On the Solution of Trivalent Decision Problems by Quantum State Identification

http://tph.tuwien.ac.at/∼svozil/publ/2008-UC2008-pres.pdf

Karl Svozil

Institut für Theoretische Physik, Vienna University of Technology,
Wiedner Hauptstraße 8-10/136, A-1040 Vienna, Austria
svozil@tuwien.ac.at

Vienna, Austria, August 28th, 2008

Main results

- Trivalent decision problems via state identification. (KS & Josef Tkadlec):
  - There does not exist a trivalent decision problem encodable into three dimensional Hilbert space.
  - There exists trivalent decision problems encodable into 27–dimensional Hilbert space.
- How to detect hypercomputation (Alexander Leitsch & Günter Schachner & KS):
  - Because of the actual infinities involved, there cannot exist any "operational" proof of hypercomputation, but:
  - "black box" model of hypercomputation with input/output interfaces;
  - find highly "asymmetric" problems which are computationally "easy" to generate and "hard" to solve;
  - two or more hypercomputers are used to "compete" against or "check" themselves.

Why quantum computation?

Why should quantum computation outperform classical computation?

- (Classical) Physics might "harvest" the power of dense sets or maybe even the continuum (e.g., Zeno squeezed time cycles, Banach-Tarski set decomposition, ...) [[Issue: there is no "actual infinity;" even "potential" infinity is only "in our minds," and not operational]]
- Quantum parallelism: n qbits (qdits) can co-represent (via "superposition") exponentially many; i.e., 2^n (d^n) classically mutually exclusive bit (dit) states. [[Issue: how to extract suitable information from the quantum state?]]
- interference; but also possible classical (Cristian Calude);
- Quantum randomness, complementarity (quantum cryptography) & value indefiniteness ...
- ... ...

[[Poll: (i) does quantum computation outperform classical computation? — (ii) and if so: why?]]

Distributing classically useful information among several quanta

(Classical) Information can be encoded by distributing it over different particles or quanta, such that:

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

Related physical concepts

- Quantum entanglement (Schrödinger's "Verschränkung"): the state of two or more "entangled" particles or quanta cannot be constructed from or decomposed into (tensor) products of the states of the "single" particles or quanta involved.
  E.g., in *The essence of entanglement* [quant-ph/0106119], Brukner, Zukowski & Zeilinger write: *"the information in a composite system resides more in the correlations than in properties of individuals."*
- Zeilinger's foundational principle: *"An elementary system carries 1 bit of information."* . . . . more generally: *n* elementary *d*-state systems (like particles or quanta) carry exactly *n* dits of information.
- Example: the (singlet) Bell state $|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle$ of two electrons is defined by the properties that the two particles have opposite spin when measured along two different (orthogonal) directions.

Quantum encoding decision problems about “collective” behaviours

Prospect: if one is interested in a *“collective”* property or behaviour associated with a decision problem; e.g.,

- involving a function on a wide range of its arguments,
- for which the single functional values are irrelevant; e.g., are of no interest, “annoying” or are otherwise unnecessary;

then maybe one could use the kind of distributive information encountered in the quantum physics of multipartite states for a more effective (encryption of the) solution?

Encoding decision problems by state identification problems

- 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
  - one could attempt to find a suitable representation of the functions in terms of the base states.
  - 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 ($d = 3$), and 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.]

Encoding decision problems by state identification problems cntd.

- 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 $\mathbb{C}^3 \otimes \mathbb{C}^3 \otimes \mathbb{C}^3$. Then, create three *equipartitions* containing three elements per partition — thus, every such partition element contains nine orthogonal states — such that
  - *one of the partitions* corresponds to the solution of the decision problem.
  - 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.

Encoding decision problems by state identification problems cntd.

- Formally, the three partitions correspond to a system of three co-measurable *filter operators* $\mathbf{F}_i$, $i = 1, 2, 3$ with the following properties:
  - (F1) Every filter $\mathbf{F}_i$ corresponds to an operator (or a set of operators) which generates one of the three equipartitions of the 27-dimensional state space into three slices (i.e., partition elements) containing $27/3 = 9$ states per slice. A filter is said to separate two eigenstates if the 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.
- 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.

Example of trivalent functions of a single trit

Formally, we shall consider the functions

$$f:\ \{-,0,+\}\rightarrow\{-,0,+\}$$

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 follows:

$f_{\mathbf{0}}$:	$(- - -)$	$f_{\mathbf{9}}$:	$(0 - -)$	$f_{\mathbf{18}}$:	$(+ - -)$
$f_{\mathbf{1}}$:	$(- - 0)$	$f_{\mathbf{10}}$:	$(0 - 0)$	$f_{\mathbf{19}}$:	$(+ - 0)$
$f_{\mathbf{2}}$:	$(- - +)$	$f_{\mathbf{11}}$:	$(0 - +)$	$f_{\mathbf{20}}$:	$(+ - +)$
$f_{\mathbf{3}}$:	$(-0-)$	$f_{\mathbf{12}}$:	$(00-)$	$f_{\mathbf{21}}$:	$(+0-)$
$f_{\mathbf{4}}$:	(-00)	$f_{\mathbf{13}}$:	(000)	$f_{\mathbf{22}}$:	$(+00)$
$f_{\mathbf{5}}$:	$(-0+)$	$f_{\mathbf{14}}$:	$(00+)$	$f_{\mathbf{23}}$:	$(+0+)$
$f_{\mathbf{6}}$:	$(- + -)$	$f_{\mathbf{15}}$:	$(0 + -)$	$f_{\mathbf{24}}$:	$(+ + -)$
$f_{\mathbf{7}}$:	$(- + 0)$	$f_{\mathbf{16}}$:	$(0 + 0)$	$f_{\mathbf{25}}$:	$(+ + 0)$
$f_{\mathbf{8}}$:	$(- + +)$	$f_{\mathbf{17}}$:	$(0 + +)$	$f_{\mathbf{26}}$:	$(+ + +)$

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

Example of trivalent functions of a single trit cntd.

For a given "quantum oracle" function

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

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

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

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.

Example of trivalent functions of a single trit cntd.

Consider 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 $\big(f(-), f(0), f(+)\big)$ and 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

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

Example of trivalent functions of a single trit cntd.

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 following scheme:

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

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

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

More generally, one can 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.

Example of trivalent functions of a single trit cntd.

The geometric constraints in threedimensional Hilbert space can be interpreted as the impossibility to “fold” a decision problem into an appropriate quantum state identification in low-dimensional Hilbert space.

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.

How to acknowledge hypercomputation?

Already in 1958, Martin Davis, in *Computability and Unsolvability* (p. 11) asks:
“ *. . . how can we ever exclude the possibility of our being presented, some day (perhaps by some extraterrestrial visitors), with a (perhaps extremely complex) device or “oracle” that “computes” a non-computable function?”*

How to acknowledge hypercomputation cntd.?

Some concepts and questions:

- Black box model;
- Are there there any “operational verifiability” beyond the capacity to solve low-polynomial (in terms of time & memory space) problems?
- Consider asymmetric problems which are “easy” to generate but “difficult” to solve; e.g., graph isomorphism.
- Consider two or more hypercomputers which are used to “compete” against or “check” themselves.

Thank you for your attention!