Recognizing how some states are built, from mixed states to singlets.

Charles Tresser
IBM, P.O. Box 218, Yorktown Heights, NY 10598, U.S.A.

Enrique Pujals
IMPA, Estrada Dona Castorina 110, 22460-320, Rio de Janeiro, Rio de Janeiro, Brazil

(Dated: June 16, 2014)

It is well known that different preparations of a mixed state cannot be distinguished by a measurement of that state. Yet we show that some other experiments let us make this distinction despite a very general belief that this would not be possible. Issues in quantum cryptography that prompted this work are only briefly mentioned in this letter.

Pacs: 03.65.-w, 03.67.-a, 03.67.Dd, 03.67.Mn.

We known that “different preparations of a mixed state cannot be discriminated by any measurement of that state”. We recall below a basic theorem to the effect that “no measurement on the mixed state would let one make this distinction”, and its proof. Yet we also provide experimental means (idealized as usual) to perform such discrimination when considering the test case of even mixtures of photons that are linearly polarized along one of two orthogonal directions. The experiments that we propose let one make this distinction against the broadly shared belief that this distinction is impossible (see, e.g., [1] and references therein for that and related EPR pairs considerations). This belief is based on the theorem below and on principles such as “any prediction in quantum mechanics can only concern measurements and the corresponding eigenvalues.” Instead of measuring the state like in that theorem, we consider how the polarized states interact with our specially designed interferometers, where each photon gets detected by one of the detectors or by none of them. One can be lead to believe that “being able to recognize how a mixed state was built would permit superluminal signaling”. But this is based on some old confusions. Consider an entangle-
ment, say of a pair \(\gamma,\gamma\). The half \(\gamma\) being measured by Bob behaves as if \(\gamma'\) had been similarly measured by Alice, for space-like separated measurements. But the measurements on the \(\gamma\)'s are indeed unaffected by those on the \(\gamma'\)'s and by whether these remote measurements are made at all. We prove specific results in some cases here (see \((7)\) and the treatment of \(|\Upsilon\rangle\) below) and more details will be part of the full version of the present paper. The one photon at a time context makes the analysis simpler (for all intensities of fluxes of photons in fact) and allows one to compare between mixtures and half of EPR pairs as needed for application to some questions in quantum cryptography that we only briefly mention here: see for instance [2] since the cryptographic applications presented here do not yet go beyond defending against the EPR attack defined in that paper. In the present paper we mostly discuss mixtures. These are conjunctions of pure states [3] (rather than sums of pure states which are again pure states). More precisely we will consider some mixtures of states of linear polarization of photons all of the same wavelength. In the context of mixtures, a pure state is a mixture made of 100% of one of the kinds that could be used. In particular, we consider mostly the polarization observable [4], a direction that is orthogonal to the propagation direction of the light (be it an intense beam, photons produced one at a time, or halves of entangled pairs) and we ignore most of the other aspects of said light; to fix the ideas, we restrict ourselves to the optical wavelengths range and propose experimental settings adapted to that range. Our mixed states are constituted by successive photons being prepared by Alice, part or all being sent to Bob. Anyway, by using the tools proposed here Bob will find out what are the orthogonal pure states being mixed at 50%–50% by Alice, or find out that he is being sent another state, hard to distinguish from a mixture (typically an EPR state: see, e.g., [1], [2] and references therein).

One of the difficulties with polarizations is that they are represented by directors, i.e., representatives of directions (in any dimension \(d\), equivalence classes of straight lines under the parallelism equivalence) that live in the projective space \(\mathbb{P}^{d-1}\). Since vectors are handy for computations we start with an elementary discussion of the way to represent linear polarizations and how to compute with that. In what follows, if the roman letter \(w\) represents some axis (i.e., a straight line equipped with an orientation, so that the abscissa along \(w\) augments when moving along \(w\) in the positive direction), then \(w\) stands for the positive unit vector along \(w\). Thus \(-w\) is the axis corresponding to the unit vector \(-w\). We will consider mixtures of pure polarization states along pairs of directions that are orthogonal to each other. We denote by \(W\) the direction defined by any of the sets \(\{w, -w\}\) and \(\{w, -w\}\), while any of the elements \(w\), \(w\) and the pair \((w, -w)\) (respectively \(-w\), \(-w\) and \((-w, w)\)) defines the axis, or oriented direction \(w\) (respectively the axis \(-w\)). The polarization state along the direction \(W\) can be denoted by \(|W\rangle\), but it is convenient to designate it also by \(|w\rangle\) which is fine as long as one sticks to
the convention that $|w⟩ = |−w⟩$ since polarizations are determined by directions and not by oriented directions (i.e., we exploit in these notations for polarization states that both opposite oriented directions specify the same direction, hence the same polarization state). Of course, $−|w_1⟩ + |w_2⟩ = |w_1⟩ − |w_2⟩ = |w_1⟩ + |w_2⟩$. We will consider several states built out of the pure polarization states $|X⟩$, $|Z⟩$, $|U⟩$, and $|V⟩$ along the directions $X$, $Z$, $U$, and $V$ where $u = \frac{1}{\sqrt{2}}(x + z)$ and $v = \frac{1}{\sqrt{2}}(z − x)$. We also assume that $x · z = 0$ so that $u · v = 0$ as well: thus $(|X⟩, |Z⟩)$ and $(|U⟩, |V⟩)$ form together a pair of Wiesner bases. More precisely we will focus on: a) The perfectly (i.e., 50% − 50%) mixed states (see the introduction of the density matrices that represent such states), $Φ = \frac{1}{2}(|x⟩⟨x| + |z⟩⟨z|)$ and $Ψ = \frac{1}{2}(|u⟩⟨u| + |v⟩⟨v|)$. $Φ$ (respectively $Ψ$) can be thought of as prepared as the mixture of the two polarizations (basis vectors) of the Wiesner base $B_0 ≡ \{x, z\}$ (respectively the Wiesner base $B_1 ≡ \{u, v\}$). Here we notice that since $z = 1/\sqrt{2}(u + v)$ and $x = 1/\sqrt{2}(u − v)$, there is a $(x, z, u, v) → (v, u, z, x)$ symmetry of the configurations that we consider. b) The photons $γ$ going along $y$ out of the pair $(γ, Γ)$ in the singlet (or EPR) state $Υ = \frac{1}{\sqrt{2}}(|+⟩⟨−| + −⟩⟨+|)$ (all singlet states will be polarization singlet states here). Our main goals are to discriminate $Φ$ and $Ψ$ from each other and then to differentiate any of these states from two half of the state $Υ$ (that is a common purification of $Φ$ and $Ψ$). With $Φ$ and $Ψ$ recognizable (as we shall show they are), it is easy to see, using the rotational invariance of $Υ$, that: $(Φ)$ behaves as $Φ$ (respectively $Ψ$) if analyzed with one of the special interferometers introduced below to give no output to the vectors of $B_0$ but some to the vectors of $B_1$ (respectively of $B_1$ but some to the vectors of $B_0$). Indeed, this would clearly be the case for the $γ_j$’s if the $Γ_j$’s where measured in said bases, but if these measurements would matter on the sequence of $γ_j$’s, then one would readily generate superluminal signaling: see also, e.g., [3]. We recall that in the basis $(|x⟩, |z⟩)$, where $|x⟩ = (1, 0)$ and $|z⟩ = (0, 1)$, with $a^t$ for the transpose of $a$, we have

$$|x⟩⟨x| = (1, 0)(1, 0) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

and $|z⟩⟨z| = (0, 1)(0, 1) = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$,

so that in that basis

$$Φ = \frac{1}{2}(|x⟩⟨x| + |z⟩⟨z|) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}Id,$$

using $Id$ for the identity matrix. Beside, we also have:

$$|u⟩⟨u| = \frac{1}{2}(|1⟩⟨1| + |−1⟩⟨−1|) = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix},$$

and $|v⟩⟨v| = (−1)⟨−1⟩⟨−1⟩ = \frac{1}{2} \begin{pmatrix} 1 & −1 \\ −1 & 1 \end{pmatrix}$,

so that in the same basis

$$Ψ = \frac{1}{2}(|u⟩⟨u| + |v⟩⟨v|) = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}Id.$$

The identity matrix is independent of the choice of basis, but more generally one would be identifying mixed states whose matrices represent the same linear operator. A general mixed state can be represented as a sequence $(p_i, |ϕ_i⟩)$ where each $p_i$ is a probability and the $ϕ_i$ are states of the pure states participating to the mixture while the first element is the probability (or proportion) of the corresponding state, and $K$ is the index set used to label the states that participate to the mixture and the corresponding probabilities. Here is a simple classical result:

**Theorem.** If the mixed state $ρ = \{p_i, |ϕ_i⟩\}_{i ∈ K}$ is measured in an orthonormal basis $\{ψ_j⟩\}_j$, then the outcome is $ψ_k⟩$ with probability $\text{Prob}(⟨ψ_k| ρ|ψ_k⟩)$ by $⟨ψ_k| ρ|ψ_k⟩$. It follows that if we measure the mixed state $ρ = \{p_i, |ϕ_i⟩\}_{i ∈ K}$ in the standard basis, we have for the basis element with index $k$ in $K$, $\text{Prob}(⟨k| ρ|k⟩) = p_k$. The corresponding diagonal entry of the density matrix $ρ$. This graphical representation shows the interferometers and the mirrors used in the experiment to discriminate $Φ$ and $Ψ$.
The proof consists of the following chain of equalities:  
\[ \text{Prob}(k) = \sum_{j} p_j |\langle \psi_j | \psi_k \rangle|^2 = \sum_{j} p_j \langle \psi_k | \psi_j \rangle \langle \psi_j | \psi_k \rangle = \langle \psi_k | \sum_{j} p_j |\psi_j \rangle \langle \psi_j | \psi_k \rangle = \langle \psi_k | \rho |\psi_k \rangle = \rho_{k,k}. \]
Q.E.D.

We now describe a collection of tools that can be seen as a cascade of Mach-Zehnder interferometers (or CMZIs): (also called here analyzers) cf. parts a) and b) of Figure 1. Our CMZIs carry polarizers (or filters) that have polarization in the set \{P, Q, F, G\} as indicated in parts a) and b) of Figure 1 while the pair \( \{P, Q\} \) is one of the (four) pairs of the quadruplets \( Q = \{(U, V), (V, U), (X, Z), (Z, X)\} \), the set \( \{F, G\} \) is one of the elements of the doubleton of doubletons \( \mathcal{D} = \{(U, V), (X, Z)\} \). Depending of the choices for \( \{P, Q, F, G\} \) one thus find eight Cases, each parameterized by a pair of polarizations out of \( Q \) and a doubleton of polarizations out of \( \mathcal{D} \). The two CMZIs corresponding to the replacement \( \{P, Q\} \leftrightarrow \{F, G\} \) are equivalent for our purpose. To the contrary, \( \{P, Q\} \) and \( \{Q, P\} \) correspond to two distinct CMZIs for any choice of \( \{P, Q\} \) in the quadruplet \( Q \). In parts a) and b) of Figure 1:
- Any object whose name starts \( BS \) is a beam splitter.
- Any object whose name starts \( M \) is a mirror.
- Any object whose name start with \( \phi \) is a phase shifter: these are tuned so that the times for the light to go between two beam splitters that are consecutive on a pair of parts of the optical paths are identical: we assume that all the phase shifters have been set to fulfill this goal so that the interferences if any are maximized and more generally any phenomenon is as sharp as possible. The only difference between the \( T+S \) and \( T-S \) settings is that in Case 1 we will let us perform the discrimination that we seek between \( |\Phi\rangle \) and \( |\Psi\rangle \). In fact, one of the settings provides a quantitative discrimination between \( |\Phi\rangle \) and \( |\Psi\rangle \) while one further permits a qualitative differentiation. This can be used to distinguish any of \( \Phi \) and \( \Psi \), not only each one from the other, but also any one of them from a half of \( \mathcal{Y} \) by using \( Q \).

Our Case 1 CMZI is specified as \( \{(P, Q), \{F, G\}\} = \{(U, V), \{U, V\}\} \), and we first consider two out of a set of four settings: The \( Top+ Side \) (read “Top Plus Minus Side”) setting (see Figure 1a) obtained by: - Adding (at \( BSF+ \) in Figure 1a) the feeds to detector \( DF \) from Top and Side, and - Subtracting (at \( BSF- \) in Figure 1a) the Side feed to detector \( DG \) from the Top feed to detector \( DG \). And the \( Top+ Side \) setting (see Figure 1b) obtained by: - Adding (at \( BSF+ \) in Figure 1b) the feeds to detector \( DG \) from Top and Side and - Subtracting (at \( BSF- \) in Figure 1b) the Side feed to detector \( DF \) from the Top feed to detector \( DF \). A standard computation yields the following results:
- \( \alpha \) : For the \( Top+ Side \) analyzer \( U \) and \( V \) have outputs, respectively from the \( U \) and \( V \) last filters, four time more probable than the corresponding outputs respectively from the \( X \) and \( Z \) inputs.
- \( \beta \) : For the \( Top- Side \) analyzer, \( U \) and \( V \) inputs give no output while \( X \) generates a positive probability \( V \) output, and \( Z \) generates a positive probability \( U \) output (see equations (**) below to perform the calculations). Thus \( |\Phi\rangle \) and \( |\Psi\rangle \) can be distinguished from each other, quantitatively by using \( \alpha \), qualitatively by using \( \beta \). The two other settings (see below) have no observable \( |\Phi\rangle\) or \( |\Psi\rangle \) difference.

We now describe the eight \( Cases \) that correspond to all choices of \( \{(P, Q), \{F, G\}\} \) with \( \{P, Q\} \) in \( Q \) and \( \{F, G\} \) in \( \mathcal{D} \) (see Figure 1d), and for each case the associated four CMZI settings. The light is emitted at the source \( \sigma \) and gets initial polarization \( I \) either in \( \{X, Z\} \) or in \( \{U, V\} \) (dependent on Alice’s choice) before reaching Bob and more precisely the first beam splitter \( BSin \). We use an adapted setting of any CMZI to investigate which Wiesner basis was used by Alice and two CMZIs with those settings to verify if she used an EPR state instead of one of the mixed states. All beam splitters and following polarizers can be rearranged using polarizing beam splitters in order to avoid the loss of some photons but the presentation is done here with beam splitters to improve the visibility of the paths in parts a) and b) of Figure 1.

For each of the eight Cases, one at least of the four settings (of a type like illustrated just above by \( \alpha \) and \( \beta \) in Case 1) will let us perform the discrimination that we seek between \( |\Phi\rangle \) and \( |\Psi\rangle \).
We use mirrors as simple mirrors or as elements of beam splitters; they act on phase shifts as represented in Figure 1-c, where the long borders of the black halves of the mirrors reflect the incident light and the grey part represent some dielectric where photons travel slower than in air. Thus, only BSOut and BSG—induce large phase shifts, both equal to $e^{i\pi}$ when the light reflects on the mirror on the dielectric side. No other reflection or passing through a half silvered mirror induces any phase shift (since we deal with the dielectric crossing by tuning the phase shifters as previously mentioned).

The amplitudes $A_{a,b,\pm}(I,L)$ for paths $Path_{a,b,\pm}(I,L)$ for $(a,b)$ in $\{s,t\}$ (grouped by pairs $(I,L)$) are as follows, up to a positive factor (for ease of use, $L_s$ is attached to the side paths, $L_t$ to the top paths, but polarization-wise, $L_s \equiv L \equiv L_t$): $A_{s,s,\pm}(I,L) = e^{i\alpha} \cdot \langle L_s | P \rangle \cdot \langle P | I \rangle$, $A_{t,t,\pm}(I,L) = \langle L_t | P \rangle \cdot \langle P | I \rangle$, $A_{s,t,\pm}(I,L) = \langle L_s | Q \rangle \cdot \langle Q | I \rangle$, $A_{t,s,\pm}(I,L) = \langle L_t | Q \rangle \cdot \langle Q | I \rangle$.

As a consequence of these amplitudes (up to a strictly positive factor), for an input with polarization $I$ we collect for instance (see Figure 1-c): $(\gamma)\langle L_t | P \rangle \cdot \langle P | I \rangle + \langle L_t | Q \rangle \cdot \langle Q | I \rangle - (e^{i\pi} \langle L_s | P \rangle \cdot \langle P | I \rangle + \langle L_s | Q \rangle \cdot \langle Q | I \rangle)$ at detectors DL using the Top $+\:$ Side setting if $L = F$ and the Top $+\:$ Side setting if $L = G$, and $(\gamma)(\langle L_t | P \rangle \cdot \langle P | I \rangle + \langle L_t | Q \rangle \cdot \langle Q | I \rangle + e^{i\pi} \langle L_s | P \rangle \cdot \langle P | I \rangle + \langle L_s | Q \rangle \cdot \langle Q | I \rangle)$ at detectors DL using the Top $+\:$ Side setting if $L = F$ and the Top $+\:$ Side setting if $L = G$.

We also recall that $|A|^2$ is a probability of occurrence for a photon and that we have left out some strictly positive factors that would not show up much in experiments. As we saw for Case 1, the eight Cases $(P,Q), (G,F), (E,M)$ each let us distinguish qualitatively the outputs generated by photons with polarizations $I$’s in $\{X,Z\}$ from the outputs generated by photons with polarizations $I$’s in $\{U,V\}$, for one of: - A) The Top $+\:$ Side setting for which the Top and Side $F$ amplitudes are added while the Side $G$’s amplitude is subtracted from the Top $G$’s, and - B) The Top $+\:$ Side setting for which the Top and Side $G$’s amplitudes are added while the Side $F$ amplitude is subtracted from the Top $F$’s. The Top $+\:$ Side and Top $+\:$ Side inhomogeneous settings are somewhat mixtures of the homogeneous settings Top $-\:$ Side and Top $+\:$ Side CMZIs, and vice-versa: despite differences at the microscopic level, the homogeneous settings do not let us distinguish $\langle \Phi | \rangle$ and $\langle \Psi |$ from each other, but as for $\alpha$ and $\beta$ in Case 1 the inhomogeneous settings are efficient discriminators in the eight Cases: for each of them in one setting neither $I = P$ nor $I = Q$ yield outputs. Furthermore, with an efficient pair of analyzers (a pair made of one CMZI with Case $\leq 4$ and one with Case $\geq 5$) beside distinguishing the states $\langle \Phi |$ and $\langle \Psi |$ from each other, one can also distinguish them from the EPR state $\langle \Upsilon |$ using $(\gamma)$. This lets one foil the EPR attack against head and tail over the phone as described in [2]. The precise succession of two Wiesner bases cannot be recognized by Bob if the base can change at each step but then Bob still recognizes the Wiesner base $B_t$ whenever he sees an output that is impossible for $B_{1-t}$, but it is not our goal to focus on the cryptographic advantages of the results of this paper. Since one expects that for first order interferences, any particle interferes with itself and with itself only, the settings proposed here to pairwise distinguish states $\langle \Phi |$ and $\langle \Psi |$ and half of $\langle \Upsilon |$ one particle at a time will let us distinguish these states for any type of photons flux compatible with equidistribution of the polarizations along the directions of any pair of orthonormed basis. As a consequence, it will be easy to see, even by mixing at 50% the properly polarized outputs form equal fluxes lasers, that despite the above classical theorem, some methods permit to identify which of the mix has been used for the generation of (at least) some density matrices.

With $y \pm e \cdot z$ standing for the momentum directions of the photons in a 50%-50% momentum mixture, one gets no interference with a double slit on a screen $S$ if $x$ is the slits direction. This imitates what we get with momentum singlet state photons. However, by progressively rotating either the preparation axis from $y \pm e z$ to $y \pm e x$ or equivalently the axis of the slits, one gets a progressive reappearance of the interferences with full visibility at angle $\frac{\pi}{2}$ with the mixture while the singlet always presents no interference. The problem, but also the solution, is that the components of the mixture separate. After the de-mix, it is easy to see what were the directions being mixed. A question then comes to mind: can one de-mix also when what is mixed are polarization states (or spins for spin $-\frac{1}{2}$ particles)?

We have described here a collection of CMZIs that lets one just do that. More precisely, out of the polarizations $(X,Z)$ and $(U,V)$, our MZCIs kill flux of the two elements of one Wiesner Base $M_t$ and produces some measurable output out of the polarizations in $M_{1-t}$. We hope that the momenta example will make the polarizations example more transparent.

Acknowledgments: Thanks from C.T. to David Mermin and Michel Le Bellac, from both authors to Hava Spiegelmann and Marc Martens. Thanks also to CNPq (grant # 10214146209159329) for its support of E.P..

--

*charlestresser@yahoo.com enrique@impa.br

[1] N.D. Mermin, Fundations of Physics, 29, 571, (1999).
[2] C.H. Bennett, G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore (IEEE Computer Society, New York, 1984), pp. 175-179.
[3] J. von Neumann, Göttingen Nachrichten 1, 245, (1927).
[4] M. Born, E. Wolf. Principles of Optics (Electromagnetic theory of propagation, interference and defraction of light), VIIth (Expanded) Edition (Cambridge University Press; Cambridge, 1999).
[5] S. Wiesner, Conjugate Coding, manuscript ca. 1970 (SIGACT News, 15:1 1983), p. 78.
[6] A. Zeilinger, Rev. Mod. Phys. 71, S288 (1999)