WAYNE C. MYRVOLD

THE DECISION PROBLEM FOR ENTANGLEMENT

1. A PROBLEM IN A DREAM

In March 1995, Abner Shimony attended a conference held in honor of the sixtieth anniversary of the famous Einstein–Podolsky–Rosen paper at Technion University in Haifa, Israel. Among the lecturers at the conference was Alain Aspect. In Paris immediately after the conference, Abner had a dream in which Aspect, in a lecture at the conference, posed the problem: is it algorithmically decidable whether a given quantum-mechanical state is entangled or not? Upon returning to the United States, Abner posed the question to me and added: "If not, can we effectively decide whether or not a state is within ε of a product state?"

The answer, as will be shown below, is that there is an algorithmic procedure that, given a real number ε and a Hilbert-space vector ψ, will return the answer "yes" if there is a product state whose distance to ψ is less than ε, the answer "no" if all product states are a distance greater than ε from ψ, and return no answer (fail to terminate) if the distance from ψ to the nearest product state is exactly ε. There is no algorithm that answers correctly in all cases the question. "Is there a product state whose distance from ψ is less than or equal to ε?" In particular, the question whether there is a product state whose distance to ψ is zero (that is, whether ψ is a product state) is not effectively decidable.

2. TERMINOLOGY

The problem occurs at the intersection of computability theory and the mathematics of quantum mechanics. Since those who are familiar with the concepts and terminology of one of these fields are often unfamiliar with the other field, I present here basic concepts from both. Readers familiar with these concepts should skip this section.

a) Concepts From Computability Theory

These concepts will be defined in a relatively informal manner (see Rogers (1967) for a more rigorous treatment). I assume that the reader is familiar with the concept of a recursive function on the natural numbers. Intuitively, a function $f\colon \mathbb{N}\rightarrow\mathbb{N}$ is recursive (or computable; I will use the terms interchangeably) if and only if there is a computer program, in one of the standard programming languages, that would compute f for any value of n if time and memory restrictions were removed. A partial function on the natural numbers is a function that is not necessarily defined for every number; a partial function ϕ is a *partial recursive function* if and only if there is a program that computes $\phi(n)$ for every number n in the domain of ϕ and fails to terminate when given numbers not in the domain of ϕ.

R.S. Cohen, et al. (eds), Potentiality, Entanglement and Passion-at-a-Distance, 177–190

It is possible to devise a system for assigning a unique code number to every computer program (or, what amounts to the same thing, to every Turing Machine). This coding gives rise to the best-known example of a problem that is not effectively solvable: the Halting Problem. There is no algorithmic procedure that determines, for every k, n, whether or not n is in the domain of the function computed by program #k – that is, whether or not program #k terminates on input n. There is not even an algorithmic procedure for solving the special case of determining whether or not program #k halts on input k.

A set $A \subseteq \mathbb{N}$ is *decidable*, or *recursive*, if and only if there is a recursive function c_A such that:

$$c_A(n) = \begin{cases} 1, & \text{if } n \in A \\ 0, & \text{if } n \notin A \end{cases}$$

A set $A \subseteq \mathbb{N}$ is *recursively enumerable* if and only if A is the range of some recursive function. Recursively enumerable sets are sometimes called *semi-recursive* sets. It can be shown that a set is recursively enumerable if and only if it is the domain of some partial recursive function.

In dealing with real numbers, we must use rational approximations as input and output of our algorithms. Assume an effective coding of the rational numbers by natural numbers; denote by $Q(n)$ the rational number whose code-number is n. A sequence $\{r_n\}$ of rational numbers is a *computable sequence* of rationals if and only if there is a recursive function $d(n)$ such that $Q(d(n)) = r_n$ for every n; a double sequence $\{r_{kn}\}$ of rationals is a *computable double sequence* if and only if there is a recursive function of two variables $g(k,n)$ such that $Q(g(k,n)) = r_{kn}$. An effective method for calculating a real number x is a recursive procedure for generating rational approximations to x: that is, a recursive function $d(n)$ such that, for all n, the number $d(n)$ codes a rational number whose distance from x is less than 2^{-n}. A real number x is a *computable real* if and only if there is a computable sequence of rationals $\{r_n\}$ such that $|x - r_n| < 2^{-n}$ for all $n \in \mathbb{N}$; a sequence of real numbers $\{x_k\}$ is a computable sequence if and only if there is a computable double sequence of rationals $\{r_{kn}\}$ such that $|x_k - r_{kn}| < 2^{-n}$ for all $k, n \in \mathbb{N}$.

To extend the notion of computability to functions of a real variable, imagine a computer program that computes a function $F(x)$ as follows. The program operates with rational approximations to both the arguments x and values $F(x)$. The initial input to the program consists of a number k, indicating that an output is required that approximates the value of $F(x)$ to within a precision of 2^{-k}. The program then requests, and is provided with, a rational approximation to x within a certain degree of precision, which it specifies. As the computation proceeds, it may request further approximations to x. After a finite amount of time, the program must respond with the desired rational approximation to $F(x)$. The class of functions computed by such programs is identical to a class of functions defined by A. Grzegorczyk (1955) and is, therefore, known as the class of *Grzegorczyk-computable* functions. Note that nothing has been said about how the rational approximations to x that are fed into the program are obtained. Nothing in the way the program works requires the

value of x for which the function $F(x)$ is computed to be a computable number. As far as the program is concerned, the source of inputs could be replaced by a "magic box" that generates rational approximations to some non-computable number. We thus obtain, by this scheme, a function F that is defined for all values of the argument, not merely the computable ones.

A program for computing a function F must respond with a value of $F(x)$ after receiving only a finite approximation to the argument x, and so "knows" only that x lies within a certain small interval. In doing so, it is, in effect, asserting that, for all values of x within that interval, $F(x)$ differs from its output by an amount less than the degree of precision that its output was requested to have. This means that a computable function is always continuous. Grzegorczyk showed that a function $F:\mathbb{R} \to \mathbb{R}$ is Grzegorczyk-computable if, and only if:

i) For any computable sequence $\{x_k\}$, $\{F(x_k)\}$ is a computable sequence.
ii) F is effectively uniformly continuous with respect to rational segments. That is, there is a recursive function $g(n, m, k)$ such that for all $n, m, k \in \mathbb{N}$ and $x, y \in [Q(n), Q(m)]$, if $|x - y| < 2^{-g(n,m,k)}$ then $|F(x) - F(y)| < 2^{-k}$.

The thesis that a function of a real variable must be continuous if it is computable has struck some people as counterintuitive. John Earman (1986:119), for example, has expressed the opinion that such a simple function as the step-function:

$$H(x) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases}$$

ought to be classed as computable. This function, however, violates another intuitively plausible principle about computable functions: a computable function ought to map computable sequences of reals onto computable sequences. To see this, suppose an effective coding of Turing machines has been given. Define a computable double sequence of rationals $\{q_{kn}\}$ as follows: if Turing machine T_k does not halt, on input k, in n steps or fewer, $q_{kn} = 0$; if T_k *does* halt on input k in n steps or fewer, let w be the number of steps taken by the machine before halting, and take $q_{kn} = -2^{-w}$. Then $\{q_{kn}\}$ converges to a limit x_k that is equal to 0 if T_k does not halt on input k, and is less than 0 if T_k halts on input k. Moreover, $|q_{kn} - x_k| < 2^{-n}$ for all k, n. $\{x_k\}$ is, therefore, a recursive sequence of real numbers, but:

$$H(x_k) = \begin{cases} 0, & \text{if } T_k \text{ halts on input } k \\ 1, & \text{if not} \end{cases}$$

Thus, if there were a machine that calculated the step function, we could construct a machine to solve the Halting Problem.

Thus far, we have assumed we have been dealing with functions defined on the entire real line; the definition may be extended to functions defined on subsets of the real line by not requiring the machine to produce an output for every value of the input variable x. The functions so computed will be called *partial computable functions* of a real variable. The modified step function:

$$H'(x) = \begin{cases} 0, & x < 0 \\ 1, & x > 0 \end{cases}$$

is a partial computable function on the domain $\mathbb{R} - \{0\}$.

A subset A of the real line will be called *recursive*, or *decidable*, if and only if there is a computable function C_A such that:

$$C_A(x) = \begin{cases} 1, & \text{if } x \in A \\ 0, & \text{if } x \notin A \end{cases}$$

A subset $A \subseteq \mathbb{R}$ is called *semi-recursive* if and only if there is a partial computable function C_A such that $C_A(x)$ is equal to 1, if $x \in A$, and is undefined for $x \notin A$.

Semi-recursive subsets of $\mathbb{R}$ are the analogs of recursively enumerable subsets of $\mathbb{N}$. Just as a subset $A \subseteq \mathbb{N}$ is recursive if and only if A and $\mathbb{N} - A$ are both recursively enumerable, a subset $A \subseteq \mathbb{R}$ is recursive if and only if A and $\mathbb{R} - A$ are both semi-recursive. An important difference lies in the following fact: the only recursive subsets of $\mathbb{R}$ are $\mathbb{R}$ itself and the empty set ø (this follows from the continuity of computable functions).

Here, again, is a consequence of our definitions that may seem counterintuitive (see Penrose, 1989: 124–129 for a discussion). It might seem, for example, that such a simple set as the closed unit interval [0,1] ought to be classed as a decidable set. The same argument used above to show that computability of the step function implies solvability of the Halting Problem can be employed to show that decidability of [0,1] implies the solvability of the Halting Problem.

If a number x lies in the open interval (0,1), then a sufficiently precise approximation to x allows one to ascertain that fact; and similarly, if x lies outside [0,1]. If, however, x is equal to 0 or 1, then no mere approximation to x permits one to determine whether or not x is in [0,1]. That is, although [0,1] is not a semi-recursive set, its interior (0,1), and its exterior, which consists of all points not in the interval [0,1], *are* both semi-recursive sets. The set [0,1], therefore, is "almost" decidable; we can effect a decision as long as the endpoints are avoided. There are cases in analysis and physics in which the boundaries of a given region are of little concern and the regions of interest are the interior and the exterior of the set. It is, therefore, useful to define the concept: a subset $A \subseteq \mathbb{R}$ is *decidable, disregarding boundaries* if and only if the interior and exterior of A are both semi-recursive sets.

The kernel of our treatment of computability for the reals and for functions on the reals was our ability to approximate any element of the uncountable set of real numbers to arbitrary precision by an element of the set of rationals, which is a countable set and therefore susceptible to being coded by the natural numbers. The treatment, therefore, can be extended to any metric space with a countable dense subset (that is, any *separable* metric space). Some examples: complex numbers can be approximated to arbitrary degree of precision by "rational" complex numbers of the form $a + bi$, with a, b rational; points in $\mathbb{R}^n$ can be approximated by points of the form $(q_1, \ldots, q_n)$ with all the q_i's rational; and if $\{u_i\}$ is a basis of an infinite-dimensional Hilbert space, then any vector in the space can be approximated by a finite linear combination of these basis vectors with coefficients that are "rational" complex numbers.

Let X be a separable metric space, and let ρ_x be the distance function on X. Let $\{Q(n)\}$ be an enumeration of a countable dense subset of X. With respect to the coding Q, an element $x \in X$ is said to be *computable* if and only if there is a computable function $d(n)$ such that $\rho_X(x, Q(d(n)) < 2^{-n}$ for all n. Similarly, a sequence $\{x_k\}$ is a *computable sequence* if and only if there is a computable function $g(k,n)$ such that $\rho_X(x_k, Q(g(k, n)) < 2^{-n}$ for all k, n.

Computability of functions $F{:}X \to Y$, where X and Y are separable metric spaces, is defined analogously to computability for functions from $\mathbb{R}$ to $\mathbb{R}$. Let $Q_X(n)$ and $Q_Y(n)$ be enumerations of dense subsets of X and Y, respectively. The initial input to the program is, again, a number k, indicating that an approximation to $F(x)$ within a radius 2^{-k} is desired. The program responds with some number m; it is then provided with a number n such that $\rho_X(x, Q_X(n)) < 2^{-m}$. As the computation proceeds, the program may request closer approximations to x. Finally, it outputs a number r such that $\rho_Y(F(x), Q_Y(r)) < 2^{-k}$.

It can be shown that a function $F{:}X \to Y$ is computable in this sense if and only if:

i) For any computable sequence $\{x_k\}$ in X, $\{F(x_k)\}$ is a computable sequence in Y.
ii) There is a recursive function $g(n, k)$ such that, for all $x \in X$ and n, $k \in \mathbb{N}$, if $\rho_X(x, Q_X(n)) < 2^{-g(n,k)}$ then $\rho_Y(F(x), F(Q_Y(n))) < 2^{-k}$.

We define recursive and semi-recursive subsets of X in the same way that they were defined for subsets of $\mathbb{R}$. Two important facts about such sets are the following:

Theorem 2.1.
a) Every semi-recursive set is open in the metric topology.
b) If X is a connected space in the metric topology, then the only decidable subsets of X are X itself and the empty set ø.

Proof. $A \subseteq X$ is semi-recursive if and only if there is a partial computable function $C_A(x)$ such that:

$$C_A(x) = \begin{cases} 1, & \text{if } x \in A \\ \text{undefined}, & \text{if } x \notin A \end{cases}$$

A program returns a verdict that $C_A(x) = 1$ with only the information that x lies close to some specified $Q(n)$; therefore, for any $x \in$ A there is some neighborhood of x consisting entirely of elements of A, and A is open. For part (b), recall that A is decidable if and only if A and $X - A$ are both semi-recursive. By (a), if A is decidable then A and $X - A$ are both open sets. Therefore, X is the union of two disjoint open sets. This is the definition of a disconnected set.◀

b) Concepts From Analysis and Physics

A *metric space* is a non-empty set X on which a two-place function $\rho: X \times X \to \mathbb{R}$ is defined such that, for all $x, y, z \in X$:

$M1.$ $\rho(x,y) \geq 0$.
$M2.$ $\rho(x,y) = 0$ if and only if $x = y$.
$M3.$ $\rho(x,y) = \rho(y,x)$.
$M4.$ $\rho(x,z) \leq \rho(x,y) + \rho(y,z)$.

A subset $E \subseteq X$ is *open* in the metric topology if and only if, for any $x \in E$ there exists $\varepsilon > 0$ such that $y \in E$ for all y such that $\rho(x, y) < \varepsilon$. A *neighborhood* of a point x is any open set containing x. For subsets Y and $Z \subseteq X$, Y is *dense* in Z if and only if every neighborhood of every point in Z contains elements of Y. A subset $Y \subseteq X$ is *somewhere dense* if and only if it is dense in some open set; otherwise; it is *nowhere dense*. A point x lies in the *interior* of a set A if and only if there is a neighborhood of x lying entirely in A. A point x lies in the *exterior* of A if and only if there is a neighborhood of x that is disjoint from A.

A space X is *disconnected* if and only if it is the union of two disjoint, non-empty open sets. X is *connected* if and only if it is not disconnected. The set of real numbers, the set of complex numbers, and Hilbert spaces are all examples of spaces that are connected in their respective metric topologies.

A metric space X is *separable* if and only if there is a countable subset of X that is dense in X. A sequence $\{x_n\}$ of elements of a metric space X is a *Cauchy sequence* if and only if:

$$(\forall k \in \mathbb{N})(\exists N \in \mathbb{N})(\forall n, m \in \mathbb{N})(n, m > N \to \rho(x_n, x_m) < 2^{-k})$$

A Cauchy sequence $\{x_n\}$ converges to a limit y if and only if:

$$(\forall k \in \mathbb{N})(\exists N \in \mathbb{N})(\forall n \in \mathbb{N})(n > N \to \rho(y, x_n) < 2^{-k})$$

A metric space X is *complete* if and only if every Cauchy sequence in X converges to some limit in X.

A *linear vector space* is a non-empty set X on which an addition function + and an operation of scalar multiplication have been defined, such that:

L1. X is an abelian group with group operation $+$. This means that:
a) for all $x, y, z \in X$, $x + (y + z) = (x + y) + z$;
b) for all $x, y \in X$, $x + y = y + x$;
c) there is an element $\mathbf{0} \in X$ such that $x + \mathbf{0} = x$ for all $x \in X$;
d) for every $x \in X$ there is an element $(-x)$ such that $x + (-x) = 0$.
L2. For all $\lambda, \mu \in \mathbb{C}$ and $x \in X$, $\lambda(\mu X) = (\lambda\mu)X$.
L3. For all $\lambda, \mu \in \mathbb{C}$ and $x \in X$, $(\lambda + \mu)X = \lambda X + \mu X$.
L4. $1x = x$.

A *subspace* of a linear vector space X is a subset of X that is closed under the operations of addition and scalar multiplication.

A *normed linear space* is a linear space X on which a norm $\|x\|$ is defined, such that, for all $x, y \in X$ and $\lambda \in \mathbb{C}$:

N1. $\|x\| \geq 0$.
N2. $\|x\| = 0$ if and only if $x = \mathbf{0}$.
N3. $\|\lambda x\| = |\lambda|\|x\|$.
N4. $\|x + y\| \leq \|x\| + \|y\|$.

Every normed linear space is a metric space with metric $\rho(x, y) = \|x + (-y)\|$.

A *Banach space* is a complete normed linear space.

A *Hilbert space* is a Banach space whose norm satisfies the parallelogram law:

$$\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$$

If $\mathscr{H}$ is a Hilbert space, we define the inner product (x, y) on $\mathscr{H}$ by.[1]

$$(x, y) = {}^1/_4[\|x + y\|^2 - \|x - y\|^2 - i(\|x + iy\|^2 - \|x - iy\|^2)]$$

The inner product satisfies, for all $x, y \in \mathscr{H}$ and $\lambda \in \mathbb{C}$:

H1. $(x,x) = \|x\|^2$.
H2. $(x,y + z) = (x,y) + (x,z)$.
H3. $(x,\lambda y) = \lambda(x,y)$.
H4. $(x,y) = (y,x)^*$.

In quantum mechanics, the state of a physical system is represented by a vector in a Hilbert space associated with the system. If the system can be decomposed into two subsystems, with which are associated the Hilbert spaces $\mathscr{H}_1$ and $\mathscr{H}_2$, respectively, then the state of the composite system is represented by a vector in the *product space* $\mathscr{H}_1 \otimes \mathscr{H}_2$. For any $u \in \mathscr{H}_1$ and $v \in \mathscr{H}_2$ there is a corresponding vector $u \otimes v$ in $\mathscr{H}_1 \otimes \mathscr{H}_2$; this mapping satisfies:

P1. For all $u \in \mathscr{H}_1$, $v \in \mathscr{H}_2$, and $\lambda \in \mathbb{C}$, $u \otimes (\lambda v) = (\lambda u) \otimes v = \lambda(u \otimes v)$.
P2. a) For all $u \in \mathscr{H}_1$ and $v_1, v_2 \in \mathscr{H}_2$, $u \otimes (v_1 + v_2) = u \otimes v_1 + u \otimes v_2$.
b) For all $u_1, u_2 \in \mathscr{H}_1$ and $v \in \mathscr{H}_2$, $(u_1 + u_2) \otimes v = u_1 \otimes v + u_2 \otimes v$.
P3. For all $u_1, u_2 \in \mathscr{H}_1$ and $v_1, v_2 \in \mathscr{H}_2$, $(u_1 \otimes v_1, u_2 \otimes v_2) = (u_1, u_2)(v_1, v_2)$.

A vector z in $\mathscr{H}_1 \otimes \mathscr{H}_2$ is a product vector (or product state) if and only if there exist $u \in \mathscr{H}_1$ and $v \in \mathscr{H}_2$ such that $z = u \otimes v$. Product vectors are also said to be *factorizable*. Vectors that are not factorizable are called *entangled*. The physical significance of this is that, if a composite system is in a product state, then each of its components has its own state and its own properties and propensities for behaving in certain ways; a system in an entangled state is not decomposable into independent subsystems. The EPR argument turns upon a system that, though its components are spatially separated, nevertheless remains in an entangled state; this allows for the possibility of the results of measurements performed on one component depending on the results of measurements on the other component.

3. THE DECISION PROBLEM FOR ENTANGLEMENT

Let $\mathscr{H}_1$ and $\mathscr{H}_2$ be (finite- or infinite-dimensional) Hilbert spaces, and let $\mathscr{H}_{12}$ be the product space $\mathscr{H}_1 \otimes \mathscr{H}_2$. Let $\{u_i\}$ and $\{v_j\}$ be orthonormal bases for $\mathscr{H}_1$ and $\mathscr{H}_2$, respectively. $\{u_i \otimes v_j\}$ is then a basis for $\mathscr{H}_{12}$. Let $\mathscr{E}$ be the set of entangled vectors in the product space $\mathscr{H}_{12}$, and let $\mathscr{F}$ be the set of factorizable vectors.

Lemma 3.1. Let ψ be a vector in the product space $\mathscr{H}_{12}$:

$$\psi = \sum_{i,j} c_{ij} u_i \otimes v_j$$

ψ is factorizable if and only if there exist sequences $\{\alpha_i\}$ and $\{\beta_j\}$ such that $c_{ij} = \alpha_i \beta_j$ for all i, j.

The proof of Lemma 3.1 is trivial and will be omitted here.

Lemma 3.2. ψ is factorizable if and only if $c_{ij}c_{mn} = c_{in}c_{mj}$ for all i, j, m, n.

Proof. $\Rightarrow$ If ψ is factorizable, then $c_{ij}c_{mn} = (\alpha_i\beta_j)(\alpha_m\beta_n) = (\alpha_i\beta_n)(\alpha_m\beta_j) = c_{in}c_{mj}$. $\Leftarrow$. Suppose that $c_{ij}c_{mn} = c_{in}c_{mj}$ for all i, j, m, n. If all the c_{ij} 's are zero, then ψ is trivially factorizable, since $\psi = \mathbf{0} = \mathbf{0} \otimes \mathbf{0}$. Suppose, then, that ψ is non-zero, and choose M,N such that $c_{MN} \neq 0$. Define $\alpha_i = c_{iN}/c_{MN}$, $\beta_j = c_{Mj}$. Then, for any i, j, $\alpha_i\beta_j = c_{iN}c_{Mj}/c_{MN} = c_{ij}c_{MN}/c_{MN} = c_{ij}$.◀

Theorem 3.3. The set of entangled states is an open set that is dense in $\mathscr{H}_{12}$.

Proof. To show that $\mathscr{E}$ is an open set, it suffices to show that, for any entangled state ψ, there is a neighborhood of ψ consisting entirely of entangled states. If ψ is entangled, then there exist numbers I, J, N, M such that $c_{IJ}c_{NM} - c_{IM}c_{NJ} \neq 0$. It is clear that, if $|c'_{IJ} - c_{IJ}|$, $|c'_{NM} - c_{NM}|$, $|c'_{IM} - c_{IM}|$ and $|c'_{NJ} - c_{NJ}|$ are all sufficiently small, then $c'_{IJ}c'_{NM} - c'_{IM}c'_{NJ}$ will also be non-zero. Thus, in order to transform ψ into a product state, at least one of c_{IJ}, c_{NM}, c_{IM}, and c_{NJ} must be transformed by a certain minimum amount ε. If $\|\psi' - \psi\| < \varepsilon$, then each of $|c'_{IJ} - c_{IJ}|$, $|c'_{NM} - c_{NM}|$, $|c'_{IM} - c_{IM}|$ and $|c'_{NJ} - c_{NJ}|$ must also be less than ε. Therefore, if $\|\psi' - \psi\| < \varepsilon$, ψ' is entangled.

To show that $\mathscr{E}$ is dense in $\mathscr{H}_1 \otimes \mathscr{H}_2$, observe that, if ψ is non-zero, an arbitrarily small change in only one of the c_{ij}'s suffices to produce an entangled state: If $c_{NM} \neq 0$, and $c_{IJ}c_{NM} - c_{IM}c_{NJ} = 0$, then $c'_{IJ}c_{NM} - c_{IM}c_{Nj} \neq 0$ if $c'_{IJ} \neq c_{IJ}$. If $\psi = \mathbf{0}$, then, since there are arbitrarily small entangled states, there are entangled states in every neighborhood of ψ.◀

Corollary 3.4. The set of factorizable states is a closed set that is nowhere dense.

Proof. This follows from the fact that $\mathscr{E}$, the complement of $\mathscr{F}$, is an open dense set.◀

Theorem 3.5. The set $\mathscr{E}$ of entangled states is semi-recursive but not recursive.

Proof. By Theorem 3.2, ψ is entangled if and only there exist i, j, m, n such that $c_{ij}c_{mn} - c_{in}c_{mj} \neq 0$. A "dovetailing" procedure yields a sequence $\{x_k\}$ such that each of $c_{ij}c_{mn} - c_{in}c_{mj}$ occurs in this sequence infinitely often. Then ψ is entangled if and only if there exists k such that $x_k > 0$. If there is some element of the sequence that is non-zero, it can be found effectively by computing rational approximations to x_k within a precision $2^{-k}\}$ for each k in turn.

To show that $\mathscr{E}$ is not recursive it suffices to observe that its complement, $\mathscr{F}$, is non-empty, and that Hilbert spaces are connected. By Theorem 2.1b, $\mathscr{E}$ is not recursive.◀

We note in passing that, since $\mathscr{E}$ is semi-recursive and its complement, $\mathscr{F}$, has no interior, $\mathscr{E}$ is, trivially, decidable ignoring boundaries. This is perhaps not very interesting, as ignoring the boundary of $\mathscr{F}$ means ignoring the whole of $\mathscr{F}$.

This brings us to the second part of the question. Given an entangled state ψ, can one determine whether or not ψ is within a distance ε of some product state? For $\varepsilon > 0$, define the set of vectors whose distance to some product state is less than ε:

$$\mathscr{F}_\varepsilon = \{\psi | (\exists \chi \in \mathscr{F})(\|\psi - \chi\| < \varepsilon)\}$$

Theorem 3.6 (The Main Result). The function $C: \mathscr{H}_{12} \times \mathbb{R}^+ \to \{0,1\}$, defined by:

$$C(\psi, \varepsilon) = \begin{cases} 1, & \text{if } \psi \in \mathscr{F}_\varepsilon \\ 0, & \text{if } \psi \in \text{Ext } \mathscr{F}_\varepsilon \\ \text{undefined}, & \text{otherwise} \end{cases}$$

is a computable partial function.

It follows immediately from this that, whenever ε is a computable number, $\mathscr{F}_\varepsilon$ is decidable disregarding boundaries.

To prove the main result, we first define the function $\delta(\psi) =$ the greatest lower bound of $\{\|\psi - \chi\| \,|\, \chi \in \mathscr{F}\}$.

Then:

$$C(\psi, \varepsilon) = \begin{cases} 1, & \text{if } \delta(\psi) < \varepsilon \\ 0, & \text{if } \delta(\psi) > \varepsilon \\ \text{undefined} & \text{if } \delta(\psi) = \varepsilon \end{cases} \tag{1}$$

If δ is a computable function, then C is a computable partial function. Theorem 3.6 is established by showing that δ is, indeed, computable. We will consider first the case in which $\mathscr{H}_1 \otimes \mathscr{H}_2$ is a finite-dimensional product space, then show that the infinite-dimensional case reduces to the finite-dimensional case.

The first step is to show that, for any vector ψ in a finite-dimensional product space, there is a closest product state – a product state that minimizes the distance to ψ among product states.

Theorem 3.7. Let $\mathscr{H}_1 \otimes \mathscr{H}_2$ be a finite-dimensional product space. For any $\psi \in \mathscr{H}_1 \otimes \mathscr{H}_2$, there exists $\chi \in \mathscr{F}$ such that $\|\psi - \chi\| = \delta(\psi)$.

Proof. Since $\delta(\psi)$ is the greatest lower bound of $\{\|\psi - \chi\| \,|\, \chi \in \mathscr{F}\}$, there is a sequence $\{\chi_n\}$ of product states such that:

$$\delta(\psi) \leq \|\psi - \chi_n\| < \delta(\psi) + 2^{-n} \tag{2}$$

The sequence $\{\chi_n\}$ is a bounded sequence in the finite-dimensional Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$; it has, therefore, a convergent subsequence (see Friedman, 1970: Theorem 4.3.3). Let $\{\chi'_n\}$ be one such convergent subsequence, and let χ be its limit. Since $\|\psi - \chi'_n\| \to \delta(\psi)$ and $\chi'_n \to \chi$ as $n \to \infty$, $\|\psi - \chi\| = \delta(\psi)$.◀

(*Parenthetical note*: Though the above proof depends on the dimension of $\mathcal{H}_1 \otimes \mathcal{H}_2$ being finite, the theorem holds also for infinite-dimensional product spaces. We will make no use of this fact, so it will not be proven here.)

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be N- and M-dimensional Hilbert spaces, respectively, and let $\{u_i | i = 1, \ldots, N\}$ and $\{v_j | j = 1, \ldots, M\}$ be orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$. Then any vector $\psi \in \mathcal{H}_1 \otimes \mathcal{H}_2$ can be written in the form:

$$\psi = \sum_{i=1}^{N} \sum_{j=1}^{M} c_{ij} u_i \otimes v_j \tag{3}$$

Let χ be a product state in $\mathcal{H}_1 \otimes \mathcal{H}_2$:

$$\chi = (\sum_{i=1}^{N} \alpha_i u_i) \otimes (\sum_{J=1}^{M} \beta_j v_j) = \sum_{i=1}^{N} \sum_{j=1}^{M} \alpha_i \beta_j u_i \otimes v_j \tag{4}$$

$$\|\psi - \chi\|^2 = \sum_{i=1}^{N} \sum_{j=1}^{M} |c_{ij} - \alpha_i \beta_j|^2 \tag{5}$$

By Theorem 3.7, there exist $\{\alpha_i\}$ and $\{\beta_j\}$ that minimize $\|\psi - \chi\|^2$. Moreover, the quantity $\|\psi - \chi\|^2$ depends smoothly on the α_i's and β_j's. We can, therefore, find the minimum by differentiating $\|\psi - \chi\|^2$ by the real and imaginary parts of each α_i and β_j and setting these partial derivatives equal to zero. Doing so yields:

$$\begin{aligned} &\sum_{j=1}^{M} \beta_j^* (c_{ij} - \alpha_i \beta_j) = 0, \quad i = 1, \ldots, N \\ &\sum_{i=1}^{N} \alpha_i^* (c_{ij} - \alpha_i \beta_j) = 0, \quad j = 1, \ldots, M \end{aligned} \tag{6}$$

or:

$$\begin{aligned} &\sum_{j=1}^{M} \beta_j^* c_{ij} - \alpha_i \sum_{j=1}^{M} |\beta_j|^2 = 0, \quad i = 1, \ldots, N \\ &\sum_{i=1}^{N} \alpha_i^* c_{ij} - \beta_j \sum_{i=1}^{N} |\alpha_i|^2 = 0, \quad j = 1, \ldots M \end{aligned} \tag{7}$$

If χ satisfies Equations (7), then, for each i:

$$\sum_{j=1}^{M} \alpha_i^* \beta_j^* c_{ij} = |\alpha_i|^2 \sum_{j=1}^{M} |\beta_j|^2 \tag{8}$$

and so:

$$\sum_{i=1}^{N} \sum_{j=1}^{M} \alpha_i^* \beta_j^* c_{ij} = \sum_{i=1}^{N} |\alpha_i|^2 \sum_{j=1}^{M} |\beta_j|^2 = \|\chi\|^2 \tag{9}$$

The quantity on the left-hand side of Equation (9) is equal to (χ, ψ); therefore, for any product state χ that minimizes the distance to ψ among product states:

$$(\chi, \psi) = (\psi, \chi) = \|\chi\|^2 \tag{10}$$

Hence:

$$\|\psi - \chi\|^2 = \|\psi\|^2 + \|\chi\|^2 - (\psi, \chi) - (\chi, \psi) = \|\psi\|^2 - \|\chi\|^2 \tag{11}$$

Thus, if we know only the value of $\|\chi\|$ for some χ satisfying Equations (7), we know also the value of $\|\psi - \chi\|$.

Multiplying the first of Equations (7) by $\Sigma|\alpha_k|^2$ yields:

$$\sum_{j=1}^{M} \beta_j^* (\sum_{k=1}^{N} |\alpha_k|^2) c_{ij} - \alpha_i \|\chi\|^2 = 0 \tag{12}$$

But, from the second of Equations (7):

$$\beta_j^* \sum_{k=1}^{N} |\alpha_k|^2 = \sum_{k=1}^{N} \alpha_k c_{kj}^* \tag{13}$$

Substituting this value in Equation (12) yields:

$$\sum_{j=1}^{M} \sum_{k=1}^{N} \alpha_k c_{kj}^* c_{ij} = \|\chi\|^2 \alpha_i \tag{14}$$

Or, reversing the order of summation:

$$\sum_{k=1}^{N} (\sum_{j=1}^{M} c_{kj}^* c_{ij}) \alpha_k = \|\chi\|^2 \alpha_i \tag{15}$$

Define the $N \times N$ matrix A by[2]:

$$A_{ik} = \sum_{j=1}^{M} c_{kj}^* c_{ij} \tag{16}$$

Then (15) becomes:

$$\sum_{k=1}^{N} A_{ik} \alpha_k = \|\chi\|^2 \alpha_i \tag{17}$$

Thus, if χ is a product state for which $\|\psi - \chi\|$ is a local minimum in the set of product states, the vector $(\alpha_1, \ldots, \alpha_N)$ is an eigenvector of the Hermitian matrix A, with eigenvalue $\|\chi\|^2$. Conversely, if $(\alpha_1, \ldots, \alpha_N)$ is an eigenvector of A and $(\beta_1, \ldots, \beta_M)$ is defined by:

$$\beta_j = \frac{\sum_{i=1}^{N} \alpha_i^* c_{ij}}{\sum_{i=1}^{N} |\alpha_i|^2} \tag{18}$$

then the sequences $\{\alpha_i\}$ and $\{\beta_j\}$ satisfy Equations (7). Thus, the problem of finding the value of $\|\chi\|$ where χ minimizes the distance to ψ among product states, reduces to the problem of finding the maximum of the set of eigenvalues of A.

Setting the determinant of $A - \lambda I$ equal to zero yields a polynomial (the characteristic polynomial of A) in λ of degree N whose roots $\{\lambda_1, \ldots, \lambda_N\}$ are the eigenvalues of A. The coefficients of the characteristic polynomial of A are computable functions of the c_{ij}'s. The roots of this polynomial can be computed using well-known approximation techniques. Therefore, the eigenvalues of A can be effectively computed as a function of ψ. Moreover, the maximum of these eigenvalues, λ_{MAX}, can be computed effectively as a function of $\{\lambda_1, \ldots, \lambda_N\}$: to compute λ_{MAX} within a tolerance of 2^{-n}, compute rational approximations to each of $\{\lambda_1, \ldots, \lambda_N\}$ within a tolerance of 2^{-n}, and take the largest of these rational approximations (comparison of rationals, unlike comparison of reals, can be performed effectively). The square-root function is a computable function on $[0, \infty)$. Therefore:

$$\delta(\psi) = \sqrt{(\|\psi\|^2 - \lambda_{MAX})}$$

is a computable function of ψ.

This completes the proof of the Main Result for the finite case.

A program computing a function of a vector ψ in an infinite-dimensional Hilbert space:

$$\psi = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} c_{ij} u_i \otimes v_j$$

works with finite-dimensional approximations to ψ of the form:

$$\psi' = \sum_{i=1}^{N} \sum_{j=1}^{M} c'_{ij} u_i \otimes v_j$$

where the c'_{ij}'s are rational complex numbers. The reduction of the infinite-dimensional case to the finite-dimensional proceeds as follows. First, it is shown that, if ψ' lies in the finite dimensional subspace spanned by $\{u_i \otimes v_j | i = 1, \ldots, N; j = 1, \ldots, M\}$, then the closest product state to ψ' lies in the same subspace. Thus the procedure outlined above, for the finite-dimensional case, suffices for the computation of $\delta(\psi')$. Next it is shown that $\delta(\psi')$ uniformly approximates $\delta(\psi)$ when ψ' approximates ψ, and hence that $\delta(\psi)$ can be computed with arbitrary precision by computing $\delta(\psi')$ for ψ' sufficiently close to ψ.

Theorem 3.8. Let Γ be the finite-dimensional subspace spanned by $\{u_i \otimes v_j | i = 1, \ldots, N; j = 1, \ldots, M\}$. For any $\psi' \in \Gamma$, if χ is a product state such that $\|\psi' - \chi\| = \delta(\psi')$, then $\chi \in \Gamma$.

Proof. Let P and $P^{\perp}$, be the projection operators onto Γ and $\Gamma^{\perp}$ respectively. Then, for any product state χ and any $\psi' \in \Gamma$:

$$\|\psi' - \chi\|^2 = \|\psi' - P\chi\|^2 + \|P^{\perp}\chi\|^2 \tag{19}$$

Since χ is a product state so is $P\chi$. Moreover, if $\|P^{\perp}\chi\|$ is non-zero, $\|\psi' - P\chi\| < \|\psi' - \chi\|$. Therefore, for any product state not lying entirely in Γ there is another product state in Γ that is closer to ψ'.◀

Theorem 3.9 (Uniform Continuity of δ). For any $\psi, \psi' \in \mathscr{H}_1 \otimes \mathscr{H}_2$:

$$|\delta(\psi) - \delta(\psi')| \leq \|\psi - \psi'\| \tag{20}$$

Proof. For all $\chi \in \mathscr{F}$:

$$\delta(\psi) \leq \|\psi - \chi\| \leq \|\psi - \psi'\| + \|\psi' - \chi\| \tag{21}$$

Therefore:

$$\delta(\psi) - \|\psi - \psi'\| \leq \|\psi' - \chi\| \tag{22}$$

for all $\chi \in \mathscr{F}$. $\delta(\psi') - \|\psi - \psi'\|$ is, therefore, a lower bound of the set $\{\|\psi' - \chi\| | \chi \in \mathscr{F}\}$. Since $\delta(\psi')$ is the *greatest* lower bound of this set:

$$\delta(\psi') \geq \delta(\psi) - \|\psi - \psi'\| \tag{23}$$

The same argument with the roles of ψ and ψ' reversed yields:

$$\delta(\psi) \geq \delta(\psi') - \|\psi' - \psi\| \tag{24}$$

Combining the two gives:

$$\delta(\psi) - \|\psi - \psi'\| \leq \delta(\psi') \leq \delta(\psi) + \|\psi - \psi'\| \tag{25}$$

or:

$$|\delta(\psi) - \delta(\psi')| \leq \|\psi - \psi'\| \tag{26}$$

Q.E.D.◀

To compute $\delta(\psi)$ within an accuracy of 2^{-n}, request a finite rational approximation ψ' such that $\|\psi - \psi'\| < 2^{-(n+1)}$. Then compute a rational approximation Q to $\delta(\psi')$, such that $|Q - \delta(\psi')| < 2^{-(n+1)}$. Then:

$$|\delta(\psi) - Q| \leq |\delta(\psi) - \delta(\psi')| + |Q - \delta(\psi')| \leq \|\psi - \psi'\| + |Q - \delta(\psi')| < 2^{-n} \tag{27}$$

This completes the proof that δ is a computable function, whether $\mathcal{H}_{12}$ is finite- or or infinite-dimensional, hence that $C(\psi, \varepsilon)$ is a computable partial function.

Note that the computation of $\delta(\psi)$ does not require the computation of a closest product state χ, only its norm $\|\chi\|$. We may, therefore, ask in closing whether the task of finding a product state χ that minimizes $\|\psi - \chi\|$ can be performed effectively. That is, is there a computable function $\Delta: \mathcal{H}_{12} \rightarrow \mathscr{F}$ such that $\|\psi - \Delta(\psi)\| = \delta(\psi)$ for all $\psi \in \mathcal{H}_{12}$? The answer is no.

Consider the family of states:

$$\psi_t = \sqrt{(1-t)}u_1 \otimes v_1 + \sqrt{t}\, u_2 \otimes v_2, \quad 0 \le t \le 1$$

If $0 \le t < \frac{1}{2}$, the nearest product state to ψ_t is $\sqrt{(1-t)}u_1 \otimes v_1$, and if $\frac{1}{2} < t \le 1$, the nearest product state is $\sqrt{t}\, u_2 \otimes v_2$. For $t = \frac{1}{2}$, any product state of the form:

$$\frac{1}{\sqrt{2}}(\cos\theta\, u_1 + e^{i\phi}\sin\theta\, u_2) \otimes (\cos\theta\, v_1 + e^{-i\phi}\sin\theta\, v_2)$$

suffices to minimize the distance to ψ. Clearly, Δ cannot depend continuously on ψ, and so cannot be a computable function.

To sum up, the question: "Is there a product state within ε of ψ?" is almost decidable – there is an algorithmic procedure that answers correctly in all but the borderline cases, and for these cases fails to terminate. As we have seen (Theorem 2.1b), this is as good as can be expected for any but the most trivial of decision-problems in a connected space. The function $\delta(\psi)$, which gives the minimum distance from ψ to a product state, is a computable function of its argument, even though there is no effective procedure that always produces a product state that achieves this minimum.

6 Brook Street
Sherborn, MA 01770

NOTE

[1] Some authors define the inner product as the complex conjugate of the function here defined. The convention adopted here is typical of mathematical physicists (e.g. Reed and Simon, 1972); mathematicians usually adopt the opposite convention (e.g. Friedman, 1970).

[2] Readers familiar with the standard proofs of the Schmidt Biorthogonal Decomposition Theorem (von Neumann 1955, pp. 431–437) will recognize this matrix. There is a close relationship between the Schmidt Theorem and the problem of finding the closest product state; the terms of the biorthogonal decomposition of ψ are the relative minima of $\|\psi - \chi\|$. The closest product state to ψ, *is therefore, the largest term in the biorthogonal decomposition of* ψ

REFERENCES

Earman, John (1986), *A Primer on Determinism*, Dordrecht, D. Reidel.
Friedman, Avner (1970), *Foundations of Modern Analysis*, New York, Dover Publications.
Grzegorczyk, A. (1955), "Computable Functionals," *Fundamenta Mathematicae*, **42**, 168–202.
Grzegorczyk, A. (1957), "On the Definitions of Computable Real Continuous Functions," *Fundamenta Mathematicae* **44**, 61–71.
Penrose, Roger (1989), *The Emperor's New Mind*, New York, Oxford University Press.
Reed, Michael and Barry Simon (1972), *Methods of Mathematical Physics. I. Functional Analysis*, New York, Academic Press.
Rogers, Hartley, Jr. (1967), *Theory of Recursive Functions and Effective Computability* (reprint), Cambridge, MA, The MIT Press, 1987.
von Neumann, John (1955), *Mathematical Foundations of Quantum Mechanics*, Princeton, Princeton University Press.