and Effective Computability* (MacGraw-Hill, New York, 1967).

[10] P. Odifreddi, *Classical Recursion Theory, Vol. 1* (North-Holland, Amsterdam, 1989).

[11] N. D. Mermin, "From Cbits to Qbits: Teaching computer scientists quantum mechanics," American Journal of Physics **71**, 23–30 (2003). http://dx.doi.org/10.1119/1.1522741

[12] K. Svozil, "Characterization of quantum computable decision problems by state discrimination," in *Quantum Theory: Reconsideration of Foundations - 3*, G. Adenier, A. Khrennikov, and T. M. Nieuwenhuizen, eds., **810**, 271–279 (2006). http://link.aip.org/link/?APC/810/271/1

[13] A. Zeilinger, "A Foundational Principle for Quantum Mechanics," Foundations of Physics **29**, 631–643 (1999). http://dx.doi.org/10.1023/A:1018820410908

[14] Č. Brukner and A. Zeilinger, "Malus' law and quantum information," Acta Physica Slovaca **49**, 647–652 (1999).

[15] Č. Brukner and A. Zeilinger, "Operationally invariant information in quantum mechanics," Physical Review Letters **83**, 3354–3357 (1999).

[16] Č. Brukner and A. Zeilinger, "Information and fundamental elements of the structure of quantum theory," in *Time, Quantum and Information*, L. Castell and O. Ischebek, eds. (Springer, Berlin, 2003), pp. 323–355.

[17] N. Donath and K. Svozil, "Finding a state among a complete set of orthogonal ones," Physical Review A (Atomic, Molecular, and Optical Physics) **65**, 044 302 (2002). http://dx.doi.org/10.1103/PhysRevA.65.044302

[18] K. Svozil, "Quantum information in base n defined by state partitions," Physical Review A (Atomic, Molecular, and Optical Physics) **66**, 044 306 (2002). http://dx.doi.org/10.1103/PhysRevA.66.044306

[19] K. Svozil, "Quantum information via state partitions and the context translation principle," Journal of Modern Optics **51**, 811–819 (2004). http://dx.doi.org/10.1080/09500340410001664179

[20] Č. Brukner, M. Zukowski, and A. Zeilinger, "The essence of entanglement," (2002), translated to Chinese by Qiang Zhang and Yond-de Zhang, New Advances in Physics (Journal of the Chinese Physical Society). http://xxx.lanl.gov/abs/quant-ph/0106119

[21] D. Deutsch, "Quantum theory, the Church-Turing principle and the universal quantum computer," Proceedings of the Royal Society of London. Series A, Mathematical and Physical Sciences (1934-1990) **400**, 97–117 (1985). http://dx.doi.org/10.1098/rspa.1985.0070

[22] D. Deutsch and R. Jozsa, "Rapid solution of problems by quantum computation," Proceedings of the Royal Society: Mathematical and Physical Sciences (1990-1995) **439**, 553–558 (1992). http://dx.doi.org/10.1098/rspa.1992.0167

[23] R. Cleve, A. Ekert, C. Macchiavello, and M. Mosca, "Rapid solution of problems by quantum computation," Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **454**, 339–354 (1998). http://dx.doi.org/10.1098/rspa.1998.0164

[24] E. Farhi, J. Goldstone, S. Gutmann, and M. Sipser, "Limit on the Speed of Quantum Computation in Determining Parity," Physical Review Letters **81**, 5442–5444 (1998). http://dx.doi.org/10.1103/PhysRevLett.81.5442

[25] X. Miao, "A polynomial-time solution to the parity problem on an NMR quantum computer," (2001).

[26] R. Orus, J. I. Latorre, and M. A. Martin-Delgado, "Systematic Analysis of Majorization in Quantum Algorithms," European Physical Journal D **29**, 119–132 (2004). http://dx.doi.org/10.1140/epjd/e2004-00009-3

[27] R. Stadelhofer, D. Suterand, and W. Banzhaf, "Quantum and classical parallelism in parity algorithms for ensemble quantum computers," Physical Review A (Atomic, Molecular, and Optical Physics) **71**, 032 345 (2005). http://dx.doi.org/10.1103/PhysRevA.71.032345