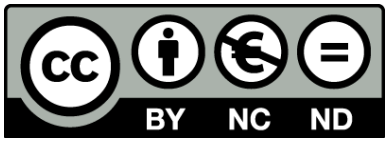
UNIVERSITAT DE BARCELONA

Quantum entanglement and quantum state estimation

Entrelazado cuántico y estimación de estados cuánticos

Antonio Acín dal Maschio



Entrelazado cuántico y estimación de estados cuánticos

Quantum entanglement and quantum state estimation

Antonio Acín Dal Maschio

Departament d'Estructura i Constituents de la Matèria

Universitat de Barcelona

Junio 2001

Entrelazado cuántico y estimación de estados cuánticos

Quantum entanglement and quantum state estimation

Memoria de la tesis presentada por Antonio Acín Dal Maschio
para optar al título de Doctor en Física.

Director de tesis: Dr. José Ignacio Latorre.

Programa de doctorado (bienio 1997-1999)
Partículas, campos y fenómenos cuánticos colectivos,
del Departament d'Estructura i Constituents de la Matèria,
Universitat de Barcelona.

Barcelona, junio de 2001.

A Natalia.

Agradecimientos

Creo que todo doctorando, o al menos a mí siempre me pasaba, que tiene la oportunidad de leer la tesis de un compañero mientras él está realizando la suya, no puede evitar pensar en sí mismo escribiendo la sección de agradecimientos en un futuro que espera no sea demasiado lejano. Pues bien, al fin ha llegado el ansiado momento.

En primer lugar agradezco a José Ignacio Latorre el haberme dirigido la tesis doctoral. No me conocía demasiado, cosa normal dada la alergia durante mi etapa de estudiante a pasar por los departamentos, pero pensó que podíamos sacar adelante un trabajo de investigación en un campo, relativamente nuevo también para él, como la Información Cuántica. Durante estos años creo que hemos mantenido siempre una buena relación tanto profesional como personal, y es suyo gran parte del mérito de que guarde un buen recuerdo de todo lo que ha significado y me ha aportado la realización de la tesis.

También me gustaría mostrar mi gratitud hacia Rolf Tarrach y Pedro Pascual, con los cuales he tenido la fortuna de trabajar en varias ocasiones y que siempre me han ayudado. Y ya metidos en el departamento, quisiera aprovechar para agradecer al resto de profesores y personal su amabilidad conmigo durante los tres años que he pasado en él. Sin olvidar, como es evidente, el apoyo económico que se me ha dado y que me ha permitido asistir a diversos congresos y centros en el extranjero.

Agradezco a Maciek Lewenstein y Anna Sanpera la invitación al *Institute für Theoretische Physik* en Hannover, donde aprendí muchísimo y lo pasé muy bien, sobre todo teniendo en cuenta la nostalgia que me entra cada vez que salgo de Barcelona. Claro que parte de la "culpa" es de Dagmar, Luis, Philip, Lukasz y el resto del grupo. De igual modo, me gustaría dar las gracias a Ignacio Cirac por la estancia en Innsbruck, y a toda la gente que la hizo muy agradable, Guifré, Wolfgang, Geza, Lluís, Belén,... Y también agradezco a Nicolas Gisin la oportunidad que me dio de conocer su grupo y la ciudad de Ginebra, que me van a resultar muy familiares a partir del verano.

La transición de los agradecimientos "profesionales" a otros más "per-

sonales", por llamarlos de algún modo, se hace más suave gracias a Guifré y Enric. Ha sido un placer trabajar con vosotros durante estos años. De Guifré he aprendido muchas cosas, y en particular a perder parte, que no todo, del respeto a las matemáticas y entender cómo pueden convertirse en una herramienta muy útil. Y en cuanto a Enric, creo que una de las mejores experiencias durante la tesis ha sido el poder colaborar con él: hemos trabajado de manera muy cómoda juntos, y espero que podamos seguir haciéndolo en adelante. Además nos lo hemos pasado muy bien y quedan muchas anécdotas: el dichoso viaje a Argentina, la semana fantástica, las tertulias por correo electrónico,...

Mi relación con el resto de los doctorandos del departamento y la facultad creo que también ha sido buena. Agradezco a todos los compañeros de despacho que he tenido, y en particular a Toni, Dolors, Ignasi, Dani y Julián la paciencia que han demostrado al aguantarme. Lo he pasado muy bien en los partidos de fútbol con Joan, Guifré, David Mateos, David Gascón, Enric, Toni, Iván, Albert, Adán, Dani, Álex Moreno, Álex Domínguez, Aleix, José y demás. Y por no hablar de las grandes tertulias balompédicas y quinielísticas con Adán, Toni, antes Joan y Enric, y ahora Álex y Dani. En general gracias a todos (Paco, Ernest, los condensados, los fundamentales,...).

Salgamos de la facultad. Agradezco a toda mi familia el apoyo durante estos años, en particular a mis padres y mis hermanos. Sé que a veces no es fácil entender los motivos que le llevan a uno a hacer una tesis, pero creo que han acabado por hacerse a la idea. También estoy francamente agradecido a Marina, el Negro y su número mágico π y a Pablito.

Quiero dar las gracias a todos los amigos que me han ayudado a desintoxicar en los ratos de ocio de la actividad académica: Óscar, Carmen, Pablo, Gemma, Enrico, Carme, Fabio, Oriol, Mireia, Yunki, Ariel y el resto de la "penya", así como a toda la gente de Broto. La verdad es que me habéis ayudado a pasar grandes ratos fuera del despacho. Y también mis compañeros de tertulia virtual con los cuales me he desahogado en inmaduros e impresentables debates: el pibe, el vecchio signore, Menichetti y Microperls.

Pero si a alguien se merece realmente estar en esta sección de agradecimientos es Natalia. Como ella bien sabe, esta tesis nunca hubiera sido posible sin su ayuda y su apoyo. Ha aguantado con paciencia todos los rollos, depresiones, euforias que he atravesado durante el doctorado, y siempre me ha animado a seguir adelante. Por ello, pocas cosas me han parecido nunca más justificadas que dedicarle la tesis. Gracias, Natalia.

Prefacio

Esta tesis trata diferentes aspectos de Información Cuántica, una nueva rama de la física teórica en la que se trasladan resultados ya establecidos de la Teoría de la Información Clásica al dominio cuántico. Contiene gran parte del trabajo que he realizado durante los últimos tres años en el grupo de Información Cuántica del Departamento de Estructura y Constituyentes de la Materia de la Universidad de Barcelona, y en ocasiones en colaboración con el *Institut für Theoretische Physik* de la Universidad de Hannover y el de la Universidad de Innsbruck.

La tesis está organizada como un compendio de seis artículos: los cuatro primeros son sobre entrelazado de tres bits cuánticos y los otros dos sobre estimación de estados. El primer capítulo es el único escrito en español, proporciona una introducción muy general al campo y resume los principales resultados que han sido obtenidos. Al final hay también una breve sección con conclusiones. Es la mejor elección para los lectores que entiendan el español y no sepan nada de Información Cuántica. En el segundo capítulo hay una introducción más técnica al entrelazado, el ingrediente clave en muchas aplicaciones de información cuántica. El objetivo del tercer y cuarto capítulo es presentar, con bastante más detalle que en el primero, los puntos más importantes tratados en esta tesis: se muestra la motivación y las conclusiones de nuestro trabajo. Finalmente, los seis artículos, donde es posible encontrar las derivaciones explícitas de todos los resultados, se encuentran como apéndices.

Preface

The main subject of this thesis is Quantum Information, a new branch of Theoretical Physics that translates known results of Classical Information Theory into the quantum domain. It contains most of my work during the last three years in the Quantum Information Group of the *Departament d'Estructura i Constituents de la Matèria* of the University of Barcelona, and sometimes in collaboration with the *Institut für Theoretische Physik* of the University of Hannover and of the University of Innsbruck.

The thesis is organized as a compendium of six articles: the first four are about three-qubit entanglement and the other two about state estimation. The first chapter is the only one written in Spanish, it gives a very general introduction to the field and summarizes the main results that have been obtained. At the end there is also a brief section with conclusions. It is the best choice for those readers that understand Spanish and do not know anything about Quantum Information. In the second chapter there is a more technical introduction to entanglement, the key ingredient in many quantum information applications. The aim of the third and fourth chapter is to present, with quite more detail than in chapter one, the main points studied in this thesis: it shows the motivation and the conclusions of our work. Finally, the six articles, where it is possible to find the explicit derivation of all the results, are given as appendices.

Contents

Capítulo 1

Resumen

1.1 Introducción

El objetivo de esta tesis ha sido el estudio de diferentes problemas en Información Cuántica, un campo joven y dinámico en el que se fusionan aspectos de Teoría de la Información y de la Computación con la Mecánica Cuántica. La Teoría de la Información analiza la manera de transmitir datos desde un emisor a un receptor, mientras que la Teoría de la Computación se centra en el modo en que éstos son procesados de cara a realizar una determinada tarea. Aparentemente son dos disciplinas abstractas, en las cuales el estudio es independiente de los dispositivos físicos mediante los que se codifique o transmita la información. Esta premisa se ha revelado sin embargo falsa, y la contribución de los nuevos resultados en Información Cuántica ha sido capital para este cambio de paradigma.

La unidad básica de información es el bit, y su realización física puede darse por medio de cualquier sistema que tome dos valores definidos. Así, el paso o no de corriente eléctrica por un transistor puede servir para representar los dos valores que toma el bit, el "0" o el "1" de la lógica booleana. Con esta simple unidad de información pueden describirse todos los procesos de computación y de transmisión de información que se dan hoy en día. Todo ello se realiza en dispositivos que trabajan a una escala en la cual las leyes de la Física Clásica ofrecen una correcta descripción de los fenómenos naturales. Es sabido, sin embargo, que al pasar a escalas microscópicas, este formulismo deja de ser válido y es la Mecánica Cuántica la que proporciona

una correcta interpretación de los resultados experimentales, por lo que la Física Clásica es una aproximación de la Mecánica Cuántica que funciona bien para escalas macroscópicas. Cabe preguntarse entonces qué pasará si la codificación de la información se lleva a cabo en dispositivos físicos microscópicos cuya descripción debe realizarse en términos cuánticos y ver si ello supone alguna variación en la manera en la que la información puede procesarse. Es importante incidir en el hecho de que si se produjera este cambio, no podemos considerar el bit y el resto de elementos que aparecen en la Teoría de la Información como entes abstractos, tal y como se ha venido haciendo hasta hace poco, sino claramente dependientes del entorno físico en el que se encuentran. De ese modo se haría evidente, y citando a Landauer, que la "información es física".

Hasta ahora toda justificación acerca de la importancia de plantearse si el cambio en las leyes físicas supone una variación del tratamiento de la información ha sido dada desde un planteamiento estrictamente teórico. Pero también desde el punto de vista experimental resulta muy interesante preguntarse por las consecuencias que llevará el cambio desde una descripción clásica a una cuántica. El desarrollo tecnológico de los dispositivos electrónicos está mejorando de manera notable y se están alcanzando resultados espectaculares en la miniaturización de los componentes. De seguir la actual tendencia, se alcanzará la frontera en la que los efectos cuánticos empiezan a manifestarse. Es importante por tanto conocer la influencia que éstos tendrán en los sistemas de información, así como saber si es posible obtener algún tipo de ventaja en caso de que puedan ser controlados.

La Información Cuántica busca dar respuesta a estas preguntas, conocer las variaciones que se derivarán del cambio de la física de los dispositivos, en la transición de la Mecánica Clásica a la Cuántica. Los resultados que hasta ahora se han obtenido en esta disciplina muestran que espectaculares y novedosos procesos de tratamiento de la información pueden darse utilizando las leyes cuánticas. A parte de ofrecer interesantes perspectivas teóricas (también para una mejor comprensión de la Mecánica Cuántica), el interés es básicamente de tipo práctico, de cara a conocer las modificaciones que se podrán obtener si sigue el actual progreso tecnológico. De hecho en el campo de la óptica cuántica ya se han realizado múltiples experimentos desarrolando parte de estos nuevos resultados. Conviene notar que todo el tratamiento previo de la Teoría de la Información Clásica se encuentra recogido en la versión cuántica (es un caso particular), puesto que la

Mecánica Clásica no deja de ser, como se ha mencionado, una aproximación de la Mecánica Cuántica. Al codificar la información en estados cuánticos, dos son los fenómenos que aparecen sin análogo en la Teoría de la Información Clásica: la superposición de estados y las correlaciones cuánticas o entrelazado (en inglés *entanglement*). En el resto de esta sección discutiremos con algo más de detalle estos dos puntos, así como las dificultades que aparecen al intentar leer la información almacenada en un estado cuántico debidas a la no ortogonalidad.

1.1.1 Superposición de estados: el bit cuántico

La Información Cuántica estudia cómo manipular y procesar datos que han sido almacenados en estados cuánticos. De manera similar al bit clásico, un estado cuántico de dos niveles representa la unidad básica de información cuántica, el bit cuántico o *qubit*. Matemáticamente se tiene un vector, $|\psi\rangle$, perteneciente a un espacio vectorial complejo de dimensión dos, $\mathcal{C}^2$. Los dos valores lógicos del bit serán entonces los dos elementos de una base ortonormal en este espacio,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.1}$$

Dado que estamos en un espacio vectorial, podemos encontrar cualquier estado superposición resultante de la combinación lineal de estos elementos, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde α y β son dos números complejos que satisfacen $|\alpha|^2 + |\beta|^2 = 1$. Con ello los posibles valores que puede tomar el bit cuántico son infinitos, al contrario de lo que sucedía para el bit clásico.

Consideremos el caso en que se tiene que realizar una tarea en la que se llama a una función f. Clásicamente los $N = 2^d$ posibles valores de entrada se codifican por medio de d bits, por lo que si queremos saber el valor de la función para todas las entradas es necesario calcularla N veces. Ahora bien, si preparamos un estado cuántico de d qubits, $|\psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \ldots \mathcal{C}^2 = \mathcal{C}^{2^d}$, en el estado superposición de todos los elementos de la base, es decir

$$|\psi\rangle = \frac{1}{2^{d/2}}(|0\ldots00\rangle + |0\ldots01\rangle + \ldots + |1\ldots11\rangle) = \frac{1}{2^{d/2}} \sum_{i=0}^{2^d-1} |i\rangle, \tag{1.2}$$

y aplicamos f sobre este estado, se tiene la información de todos los valores que toma la función distribuida en el estado resultado con una única llamada

a f,

$$|\phi\rangle = \frac{1}{2^{d/2}} \sum_{i=0}^{2^d-1} |f(i)\rangle. \tag{1.3}$$

Por medio de la superposición se tiene un paralelismo cuántico que permite en principio acelerar la realización de diferentes tareas. Sin embargo es importante tener en cuenta que no toda la información en el estado superposición es accesible debido a la no ortogonalidad de los estados cuánticos, por lo que el método a la hora de procesar y leer los datos no es trivial.

1.1.2 El entrelazado cuántico

El entrelazado es un fenómeno que no puede tener análogo en una descripción clásica de un sistema físico y que aparece en sistemas compuestos de diferentes partículas. Para muchos de los estados, puros o mezcla, que describen su preparación, se observan unas correlaciones entre las diferentes partículas o subsistemas que no pueden explicarse por medio de ningún modelo local clásico, es decir son intrínsicamente cuánticas y suelen también llamarse propiedades no locales del estado. Al no tener análogo clásico, es muy importante conocer qué mejoras puede suponer el poder manipular este nuevo tipo de correlaciones, dado que no será posible encontrar ningún método alternativo utilizando dispositivos clásicos capaz de realizar las mismas tareas. De hecho muchas de los nuevos, y en ocasiones espectaculares, resultados en Información Cuántica se basan en el aprovechamiento de estas correlaciones, y en este sentido se suele afirmar que el entrelazado es un recurso de gran utilidad práctica.

El típico esquema en gran parte de las aplicaciones de Información Cuántica consiste en diversos observadores que comparten un estado en el que existen correlaciones cuánticas entre ellos. En general, las diferentes partes no pueden juntar sus subsistemas y realizar operaciones conjuntas, pero sí que pueden manipular de manera arbitraria su subsistema local y comunicarse de un modo clásico. En esta situación estamos interesados en conocer cómo pueden los diferentes observadores modificar las propiedades del estado cuántico en el que se encuentran, y en particular las correlaciones cuánticas entre ellos, por medio de operaciones locales y comunicación clásica.

1.1.3 La no ortogonalidad de los estados

El bit cuántico como hemos visto puede tomar un número infinito de valores, lo que comparado con las dos posibilidades clásicas permite agilizar ditintas tareas por medio del llamado paralelismo cuántico, como en (1.2) y (1.3). Sin embargo es un resultado bien conocido en Mecánica Cuántica que se pueden distinguir con certeza sólo estados que sean ortogonales entre sí. Eso implica que en un sistema de dimensión igual a d, únicamente d estados pueden ser discriminados, o en el caso del bit cuántico sólo dos. Parecería por tanto que se pierden todas las posibilidades que aparecían al codificar datos en bits cuánticos, dado que el paralelismo cuántico queda en la práctica a un nivel en el que no puede ser utilizado. Si bien las consecuencias no son tan dramáticas, es cierto que la no ortogonalidad es un problema de gran importancia en Información Cuántica. Se debe conocer entonces la mejor manera en que la información codificada en estados cuánticos puede ser recuperada de cara a reducir sus efectos. Es sabido que dado un estado desconocido no es posible en general distinguirlo con certeza, pero queremos conocer la mejor manera en la que puede ser estimado.

1.2 Resultados

El trabajo realizado en esta tesis se ha centrado de manera principal en estudiar el entrelazado en sistemas compuestos de distintas partes, así como en la estimación de estados cuánticos, que son dos de los problemas más importantes en Información Cuántica. El objetivo de esta sección es recoger de manera resumida los principales resultados encontrados.

1.2.1 Entrelazado en sistemas de tres bits cuánticos

El entrelazado es un recurso en Información Cuántica, por lo que es imprescindible conocer sus propiedades de cara a su aprovechamiento. Como se ha mencionado anteriormente, se analizan sistemas de diferentes observadores que comparten un estado en el que hay correlaciones cuánticas (es decir sin análogo clásico) entre ellos, y se estudia cómo varían estas correlaciones al actuar cada parte en su subsistema y comunicarse clásicamente con el resto. Esto permite conocer de un modo cualitativo, y también cuantitativo, las propiedades de entrelazado de los distintos estados cuánticos de

sistemas compuestos. Existen dos situaciones distintas en las que se realiza este análisis: la primera es cuando las distintas partes comparten una copia del estado cuántico, mientras que la segunda se centra en un régimen asintótico en el que se tiene un número infinito de copias del estado, en un análogo del límite termodinámico. Los primeros pasos en ambas direcciones se dieron para el caso de espacios de dos partículas, tanto para estados puros como mezcla. Podemos afirmar que las correlaciones cuánticas que se tienen en estados puros en sistemas de dos observadores están bien entendidas, tanto en el límite asintótico como en el caso de una única copia, mientras que para matrices densidad existen todavía varias preguntas fundamentales que permanecen abiertas.

En esta tesis nos hemos centrado en el estudio de las correlaciones cuánticas en sistemas de tres bits cuánticos que se encuentran en un estado puro, $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$. No hemos considerado el límite asintótico, por lo que se tiene una única copia del estado. Un estado genérico de tres bits cuánticos pertenece a un espacio complejo de dimensión ocho, por lo que depende de dieciséis parámetros reales, y si tomamos los estados ya normalizados, este número se reduce a quince. Es sabido que las propiedades de entrelazado o no locales de un estado puro de tres qubits dependen de seis parámetros reales (cinco si están normalizados), por lo que es importante individuar, a partir de los dieciséis (quince) parámetros que se necesitan para especificar un estado, un conjunto de seis (cinco) que releje toda la información acerca de sus correlaciones cuánticas. En el artículo que se encuentra en el apéndice A se demuestra que es posible escribir cualquier estado de tres bits cuánticos en una forma canónica en la que aparecen seis coeficientes especificando sus propiedades no locales. De este modo dos estados, en el caso de una copia, tienen el mismo entrelazado si y sólo si son iguales los coeficientes de sus dos respectivas descomposiciones. Es la primera parametrización completa y mínima de las correlaciones cuánticas de estados puros de tres bits cuánticos que se ha obtenido. La idea en la que hemos basado la descomposición es en buscar la manera de representar el estado en la que toda la información sobre sus propiedades locales es minimizada, de modo que los parámetros no locales son fácilmente reconocibles.

Siguiendo con esta idea, en el artículo del apéndice B hemos comparado las maneras mínimas de escribir cualquier estado para obtener una representación simple de sus correlaciones cuánticas que facilite posteriores aplicaciones de ellas. Además se ha relacionado la parametrización encontrada

con otras ya existentes que no eran completas o mínimas.

Las propiedades de entrelazado en estados puros de tres bits cuánticos empieza a ser entendidas, sobre todo en el caso de una copia. En el artículo del apéndice C, extendemos parte de la estructura ya conocida a estados mezcla. Definimos una división del espacio de matrices densidad de tres bits cuánticos en términos de conjuntos compactos y convexos que están contenidos el uno en el otro. El esquema que resulta aparece como una generalización natural de varios de los conceptos y resultados ya existentes para estados puros de tres qubits, y para estados de sistemas de dos partículas. Además permite una traslación fácil de varias de las técnicas matemáticas que ya se han utilizado para el estudio de las propiedades de entrelazado de las matrices densidad de espacios de dos observadores.

Finalmente, en el artículo del apéndice D hemos llevado a cabo una aplicación práctica de los resultados encontrados en los trabajos anteriores. Como se ha indicado, las descomposiciones encontradas permiten escribir estados genéricos de tres bis cuánticos en representaciones simples que facilitan el estudio de sus correlaciones cuánticas. Nos centramos en el estado puro de tres bits cuánticos que describe las polarizaciones de los tres fotones resultantes de la desintegración del ortopositronio, el estado ligado de un positrón y un electrón. Analizamos las correlaciones cuánticas de este estado para demostrar la imposibilidad de que un modelo clásico refleje los resultados estadísticos que se derivan de ellas. De hecho, aparece un contraste, en principio experimentalmente medible, entre las predicciones que realiza la Mecánica Cuántica para el estado de tres fotones analizado y cualquier teoría local. Demostramos que la contradicción que se tiene es más fuerte que la que se encontraría para cualquier estado entrelazado de dos bits cuánticos.

1.2.2 Estimación de estados

El segundo tema que se ha tratado en esta tesis es la estimación óptima de estados. Dado un estado desconocido, debido a la no ortogonalidad nos es imposible distinguirlo con exactitud a no ser que un número infinito de copias de él estén a nuestra disposición. Como es lógico no es ésta la situación habitual, en general tendremos un número finito de copias del estado incógnita, por lo que sólo podemos aspirar a estimarlo sin garantizar una seguridad completa. Se debe encontrar entonces la estrategia que en media se comporta mejor, es decir que maximiza la ganancia de información acerca del estado en función

de los recursos, o número de copias, que se poseen. Los dos artículos en esta tesis que consideran problemas de estimación se encuentran recogidos en los apéndices E y F. Ambos tratan sólo con estados puros, pero mientras que el primero se centra en diseñar la mejor estrategia para la estimación del estado en su totalidad, del conjunto de sus propiedades, el segundo sólo analiza la mejor manera de poder inferir la cantidad de entrelazado en el caso de un estado puro de dos bits cuánticos. A continuación resumimos con más detalle los resultados hallados.

En el artículo que se encuentra en el apéndice E buscamos la mejor manera de estimar un estado puro de dimensión arbitraria d. Se utiliza una función fidelidad que mide el grado de bondad de la estrategia de estimación; así la mejor estrategia será aquella que maximice la fidelidad. Puesto que el máximo que puede tomar esta función ya ha sido calculado, se debe encontrar la medida que permite alcanzar este valor. La resolución del problema es conocida cuando el estado puro a ser estimado pertenece a un espacio de dimensión dos, es un bit cuántico. En el artículo del apéndice E extendemos este resultado para dimensión arbitraria, diseñamos el método para maximizar la fidelidad, y como ejemplo damos la contrucción explícita de la estrategia de estimación óptima para el caso en que se tienen dos copias de un estado desconocido de dimensión tres. Se observa sin embargo que la generalización es no trivial y que se tienen nuevos elementos que no aparecían para el caso de qubits.

Finalmente, en el artículo del apéndice F se analiza un problema ligeramente distinto: dado un estado desconocido de dos bits cuánticos compartido por dos observadores o partes, debemos hallar la mejor manera de estimar las correlaciones cuánticas entre ellos. Se debe notar que en este caso no estamos interesados en la determinación del estado en su totalidad, sino sólo en alguna de sus propiedades. De hecho un estado de dos qubits, ya normalizado, depende de siete parámetros reales, pero sus propiedades no locales están recogidas por un único valor, que es el que debe estimarse. Consideramos el caso más general en que las dos partes pueden juntar sus sistemas cuánticos y realizar operaciones globales sobre ellos, pero demostramos que la estrategia de estimación óptima puede ser llevada a cabo por uno de los observadores sin necesidad de colaboración del otro. Esto lleva al interesante resultado de que las propiedades no locales de un estado de dos bits cuánticos pueden ser estimadas de manera óptima localmente por una de las partes.

1.3 Conclusiones

En esta tesis hemos analizado algunas de las cuestiones concernientes a dos de los temas más importantes en Información Cuántica: la estimación de estados y las propiedades de entrelazado, o correlaciones cuánticas en estados de sistemas compuestos.

En el primer caso, los principales resultados hallados son:

- Hemos diseñado la estrategia óptima para la estimación de estados puros de dimensión arbitraria, generalizando resultados ya existentes.
- Demostramos que en el caso de estados puros de dos bits cuánticos, la estimación de su entrelazado, es decir de sus propiedades no locales, puede realizarse localmente.

En todo este tipo de aplicaciones es importante saber explotar las simetrías del problema, dado que ello facilita la obtención de la estrategia óptima. Siguiendo con esta línea, una de las preguntas que quedan abiertas es encontrar la mejor manera de estimar estados mezcla de dimensión mayor que dos. De todos modos a un nivel fundamental casi todas las ideas han sido entendidas, y el problema se reduce en gran parte a un ejercicio de cálculo.

Para el caso de las correlaciones cuánticas, pensamos que esta tesis ha contribuido a mejorar la comprensión de las propiedades de entrelazado de sistemas de tres bits cuánticos, y en general a entender las dificultades que aparecen al intentar extender los resultados ya conocidos para espacios de dos partes a sistemas de más observadores. Los siguientes puntos resumen nuestro trabajo en este tema:

- Hemos encontrado una descomposición de todo estado de tres bits cuánticos en la cual aparece un conjunto de parámetros especificando de manera completa las propiedades no locales del estado.
- Definimos una estructura para el espacio de matrices densidad de tres bits cuánticos que extiende muchos de los resultados ya conocidos y que permite una traslación sencilla de gran parte de las técnicas matemáticas que se han venido utilizando hasta ahora.
- Analizamos el estado puro que describe las polarizaciones de los tres fotones obtenidos en la desintegración del ortopositronio y mostramos

que sus correlaciones cuánticas son más "fuertes" que las de cualquier estado de dos qubits a la hora de descartar cualquier teoría local, como por ejemplo la Mecánica Clásica.

Desde un punto de vista teórico una cuestión interesante que queda por resolver es el comportamiento de las correlaciones cuánticas de estados puros de tres partes en el régimen asintótico de infinitas copias. Pero quizás todavía más importante es encontrar aplicaciones prácticas del entrelazado entre más de dos partículas. Para el caso de estados mezcla quedan preguntas básicas por responder aún en el caso de sistemas de dos observadores; por encima de todas, conocer, dada una matriz densidad, cómo detectar si contiene correlaciones cuánticas, y en caso afirmativo, si son aprovechables.

Chapter 2

Quantum Entanglement

2.1 Introduction

Quantum correlations or entanglement among many particles is one of the most intrinsic properties of Quantum Mechanics. From an historical point of view, its importance was first related to the fact that there does not exist any local realistic (LR) theory *à la* Eintein-Podolsky-Rosen (EPR) [1] being able to reproduce these correlations. Indeed, all the LR theories satisfy some inequalities, known as Bell inequalities [2], that are violated by quantum entangled states. This provides us experimental conditions for testing LR theories against Quantum Mechanics. Many experiments have been performed showing a violation of some Bell inequalities [3], and proving that no LR theory can reproduce all the correlations observed in Nature. In this sense, entanglement is crucial for our understanding of Quantum Mechanics.

More recently, it has been realised that entanglement can also be a very useful resource from a more practical point of view. Contrary to what happens for Quantum Mechanics, Classical Physics admits a description by means of a LR model (indeed it is a LR theory). This means that there are some correlations that do not appear in our *classical world*, and they are intrinsically quantum. Can we take profit of this new kind of correlations? Quantum Information gives an affirmative answer to this question: quantum teleportation or superdense coding are examples of tasks that use entanglement in order to achieve some results which are not possible in a classical environment. Of course, these information processings have not classical

analogue and can not be explained in terms of Classical Information Theory.

In this chapter we review most of the known results concerning quantum correlations, focusing into the case of two systems, i.e. bipartite entanglement. After giving some definitions, we consider Bell inequalities and their violation by means of an entangled pure state. Then, we show some of the applications of entanglement (teleportation and superdense coding), and we study the differents ways of characterizing it. Although we mainly restrict our analysis to pure states, in the end we will also sketch the mixed-state case.

2.2 Quantum correlations

Consider a composite quantum system of N parties, or subsystems, each described by a Hilbert space of dimension d_i, $i = 1, \ldots, N$. The global Hilbert space is equal to the tensor product of all the spaces, $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N = \bigotimes_{i=1}^{N} \mathcal{H}_i$, with dimension $d = \prod_{i=1}^{N} d_i$. The preparation of the system is given by a quantum pure state in the whole space $|\Psi\rangle \in \mathcal{H}$.

A pure state is called separable when it can be expressed as the tensor product of pure states in each party, i.e. $|\Psi\rangle$ is separable if and only if

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle, \tag{2.1}$$

where $|\psi_i\rangle \in \mathcal{C}^{d_i}$. A state that can not be expressed in this form is non-separable or entangled. There are no correlations between the subsystems when the preparation of the whole system is described by a state (2.1).

This definition can be easily extended to density matrices, and a mixed state, ρ, is said to be separable when it can be written as a convex combination of projectors onto product states [4], i.e. there is a decomposition of the state in terms of separable pure states,

$$\rho = \sum_{j=1}^{r} p_j |\psi_1^j\rangle\langle\psi_1^j| \otimes \cdots \otimes |\psi_N^j\rangle\langle\psi_N^j| \equiv \sum_{j=1}^{r} p_j |\Psi_j^s\rangle\langle\Psi_j^s|, \tag{2.2}$$

where $p_j \geq 0, \sum_{j=1}^{r} p_j = 1$. The state ρ is a probabilistic mixture of the product states $|\Psi_j^s\rangle$, $j = 1, \ldots, r$, so it does not contain any type of entanglement and all its correlations are classical. In fact, ρ can be prepared by the parties when they are able to perform locally any quantum operation and are allowed to use only classical communication.

2.3 Bell inequalities

As it has been mentioned, a state in a composite system is entangled when it contains quantum correlations, i.e. the subsystems are correlated in a way that can not be described by any LR model. But, what is understood by a local realistic model? And, how can we know that none of these models is able to reproduce these kind of intrinsically quantum correlations?

The answer for the first question comes from the scheme proposed in [1]. There, it is stated that any complete local realistic theory must not contradict the following three quite plausible premisses:

- *Locality:* No change can be produced in one system by acting in another space-separated system.
- *Reality:* If our theory predicts the value of a physical quantity with certainty without disturbing the system, there exists an element of physical reality corresponding to this quantity.
- *Completeness:* Every element of physical reality must appear in our theory.

There is an infinite number of such theories, but, as Bell proved [2], there are some constraints that they should verify. Let us sketch here his argument.

Consider for instance a composite system of two space-separated spin-$\frac{1}{2}$ particles, A and B (or Alice and Bob), whose observed statistical results are described, in terms of Quantum Mechanics, by the singlet state,

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{2.3}$$

Adapting the three assumptions of [1] to this situation, due to the perfect correlations present in (2.3) and because of locality (the subsystems are space-separated), any spin component of each party is an objective property of A and B and, then, it should be reflected by our complete theory. Nevertheless, Quantum Mechanics can not assign definite values to spin components that do not commute, so it does not provide a complete description of the state of the system. The authors of [1] claimed that there should be an alternative LR description that, without changing the statistical results predicted

by Quantum Mechanics, which are right, is able to overcome this lack of completeness.

In this new theory there will be a space, Λ, of possible states for the whole system, and the description of the observed statistical results consists on a probability distribution $p(\lambda)d\lambda$ over this space of states, where λ is a set of coordinates parametrizing it. Each of the parties is able to measure the spin component of the corresponding particle, where the differents measurements are specified by a set of parameters n_a and n_b for A and B (the directions of the Stern-Gerlach apparatus in this case), the outcome being labelled by ± 1. Since the theory is complete, there should exist some functions, a, predicting the outcome of an experiment specified by n_a when the state of the system is λ. No dependence on party B, and in particular on n_b, is allowed for this function because of locality, i.e. the second space-separated system can not influence the measurement A performs. Simple algebra shows that for four measurements, a and a' for party A, and b and b' for party B, it is verified

$$ab + ab' + a'b - a'b' = \pm 2, \tag{2.4}$$

and then, the corresponding expectation value of these combination of observables is bounded by

$$-2 \leq \langle ab + ab' + a'b - a'b' \rangle \leq 2. \tag{2.5}$$

This is an example of a Bell inequality found in [5]. It is not difficult to prove that for the singlet state (2.3) there are four directions, $\hat{n}_a = (0, 0, 1)$, $\hat{n}'_a = (1, 0, 0)$, $\hat{n}_b = (1/\sqrt{2}, 0, -1/\sqrt{2})$ and $\hat{n}'_b = (1/\sqrt{2}, 0, -1/\sqrt{2})$, or quantum observables, specified by $\hat{n}_i \cdot \vec{\sigma}$, where $i = a, a', b, b'$ and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$, such that (2.5) takes its maximum value, which is equal to $2\sqrt{2}$. The consequences resulting from the violation of this Bell inequality are very strong, since no LR model, following the three EPR premisses, will be able to reproduce this statistical value. This answers the second question raised at the beginning of this section.

It is evident that this demonstration depends on the initial state (2.3), but similar (and even stronger) results have been obtained for higher dymensional systems of two particles and systems of more than two parties. Entanglement, or nonseparability, plays a crucial role in these derivations and indeed it has been proved that any pure state which is not separable violates some Bell inequality [6], while product states do not. Since Classical Physics is a LR

theory, these correlations cannot be observed in *our classical world*, they are intrinsically quantum and Quantum Mechanics is said to be nonlocal.

2.4 Entanglement as a resource

In the preceeding section we have shown the importance of entanglement from a very fundamental point of view: entangled states contain some kind of correlations that do not have analogue in Classical Physics, since the latter is a LR theory. One may wonder whether these intrinsically quantum correlations are useful, whether it is possible to find some applications taking advantage of them. Most of the recent quantum information processings are based on this idea: they use this quantum feature as a resource for accomplishing some tasks that are not possible in Classical Information Theory. Indeed, entanglement plays a key role in many quantum information applications, such as, for instance, quantum cryptography [7], quantum error-correction [8], superdense coding [9] and quantum teleportation [10]. In this section, we review superdense coding and teleportation, in order to illustrate with these two examples the usefulness of entangled states.

2.4.1 Superdense coding

Consider two observers A and B, Alice and Bob, who share an entangled state,

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B), \tag{2.6}$$

where each of the parties can manipulate only one of the two subsystems. As we will see, the singlet state and $|\Phi^+\rangle$ are examples of a maximally entangled state of two spin-$\frac{1}{2}$ particles, or qubits [11]. Alice wants to send two bits of classical information to Bob. She can choose a unitary transformation, U_i, from the set $\{I, \sigma_x, i\sigma_y, \sigma_z\}$ and apply it to her qubit. Then, she sends her particle or qubit to Bob, who is now able to manipulate the two-qubit state $|\Phi_i\rangle = U_i \otimes I|\Phi^+\rangle$. He doesn't know the unitary transformation performed by Alice, but, since the four states $|\Phi_i\rangle$, with $i = 1, \ldots, 4$, are orthogonal, he can recover it with just a Von Neumann measurement in the basis given by

the four states,

$$\begin{aligned}
|\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = I \otimes I\,|\Phi^+\rangle \\
|\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \sigma_z \otimes I\,|\Phi^+\rangle \\
|\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \sigma_x \otimes I\,|\Phi^+\rangle \\
|\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = i\sigma_y \otimes I\,|\Phi^+\rangle. \qquad (2.7)
\end{aligned}$$

This is the so-called Bell basis. At the end of this protocol, two bits of classical information have been transmitted from Alice to Bob by sending one of the qubits of a maximally entangled state of two qubits, initially shared by sender and receiver. This quantum information process is known as superdense coding.

2.4.2 Quantum teleportation

Quantum teleportation is another quantum information application that uses similar techniques. In this case Alice wants to transmit a spin-$\frac{1}{2}$ particle to Bob, but the qubit cannot be sent since only classical communication can be performed faithfully. If Alice knows the state of her particle, the direction of its Bloch vector, she can use a very large string of classical bits for codifying it, and send it to Bob, who prepares a quantum system according to the received information. Note that the state in Bob's side can not be equal to Alice's unless an infinite number of classical bits are transmitted. However the situation is still worse if Alice doesn't know her state! Of course, she can measure it and send classically to Bob the partial information she has obtained. However, this solution is approximate, and the initial state is destroyed after the measurement. Quantum teleportation solves this problem exploiting the nonlocality of entanglement. If we provide the two observers with a maximally entangled state of two qubits (2.6), Alice is able to send all the information about her unknown qubit to Bob, without sending the particle!

A maximally entangled state (2.6) is shared by the two parties. Alice has an unknown qubit, in state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathcal{C}^2$, that she wants to send

to Bob. The global state is

$$|\Psi\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{2.8}$$

where Alice can manipulate the first two qubits, and the third one is in Bob's hands. It is easy to see that this state can be written as

$$\begin{aligned} |\Psi\rangle &= \frac{1}{2}\Big(|\Psi^-\rangle(-\alpha|0\rangle - \beta|1\rangle) + |\Psi^+\rangle(-\alpha|0\rangle + \beta|1\rangle) \\ &\quad +|\Phi^-\rangle(\alpha|1\rangle + \beta|0\rangle) + |\Phi^+\rangle(\alpha|1\rangle - \beta|0\rangle)\Big). \end{aligned} \tag{2.9}$$

Alice now performs a measurement in the Bell basis (2.7) on her two qubits. Due to the correlations of the entangled state, Bob's state is projected, with equal probability, into one of the following four states

$$\begin{aligned} -\alpha|0\rangle - \beta|1\rangle &= -|\psi\rangle \\ -\alpha|0\rangle + \beta|1\rangle &= -\sigma_z|\psi\rangle \\ \alpha|1\rangle + \beta|0\rangle &= \sigma_x|\psi\rangle \\ \alpha|1\rangle - \beta|0\rangle &= -i\sigma_y|\psi\rangle. \end{aligned} \tag{2.10}$$

Alice sends the result of her measurement to Bob, by means of two bits of classical information, and Bob, after receiving them, can apply the corresponding unitary transformation in order to recover $|\psi\rangle$. Note that $|\psi\rangle$ is in Bob's hands but he doesn't know the state. However, all the information about the particle has been transferred from Alice to Bob just using two bits of classical communication and the pre-shared maximally entangled state.

Teleportation is one of the most spectacular quantum information applications that use entanglement as a resource. After completing the protocol, the whole state is separable respect the partition $A-B$, i.e. the entanglement has been consumed. Moreover, it does not allow for superluminal signaling, since Bob can not infer any information about the unknown Alice's qubit until he receives the two bits of classical information. Finally, note that no trace of the unknown particle remains in Alice's hands, and therefore, there isn't any contradiction with the no-cloning theorem [12].

2.5 LOCC: the set of local operations and classical communication

Entanglement are the quantum correlations that appear in composite quantum systems. Given a state, we can always increase the amount of quantum correlations between the parties performing some global operation over the state. As an example of entangling operations in $\mathcal{C}^2 \otimes \mathcal{C}^2$, take the unitary transformation that changes the product basis $|ij\rangle$, where $i = 0, 1$ ($j = 0, 1$) is an orthonormal basis in A (B), into the Bell basis (2.7), or a measurement in this basis, known as Bell measurement. Nevertheless, this is not the usual situation in most of the quantum information applications, where the parties are in space-separated locations and can not perform joint operations on the global system. Usually, they are only able to make any quantum operation on their local system and to communicate classically with the rest of the parties. It is then very useful to study how quantum states of composite systems change their entanglement properties under this restricted set of quantum operations, i.e. under local operations assisted with classical communication (LOCC). Note that entanglement is a resource that can not increase under LOCC, since classical communication just increases the amount of classical correlations among the subsystems, while local (quantum) operations do not correlate the parties at all. Thus, our scenario for the study of entanglement will consist on composite systems where the parties are allowed to manipulate arbitrarily their own system and to broadcast the implemented local operation.[1]

2.6 Bipartite entanglement

In the preceding sections we have defined what entangled states are and we have shown the utility of these states, either from a fundamental point of view or in practical quantum information applications. Although entangled states can be shared by any number of parties, our reasonings above were mainly restricted to two-party systems. In fact, bipartite pure-state entanglement is rather well-understood, and in this section we review some of the most

[1] A detailed mathematical formulation of quantum operations is given in [13], while see [14] for the restricted case of LOCC.

important results. In the next capter three-party, and in particular three-qubit, entanglement will be analyzed.

2.6.1 Schmidt decomposition

The aim of this section is to study the quantum correlations that appear between two subsystems, A and B. The Hilbert space of the whole system is given by the tensor product of the two Hilbert spaces associated with each subsystem $\mathcal{H}_A$ and $\mathcal{H}_b$, with dimension d_A and d_B. A pure state of the composite system corresponds to a vector $|\Psi\rangle \in \mathcal{C}^{d_A} \otimes \mathcal{C}^{d_B}$. We can build an orthonormal basis for the global system from two orthonornormal bases in each subsystem, and any pure state, $|\Psi\rangle$, can be expressed in this basis as

$$|\Psi\rangle = \sum_{i=1}^{d_A} \sum_{j=1}^{d_B} t_{ij} |ij\rangle, \tag{2.11}$$

where $\{|1\rangle, \ldots, |d_A\rangle\}$ ($\{|1\rangle, \ldots, |d_B\rangle\}$) is the basis for A (B) and t_{ij} are the coordinates of the vector in the product basis $|ij\rangle$. Define the $d_A \times d_B$ matrix T with elements $(T)_{ij} \equiv t_{ij}$.

Theorem 2.1 (Schmidt decomposition) *[15] Suppose a normalized state of a composite system, $|\Psi\rangle \in \mathcal{C}^{d_A} \otimes \mathcal{C}^{d_B}$, whose coordinates in a product basis, $|ij\rangle$, are given by the matrix T. There exists a choice of the local bases such that T has only diagonal terms, and thus, the state written in this basis is*

$$|\Psi\rangle = \sum_{i=1}^{r} \alpha_i |ii\rangle, \tag{2.12}$$

where $r \leq \min(d_A, d_B)$ and α_i are positive numbers satisfying $\sum_i \alpha_i^2 = 1$.

Proof: Starting from (2.11), the effect of a change of basis in the first (second) subsystem can be represented by left-multiplying (right-multiplying) the matrix of coordinates, T, by a unitary matrix U_A (U_B). It is a well-known result that it is always possible to diagonalize any matrix by means of two unitary transformations (singular value decomposition),

$$T_d = U_A T U_B, \tag{2.13}$$

where T_d has only positive diagonal terms. □

Equation (2.12) is the Schmidt decomposition of state $|\Psi\rangle$, α_i are its Schmidt coefficients and r, the number of nonvanishing coefficients, is the Schmidt number. This decomposition is unique. The proof of the theorem provides us the method to be applied in order to build the decomposition. The change of local bases are given by the eigenvectors of the matrices $T^\dagger T$ and $TT^\dagger$, while the Schmidt coefficients are the square roots of the eigenvalues of these self-adjoint matrices (which are equal). In a similar way, defining $\rho_A \equiv \mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$ and $\rho_B \equiv \mathrm{tr}_A(|\Psi\rangle\langle\Psi|)$, the spectrum of these density matrices gives us the Schmidt decomposition of the initial state. Note that the eigenvalues of ρ_A and ρ_B are equal and correspond to the square of the Schmidt coefficients.

2.6.2 Local unitary transformations

The study of the entanglement properties of quantum states is related to the way they transform under the set of local operations and classical communication. Consider two states, $|\Psi_1\rangle, |\Psi_2\rangle \in \mathcal{C}^d \otimes \mathcal{C}^d$. We can take the same dimension in each subsystem without loosing generality because the Schmidt number satisfies $r \leq \min(d_A, d_B) = d$. These states have the same amount of quantum correlations when they can be transformed one into another by LOCC with probability equal to one. Then, they are equivalent in terms of quantum nonlocality, $|\Psi_1\rangle \sim |\Psi_2\rangle$. This condition corresponds to see whether the two states can be connected by local unitary transformations [14], i.e. two states have the same amount of entanglement when they can be transformed reversibly by local unitaries, LU. The Schmidt decomposition is a very useful tool for checking this condition. Indeed, denoting by $\{\alpha_i^{(j)}\}$ the Schmidt coefficients of the state $|\Psi_j\rangle$, $j = 1, 2$, we have that $|\Psi_1\rangle \sim |\Psi_2\rangle$ if and only if $\alpha_i^{(1)} = \alpha_i^{(2)}$, $i = 1, \ldots, d$. Thus, the Schmidt coefficients can be thought of as the coordinates in the space of bipartite entanglement, and at most d numbers, the norm being included, are enough for specifying the nonlocal properties of a quantum state belonging to $\mathcal{C}^d \otimes \mathcal{C}^d$.

Another approach to the same problem is to look for polynomial combinations of the coordinates, t_{ij} in (2.11), that are invariant under local unitary transformations [16, 17]. We can parametrize the space of entanglement properties in an alternative way in terms of, at least, d of these invariant quantities that are linearly independent. It can be proved that the algebra of polynomial invariants of two-particle states is generated by the traces of

powers of the local mixed state, $\mathrm{tr}(\rho_A^i)$, with $i = 1, \ldots, d$ [17] (or $\mathrm{tr}(\rho_B^i)$, since the local states have the same eigenvalues). Note that traces of higher powers, $i > d$, of ρ_A (ρ_B) can be written in terms of this set of traces because of the Cayley-Hamilton theorem. It is easy to relate these functions to the Schmidt coefficients.

2.6.3 LOCC transformations in the single-copy case

Local unitary transformations are the type of LOCC that connect states with the same entanglement properties. However, it is possible to relax this condition and, starting from a single copy of a state $|\Psi\rangle$ of the composite system, try to determine those states that we can reach using LOCC, either in a deterministic way or with some nonvanishing probability.

In the first case, we look for those states, $|\Phi\rangle$, into which $|\Psi\rangle$ can be converted by LOCC with probability equal to one, denoted by $|\Psi\rangle \Longrightarrow |\Phi\rangle$. When this transformation is possible, the state $|\Psi\rangle$ is at least as useful as $|\Phi\rangle$ for any task involving quantum correlations, so we will express this fact in terms of entanglement as $|\Phi\rangle \leq |\Psi\rangle$. The necessary and sufficient conditions for these deterministic transformations were given by Nielsen [18], pointing out a very interesting connection between entanglement and the mathematical theory of majorization.

Theorem 2.2 (Nielsen) *[18] Consider two states of a composite system, $|\Psi\rangle, |\Phi\rangle \in \mathcal{C}^d \otimes \mathcal{C}^d$. Denote by $\vec{\lambda}^\Psi \equiv (\lambda_1^\Psi, \ldots, \lambda_d^\Psi)$ the vector with the square of the Schmidt coefficients of $|\Psi\rangle$ taken in decreasing order, i.e. $\lambda_i^\Psi \equiv (\alpha_i^\Psi)^2$, $\forall i$ and $\lambda_1^\Psi \geq \lambda_2^\Psi \geq \ldots \geq \lambda_d^\Psi$, and construct the analogous $\vec{\lambda}^\Phi$ for $|\Phi\rangle$. The state $|\Psi\rangle$ can be transformed into $|\Phi\rangle$ by LOCC in a deterministic way if and only if $\vec{\lambda}^\Psi$ is majorized by $\vec{\lambda}^\Phi$ (denoted by $\vec{\lambda}^\Psi \prec \vec{\lambda}^\Phi$), which means that for each k*

$$\sum_{i=1}^{k} \lambda_i^\Psi \leq \sum_{i=1}^{k} \lambda_i^\Phi, \tag{2.14}$$

with equality for $k = d$.

Proof: See [18]. □

Note that this theorem provides a partial ordering in the space of entangled states, although we can find states such that neither $|\Psi\rangle \Longrightarrow |\Phi\rangle$ nor $|\Phi\rangle \Longrightarrow |\Psi\rangle$ are possible. It should be emphasized that Nielsen proves

the theorem building the LOCC protocol, the sequence of operations, that achieves the deterministic transformation.

For the second situation, we look for probabilistic conversion. Nielsen's theorem gives the conditions for transformations with probability one, but if this is not possible, we may wonder whether the states can be connected with some nonvanishing probability, $|\Psi\rangle \longrightarrow |\Phi\rangle$, and if yes, what the maximum of this probability, $P(\Psi \longrightarrow \Phi)$, is. The answer to these questions were given by Vidal in [19]; his result is summarized in the following theorem:

Theorem 2.3 (Vidal) *[19] Take two states of a composite system, $|\Psi\rangle, |\Phi\rangle \in \mathcal{C}^d \otimes \mathcal{C}^d$ and define the vectors of square of the Schmidt coefficients as above. The maximum probability for a conversion $|\Psi\rangle \longrightarrow |\Phi\rangle$ by LOCC, $P(\Psi \longrightarrow \Phi)$, is*

$$P(\Psi \longrightarrow \Phi) = \min_{l \in [1,d]} \frac{\sum_{i=l}^{d} \lambda_i^{\Psi}}{\sum_{i=l}^{d} \lambda_i^{\Phi}} \tag{2.15}$$

Proof: See [19]. □

Again the explicit protocol for this conversion was given with the proof of the theorem. Let us mention here that $P(\Psi \longrightarrow \Phi) = 0$ when the Schmidt number of the first state is lower than that of the second.[2]

2.6.4 Asymptotic regime

The tranformations between entangled states under local operations and classical communication are also studied in the case in which an infinite number of copies of the entangled states are given. From a practical point of view, this means that the parties are able to perform arbitrary operations in very large (infinite dimensional) Hilbert spaces.

It was proved in [21] that the asymptotic conversion of N copies of the state $|\Psi\rangle$ into an optimal number of copies N' of $|\Phi\rangle$ can be done in a reversible way when $N \to \infty$, and the optimal ratio of the transformation is

$$\lim_{N \to \infty} \frac{N'}{N} = \frac{E(|\Psi\rangle)}{E(|\Phi\rangle)}, \tag{2.16}$$

[2]There is another way of transforming states, by means of the so-called entanglement assisted local operations and classical communication (ELOCC), where entangled states are used as catalyst (see [20]).

where $E(|\Psi\rangle)$ is the entropy of entanglement defined as $E(|\Psi\rangle) \equiv S(\rho_A) = S(\mathrm{tr}_B(|\Psi\rangle\langle\Psi|))$, and $S(\rho) = -\mathrm{tr}(\rho \log \rho)$ is the usual Von Neumann entropy of mixed states, where the log is taken in basis two.

This result is very important since it follows that in the asymptotic limit entangled states, satisfying (2.16), are interconvertible in a reversible way, i.e. there is only one kind of bipartite entanglement. The entropy of entanglement is the measure that quantifies it, in the so-called ebits [22]. Note that this function, $E(|\Psi\rangle)$, depends only on the spectrum of the local density matrix, ρ_A or ρ_B, i.e. on the Schmidt coefficients of the entangled state, $|\Psi\rangle$. It is equal to zero for separable states, and its maximum is $\log d$ (where d is the dimension of the local spaces). This value is achievable if and only if the local states are the totally mixed state, i.e. if $\lambda_i^\Psi = 1/d$, $\forall i$, which gives the maximally entangled state in $\mathcal{C}^d \otimes \mathcal{C}^d$. For the case of qubits, we have found above some examples of maximally entangled states (2.7), and their amount of entanglement is equal to one ebit. Furthermore, the authors of [21] gave the LOCC protocol for the reversible asymptotic conversions.

2.6.5 Mixed states

Entanglement in bipartite systems is rather well understood for pure states, but this is not the case for density matrices. Indeed, effective necessary and sufficient conditions for a mixed state ρ to be separable are not known, apart from the cases $\mathcal{C}^2 \otimes \mathcal{C}^2$ and $\mathcal{C}^2 \otimes \mathcal{C}^3$ (see [23]). Thus, in general we are not able to detect whether a mixed state contains quantum correlations and therefore the problem of separability remains open. Significant steps in this direction have been made, mainly by the Horodecki family, the IBM group, and the Hannover and Innsbruck groups, using positive maps which are not completely positive and entanglement witnesses. A related problem, which is also unsolved, is whether the entanglement in a mixed state can be distilled or transformed into some amount of maximally entangled pure states, which are the states useful for most of the quantum information applications. Moreover, from a fundamental point of view the picture is far from being clear, and it is not known which entangled mixed states do violate Bell inequalities. For an introduction on these and other related problems see [24].

2.7 Conclusions

In this chapter we have reviewed part of the present knowledge on quantum correlations, mainly on bipartite pure-state entanglement. The following points summaryze the most important results:

- A pure state in an N-party system, $|\Psi\rangle \in \mathcal{C}^{d_1} \otimes \cdots \otimes \mathcal{C}^{d_N}$, is separable when it can be written as the tensor product of pure states in each subsystem.
- A mixed state is separable if and only if it can be expressed as a convex sum of projectors onto product pure states.
- Quantum states that are not separable are entangled, i.e. they have quantum correlations.
- Entanglement or quantum correlations can not be described by local realistic theories and it is a powerful resource for many quantum information tasks.
- The set of local operations and classical communication, LOCC, is a very useful tool for the study of the entanglement properties of quantum states. All the information concerning quantum correlations of pure states is encoded in the Schmidt coefficients.
- Single-copy case: two states have the same amount of entanglement when they can be connected by local unitary transformations, i.e. their Schmidt coefficients are equal. Necessary and sufficient conditions, in terms of these coefficients, are known for deterministic and probabilistic conversions between states by LOCC.
- Asymptotic regime: there is only one kind of bipartite pure-state entanglement, that is quantified by the entropy of entanglement. In this limit, entangled states can be transformed in a reversible way according to this measure.
- There are still many open questions for mixed states.

Chapter 3

Three-qubit entanglement

3.1 Introduction

In the previous chapter we have shown that the entanglement properties of pure states of bipartite systems are quite well understood. We know how the quantum correlations of these states change under local operations and classical communication, either in the single-copy case or in the asymptotic regime. In this chapter we give an introduction for the articles:

- *Generalized Schmidt decomposition and classification of three-quantum-bit states*
  A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre and R. Tarrach
  Physical Review Letters **85**, 1560 (2000), quant-ph/0003050.
  See appendix A.

- *Three-qubit pure-state canonical forms*
  A. Acín, A. Andrianov, E. Jané and R. Tarrach
  Submitted to Journal of Physics A, special issue on Quantum Information, quant-ph/0009107.
  See appendix B.

- *Classification of mixed three-qubit states*
  A. Acín, D. Bruss, M. Lewenstein and A. Sanpera
  Submitted to Physical Review Letters, quant-ph/0103025.
  See appendix C.

- *Three-party entanglement from positronium*
  A. Acín, J. I. Latorre and P. Pascual
  Physical Review A **63**, 042107 (2001), quant-ph/0007080.
  See appendix D.

All these articles are about entanglement in three-qubit systems; the first two ones deal with pure states, while the third generalizes to the mixed-state case the structure for pure states. The last shows an application of the results to a concrete example by studying the quantum correlations of the three-photon polarization state coming from orthopositronium decay.

In the pioneering work of Ref. [25], it was shown that entangled states of three particles exhibit new features, compared to the bipartite case, by analyzing the correlations appearing in the so-called Greenberger-Horne-Zeilinger (GHZ) state,

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle). \tag{3.1}$$

This state can be interpreted in many senses as the maximally entangled state of three spin-$\frac{1}{2}$ particles [26].

The aim of this chapter is to try to understand the way in which known results for bipartite systems can be extended to systems of three spin-$\frac{1}{2}$ particles, and to overcome the difficulties that appear due to the fact that, as we have already mentioned, this generalization is not trivial. This gives us insight into the characterization of three-party entanglement and how it compares to the bipartite case.

3.2 Reversible transformations under LOCC

Two quantum states have the same entanglement, are equivalent as fas as their nonlocal properties is concerned, when they can be transformed one into another in a deterministic way by local operations and classical communication. This statement is clearly independent of the dimension of the local systems or the number of parties. We have seen in the previous chapter that, for the bipartite case, this implies that the two states must be connected by local unitary transformations. In [27] it was proved that the same conclusion is valid for any composite system, i.e. given $|\Psi_1\rangle, |\Psi_2\rangle \in \mathcal{C}^{d_1} \otimes \cdots \mathcal{C}^{d_N}$, these

two states are equivalent in terms of entanglement, $|\Psi_1\rangle \sim |\Psi_2\rangle$, if and only if there exist N unitary transformations such that $|\Psi_1\rangle = U_1 \otimes \cdots \otimes U_N |\Psi_2\rangle$. Thus, we would like to know how pure states are related under these operations, the tensor product of local unitaries (or change of the local bases), in order to individuate a set of canonical entanglement coordinates specifying all the nonlocal properties of states of composite systems. For the bipartite case two different approaches are useful (see 2.6.2): the existence of the Schmidt decomposition allows to write any pure state of a two-party system, $\mathcal{C}^{d_A} \otimes \mathcal{C}^{d_B}$, in a canonical form where all the information about its nonlocal properties is encoded in the Schmidt coefficients. On the other hand, we can also obtain an alternative set of entanglement parameters by means of $d = \min(d_A, d_B)$ polynomial combinations of the coordinates t_{ij} in a product basis (see Eq. (2.11)), which are linearly independent and invariant under local unitaries.

3.2.1 Polynomial invariants

The first steps into the characterization of multi-particle pure-state entanglement in terms of equivalences under local unitary transformations were given in [16]. The action of a tensor product of N unitaries, $U_1 \otimes \cdots \otimes U_N$, describes orbits in the whole Hilbert space, $\mathcal{C}^{d_1} \otimes \cdots \otimes \mathcal{C}^{d_N}$; all the states in an orbit have the same quantum correlations. Every orbit, then, gives a point in the space of entanglement properties, and it would be useful to know how many parameters are needed for specifying a unique orbit, which is equivalent to determine the dimension of the space of entanglement properties.

A first estimation of this number is obtained by the following counting of parameters. A pure state, $|\Psi\rangle$, which is not normalized, depends on $2d$ real numbers[1] (d complex numbers), where d is the dimension of the whole Hilbert space, $d = \prod_{i=1}^{N} d_i$. The tensor product of N local unitaries is an element of the group $U(d_1) \times \cdots \times U(d_N)$, which reduces to $U(1) \times SU(d_1) \times \cdots \times SU(d_N)$, and it depends at most on $1 + \sum_{i=1}^{N} (d_i^2 - 1)$ real numbers. A lower bound, then, for the number of real numbers needed for specifying an orbit, or a point in the space of entanglement properties, is $2 \prod_{i=1}^{N} d_i - (1 + \sum_{i=1}^{N} (d_i^2 - 1))$. For the case of an N-qubit system ($d_i = 2, \forall i$), this expression reads

[1] Note that if we consider normalized states and the global phase is removed, the state depends on $2d - 2$ real numbers.

$2^{N+1} - (3N+1)$. The authors of [16] gave also the procedure to be applied in order to calculate exactly the number of nonlocal parameters of a state, and proved that for the case of three-qubits systems, the counting of parameters is correct, i.e. the space of entanglement properties for pure three-qubit states is six-dimensional. Let us analyze further this case.

For pure three-qubit states, Sudbery [17] found six quantities invariant under local unitary transformations which are linearly independent. Starting from a pure three-qubit state, $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$, shared by three parties, A, B and C, and writing it in a product orthonormal basis,

$$|\Psi\rangle = \sum_{i,j,k} t_{ijk} |ijk\rangle, \tag{3.2}$$

where $|i\rangle$, $i = 0, 1$, define an orthonormal basis in A, and the same for $|j\rangle$ and $|k\rangle$ for B and C, we can construct polynomial combinations of the coordinates, t_{ijk}, invariant under local unitary transformations. A trivial example of these polynomial invariants is the norm. Indeed in [17] the six linearly independent invariants of minor degree were presented, although it was not proved whether they were enough to completely specify a pure three-qubit state, up to definition of the local bases. It was known that the space of entanglement parameters for these states is six-dimensional, but this only guarantees that Sudbery's six polynomial invariants, that will be denoted by $\{I_i\}$, $i = 0, \ldots 5$, where I_0 is the norm, are able to identify a point in this space, up to some discrete symmetries. This means that it might be the case that the set of polynomial quantities $\{I_i\}$ is not complete, i.e. more polynomial invariants are needed, although most of the information they provide is redundant. The explicit form of these invariants is:

$$\begin{aligned}
&\frac{1}{2} \leq I_1 \equiv \mathrm{tr}(\rho_A^2) \leq 1 \\
&\frac{1}{2} \leq I_2 \equiv \mathrm{tr}(\rho_B^2) \leq 1 \\
&\frac{1}{2} \leq I_3 \equiv \mathrm{tr}(\rho_C^2) \leq 1 \\
&\frac{1}{4} \leq I_4 \equiv \mathrm{tr}(\rho_A \otimes \rho_B \rho_{AB}) \leq 1 \\
&0 \leq I_5 \equiv |\mathrm{Hdet}(t_{ijk})|^2 \leq \frac{1}{16},
\end{aligned} \tag{3.3}$$

where $\mathrm{Hdet}(t_{ijk})$ is the hyperdeterminant of the three-index tensor t_{ijk} (see appendix A or B for more details).

3.2.2 Generalization of the Schmidt decomposition

The Schmidt decomposition has been proved very fruitful for the determination of the nonlocal properties of pure states of two-particle systems. All the information about entanglement of bipartite pure states is encoded in the Schmidt coefficients. However it was soon realised that a trivial generalization of this decomposition for systems of N parties with $N > 2$ does not exist (see for instance [28]). Indeed, and focusing again into the three-qubit case, it is the lack of a Schmidt-like canonical decomposition that makes hard to relate the value of the polynomial invariants seen above with a specific pure three-qubit state.

In the article of appendix A, we generalize the Schmidt decomposition to three-qubit pure states. The following idea guides the generalization: starting from a generic state as (3.2), we look for the local bases that make zero the maximum number of the coordinates t_{ijk}, i.e. we search the expression of the state with the minimal number of terms built from local orthonormal bases. By a simple counting of parameters we can prove that, in general, not more than three of the eight coefficientss can be zero. Indeed this is the case, since there always exist local orthonormal bases such as the state (3.2) can be written

$$|\Psi\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\varphi}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle, \tag{3.4}$$

where $\lambda_i \geq 0$, $i = 0, \ldots, 4$, $\sum_i \lambda_i^2 = 1$, and $0 \leq \varphi \leq \pi$. For any state, there is a unique decomposition of this form.[2] The existence of this decomposition allows us to check when two states of three qubits, $|\Psi_1\rangle, |\Psi_2\rangle$, can be converted by local unitary transformations, since $|\Psi_1\rangle \sim |\Psi_2\rangle$ if and only if the parameters appearing in the generalized Schmidt decompositions of the two states are equal, i.e. $\lambda_i^{(1)} = \lambda_i^{(2)}$, $i = 0, \ldots, 4$ and $\varphi^{(1)} = \varphi^{(2)}$. Thus, these parameters are thought of as the coordinates for the six-dimensional space of entanglement properties. Similar decompositions were also found in [29].

[2] Actually this is true except for a set of states, of measure zero, where there are two possible decomposition with $\varphi = 0, \pi$ (see appendices A and B for more details).

A new set, $\{J_i\}$, $i = 1, \ldots, 5$, of five polynomial combinations of the coordinates t_{ijk}, invariant under local unitaries, is introduced (apart from the norm). This new set is related to Sudbery's invariants,

$$\begin{aligned} J_1 &\equiv \frac{1}{4}(1 + I_1 - I_2 - I_3 - 2\sqrt{I_5}) \\ J_2 &\equiv \frac{1}{4}(1 - I_1 + I_2 - I_3 - 2\sqrt{I_5}) \\ J_3 &\equiv \frac{1}{4}(1 - I_1 - I_2 + I_3 - 2\sqrt{I_5}) \\ J_4 &\equiv \sqrt{I_5} \\ J_5 &\equiv \frac{1}{4}(3 - 3I_1 - 3I_2 - I_3 + 4I_4 - 2\sqrt{I_5}), \end{aligned} \tag{3.5}$$

but the expression for the new functions in terms of the coefficients of (3.4) is easier. As it is shown in the appendix B, using the generalized Schmidt decomposition, we are able to see that these, or Sudbery's, invariants, are not enough to specify a unique normalized pure three-qubit state up to local unitary transformations. In fact, they can not discriminate between $|\Psi\rangle$ or $|\Psi^*\rangle$, which usually do not belong to the same orbit. A new, more complicate, complex polynomial invariant, I_6, introduced by Grassl [30], solves the problem, and the set $\{J_i, I_6\}$, $i = 1, \ldots, 5$ (or alternatively $\{I_i\}$, $i = 1, \ldots, 6$), plus the norm, is complete, it provides us all the information about the non-local properties of a pure three-qubit state. Indeed, given the values of these invariants, it is possible to obtain all the parameters of (3.4), i.e. to specify a unique state, up to local unitaries, or equivalently, a canonical point in the corresponding orbit. Furthermore, a set of conditions written in term of these invariants can be used in order to detect and compute, given a state, its minimal decomposition in terms of product states built form orthonormal bases.

It has been also analyzed whether this generalization of the bipartite Schmidt decomposition can be applied to higher dimensional systems. Although there have been some results in this direction (see the appendix B and [29]), it is not known how to determine a unique decomposition for any state, what would allow to see whether two states are connected by local unitary transformations. Moreover, let us mention that the number of entanglement parameters grows exponentially with the dimension of the whole

Hilbert space [16]. For higher dimensional systems, almost all the information is nonlocal, and the usefulness of these kind of decompositions seems to be small.

Another approach to the problem of generalizing the Schmidt decomposition is the following: given a state $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$, we look for its minimal decomposition in term of product states, not necessarily orthogonal. In this case, a counting of parameters tells us that at least two product states are needed for specifying a pure three-qubit state. As it is shown in appendix A, this is true for almost every state, i.e. generically any state can be expressed as

$$|\Psi\rangle = \alpha|000\rangle + \beta e^{i\delta}|abc\rangle, \tag{3.6}$$

where α and β are positive numbers, $\langle 0|a\rangle$ can be different from zero, and the same holds for the other two parties. However there is a set of states for which this decomposition is not possible, its minimal decomposition needs three product states. This set corresponds to those pure three-qubit states, apart from separable and biseparable, such that its tangle, $\tau(|\Psi\rangle)$, a function introduced in [31], is zero. The same result was independently obtained by the Innsbruck group [32].

3.3 The single-copy case

The next step in the analysis of the entanglement properties of pure three-qubit states is to enquire into the way these states are connected by local operations and classical communication, in the single-copy case. The answer to this question was given in [32]. There it was proved that, apart from product and biseparable ($A - BC$, $B - AC$ and $C - AB$) states, there are two inequivalent kinds of three-qubit entanglement, the GHZ-type and the W-type. Separable, biseparable and W-type states are of measure zero in the whole space $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$. Separable and biseparable states do not have truly three-qubit entanglement, and they can be detected since not all their local density matrices are of full rank. The states of GHZ-type are those that can be expressed as a sum of two product states (3.6), like the GHZ state (3.1), while the number of product states needed for W-type states is three, i.e. they are those states that have zero tangle (but with local mixed states of full rank).

Given a pure three-qubit state, $|\Psi\rangle$, any state resulting from a sequence of local operations on it can be written as $M_A \otimes M_B \otimes M_C |\Psi\rangle$, where M_i, $i = A, B, C$, is the matrix representing the operations performed by party i. This leads to the simple, but powerful, observation that the minimal number of product states needed for specifying a state, that will be denoted by $n(|\Psi\rangle)$, can not increase under LOCC; actually it is conserved unless the matrices M_i are not invertible. Consider an hypothetic LOCC protocol tranforming a W-state into a GHZ-state, or viceversa. Since the local density matrices of both states have full rank, the local operations connecting them must be invertible. However this transformation is not possible since it would imply a change in $n(|\Psi\rangle)$, which is not allowed if we consider only local invertible matrices. Two separated classes of pure three-qubit entangled states emerge: a state in one class can not be converted by LOCC into any state in the other. Note that in this case, the second approach for the generalization of the Schmidt decomposition has proved to be more useful. While decomposition (3.4) tells us if two pure three-qubit states have the same entanglement, the decomposition (3.6) discriminates between GHZ- and W-type states. The tangle is a useful tool for this distinction too. All the states that, being not product or biseparable, have $n(|\Psi\rangle) = 2$, or $\tau \neq 0$, can be transformed by LOCC into the GHZ state, which is the state of maximum tangle. No GHZ state can be distilled, in the single-copy case, from a W-type state.

3.4 Entanglement in mixed three-qubit states

Entanglement features of pure three-qubit states begin to be understood, in the single-copy case.[3] We know how to determine when two states are equivalent in terms of nonlocality. Apart from separable and biseparable, two inequivalent kinds of truly three-qubit entanglement have appeared, two sets of states that cannot be connected by LOCC, although it is important to take into account that the set of W-type states is of measure zero in $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$.

The aim of the article in appendix C is to generalize part of the known structure for pure states to mixed three-qubit states. Given a mixed state of three qubits, ρ, it would be very useful to know what kinds of entanglement it

[3]The picture is far from being clear in the asymptotic regime, but we do not analyze this situation.

contains. This would also give us necessary conditions for conversions under LOCC. In this sense, it is not difficult to see that, despite the fact that a pure GHZ-type state cannot be exactly transformed into a pure W-type state, we can go as close to it as desired. Thus, an approximated conversion is possible, the higher the fidelity of the approximation, the smaller the probability of success. This approximate transformation however is not allowed in the other direction, i.e. generically, starting from a W-type state, it is not possible to obtain by LOCC a state arbitrarily close to a given GHZ-type state.

In order to extend some of these ideas to the case of density matrices, we define the following classification reflecting the entanglement properties of mixed three-qubit states:

- the class S of separable states, i.e. those that can be expressed as a convex sum of projectors onto product vectors;
- the class B of biseparable states, i.e. those that can be expressed as a convex sum of projectors onto product and bipartite entangled vectors (A-BC, B-AC and C-AB);
- the class W of W-states, i.e. those that can be expressed as a convex sum of projectors onto product, biseparable and W-type vectors;
- the class GHZ of GHZ-states, i.e. the set of all physical states.

All these sets are convex and compact. Separable states do not have quantum correlations, while no truly three-qubit entanglement is required for states in B. The states in $W \setminus B$ have W-type three-qubit entanglement, while all the kinds of entanglement appear for the states in $GHZ \setminus W$. This picture resembles somehow the classification of mixed bipartite states according to their Schmit number [33].

Using techniques already known for bipartite systems, we build some operators, called tripartite entanglement witnesses, that are useful for detecting the position of a state in the classification. We are able to prove that the set $W \setminus B$ is not of measure zero and we conjecture that bound entangled states of three qubits with positive partial transpose respect all the bipartite splittings are not in $GHZ \setminus W$, that is, they do not have GHZ-like correlations.

3.5 An application of the results: quantum correlations in orthopositronium decay

In this section we give an introduction for the article in appendix D. In this work we take profit of the mathematical techniques developed for pure three-qubit states to analyze the quantum correlations of the state resulting from the disintegration of orthopositronium into three photons.

The conflict between local realistic theories and Quantum Mechanics becomes stronger when the statistical predictions of some states of three spin-$\frac{1}{2}$ particles are studied, in particular for the GHZ state (3.1) [25, 26]. Thus, it would be very interesting to find a physical realization of these GHZ-like correlations. We consider particle decays since they seem to be a *natural* source of entangled states. In fact, there have been some recent proposals for testing Bell inequalities in the decay of the Φ-meson into kaons, which are massive particles [34]. In our case, we choose positronium, a bound state of an electron and a positron. Depending on its total spin, it can decay into two or three photons; for spin one (zero) we have the orthopositronium (parapositronium) that decays into three (two) photons. Since the tangle of pure three-qubit states is somehow related to the amount of GHZ-like correlations, we look for the experimental configuration maximizing this function. The polarization pure state resulting from this decay is

$$|\Psi_{op}\rangle = \frac{1}{\sqrt{6}} \left(|001\rangle + |110\rangle + |010\rangle + |101\rangle + |011\rangle + |100\rangle \right). \tag{3.7}$$

The Schmidt-like decompositions introduced in the articles of appendices A and B allow us to write this state in simpler forms that make easier the study of its quantum correlations. We prove that this state shows a contradiction with all the LR theories, since it violates the Mermin inequality of [35]. Furthermore, we demostrate that the conflict between the quantum statistical predictions for the state (3.7) and any LR model is stronger, in the sense of Peres [36], than the obtained for any entangled state of two spin-$\frac{1}{2}$ particles.

3.6 Conclusions

The analysis of the entanglement properties of three-qubit states, either pure or mixed, has been the motivation of the four articles included in appendices A, B, C and D. We have not considered the asymptotic regime, where there is an infinite number of copies of the state, so we have restricted ourselves to the single-copy case. The main results are:

- We have found a canonical decomposition for all pure states $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$, generalizing many of the features of the bipartite Schmidt decomposition. All the information about the nonlocal properties of the state are encoded in the coefficients appearing in this decomposition. In this sense, they are the entanglement coordinates of the state. In particular, using this information, we can see if two states have the same amount of entanglement, i.e. if they can be converted one into another by local unitary transformations.

- We have determined a complete set of polynomial invariants that can specify, in an alternative way, a pure state, up to change of the local bases. The relation between these invariants and the explicit form of the state has been also found.

- We have obtained the minimal decomposition of a pure three-qubit state in terms of product states, and in terms of product states built from orthonormal local bases.

- We have extended the classification of pure three-qubit states given in [32] to the mixed-state case. It is proved that, contrary to what happens for pure states, the defined set of mixed states with W-type entanglement is not of measure zero in the whole space of states. We conjecture that bound entangled states of three qubits with positive partial trasposition do not contain GHZ-like correlations.

- Using these techniques, the quantum correlations of the polarization state resulting from orthopositronium decay into three photons are analyzed. We prove that this state allows, in principle, for a statistical dismissal of local realistic theories stronger than for any entangled state of two spin-$\frac{1}{2}$ particles.

Chapter 4

Quantum state estimation

4.1 Introduction

This chapter is devoted to another important subject in Quantum Information Theory: the estimation of quantum states. It gives an introduction to the following two articles:

- *Optimal generalized quantum measurements for arbitrary spin systems*
  A. Acín, J. I. Latorre and P. Pascual
  Physical Review A **61**, 22113 (2000), quant-ph/9904056.
  See appendix E.

- *Optimal estimation of two-qubit pure-state entanglement*
  A. Acín, R. Tarrach and G. Vidal
  Physical Review A **61**, 62307 (2000), quant-ph/9911008.
  See appendix F.

In all the quantum information processings, data are encoded in quantum states. It is natural to look for the best way in which they can be recovered from these states, i.e. how the information in a state can be decoded. The problem is not trivial, as it is reflected by the analysis of the following example: an unknown state, chosen from a set of two states that are not orthogonal, can not be perfectly determined unless we have an infinite number of copies of it. However, this is not the typical situation and, usually, we deal with a finite number of copies of the unknown state, which has been

chosen from a set of infinite alternatives. In this case, the estimation procedure that behaves better on average must be obtained. First, however, it should be defined in a quite more precise way what "behaves better" means, and this is the scope of the next section.

4.2 The scenario

In this section the usual formulation of the state-estimation problem is presented (see for instance [37]). It will lead us to a function reflecting the degree of optimality of an estimation procedure. Our purpose, then, will be to find the estimation strategy maximizing this quantity.

4.2.1 A priori probability distribution

The state-estimation problem tries to determine the optimal way in which the information encoded in a state can be obtained. Of course, the quantum state we have is not known (since then it will not give us any new information), and a probability distribution takes into account our partial knowledge about it.

Suppose for instance that a vector of parameters $\vec{\theta} = (\theta_1, \ldots, \theta_n)$ is encoded in a pure state, $|\psi(\vec{\theta})\rangle$ (we can also consider the more general case of mixed states). There is a space of possible values for the vector of parameters, Θ, and a measure function on it, $f(\vec{\theta})d\theta_1 \ldots d\theta_n$, reflecting the probability of any point in this space, or alternatively, the probability of the corresponding quantum state. Our aim is to estimate the value of these parameters by determining the quantum state. Note that in this case we have partial information about the unknown state from the beginning, since we know the a priori probability distribution in the space of parameters Θ.

It may happen however that there is no initial information about the unknown state, pure or mixed, to be estimated. Is there any probability distribution over the whole space of physical states reflecting our complete lack of knowledge? The usual assumption in these cases consists on taking all the possibilities equally weighted, i.e. there exists no preferred region in the whole space of events. When there is a finite number, M, of possibilities, this means that the *unbiased* probability distribution is equal to $\vec{p}_0 = (1/M, \ldots, 1/M)$. When the space of events is continuous, this implies

that the initial probability distribution is proportional to the volume element, i.e. to the square root of the determinant of the metric tensor in the space. In the pure-state case, we deal with the space of rays or physical states (pure states without the global phase), where there is a privileged metric, the Fubini-Study metric [38], which is the only one invariant under unitary transformations. From the corresponding volume element, the unbiased probability distribution for pure states is obtained; in the case of spinors it is equal to the isotropic distribution over the Bloch sphere. For mixed states it is not clear whether it is possible to identify a unique metric, although some candidates have been proposed (see [39]). It is worth mentioning here that the two articles in appendices E and F deal only with pure states, so in the rest of this chapter we will just consider this situation.

4.2.2 Measurement and figures of merit

The information about a given unknown state, $|\psi\rangle \in \mathcal{C}^d$, is obviously obtained by performing a measurement over it. The most general measurement in Quantum Mechanics is described by a resolution of the identity in terms of positive operators, the so-called positive-operator valued measurement (POVM) [40], i.e.

$$I = \sum_{i=1}^{r} M_i, \tag{4.1}$$

where r is arbitrary (in particular r can be greater than the dimension of the space) and $M_i \geq 0$. Usually, a finite number of copies, N, of the unknown state are at our disposal, so the most general strategy consists on performing a global measurement over the state given by the tensor product of the N copies, $|\Psi\rangle = |\psi\rangle^{\otimes N} \in \mathcal{C}^{d^N}$. There are r possible outcomes resulting from measuring (4.1) on a quantum state ρ, each with a probability equal to $\mathrm{tr}(\rho M_i)$. In our case, this expression gives

$$p_\psi(i) = \mathrm{tr}\left(|\Psi\rangle\langle\Psi| M_i\right) = \mathrm{tr}(|\psi\rangle\langle\psi|^{\otimes N} M_i). \tag{4.2}$$

After performing the measurement, and depending on the observed result, there is a gain of information about the unknown state. How can this gain of information be quantified? The initial probability distribution of states, $f_I(|\psi\rangle)$, is modified using the Bayes rule and, according to the obtained

outcome $k \in \{1, \ldots, r\}$, the a posteriori probability distribution reads

$$f_P^k(|\psi\rangle) = \frac{\mathrm{tr}(|\psi\rangle\langle\psi|^{\otimes N} M_k) f_I(|\psi\rangle)}{p(k)}, \tag{4.3}$$

where $p(k) = \int d\psi \, \mathrm{tr}(|\psi\rangle\langle\psi|^{\otimes N} M_k) f_I(|\psi\rangle)$ is the probability for outcome k summed over all the initial states. There exist functions in estimation theory that are though of as a measure of the information distance [39] between two probability distributions, $\vec{p}, \vec{q}$, i.e. they are useful in order to express the gain of information when passing from one probability distribution to another. We will denote these functions by $D(\vec{p}, \vec{q})$, and an example of them is the Kullback information distance [41] between two probability distributions, $K(\vec{p}, \vec{q}) = \sum_i p_i \log(p_i/q_i)$. Using these quantities, it is possible to calculte the gain of information averaged over the measurement outcomes,

$$\bar{D} \equiv \sum_{k=1}^{r} p(k) D(f_P^k(|\psi\rangle), f_I(|\psi\rangle)). \tag{4.4}$$

The optimal estimation strategy will consists, then, on designing the measurement, that is, the positive operators M_k appearing in (4.1), that maximize this function. This is the approach that we have applied for the article in appendix F. However this average gain of information is usually not easy to be computed, since the probability distributions of states depend on many parameters and the functions $D(\vec{p}, \vec{q})$ are not simple.

There exists another similar approach that tries to overcome this difficulty: after performing the measurement, we can make a guess, $|\psi^k\rangle$, depending on the outcome k, for the incoming unknown state, $|\psi\rangle$. A fidelity-like function, $F(|\psi^k\rangle, |\psi\rangle)$, measures the degree of similarity between the guess and the initial state. In principle there are many candidates for this fidelity function. It is usually just required to be a concave and symmetric function taking values between zero and one. An average fidelity is defined

$$\bar{F} \equiv \sum_{k=1}^{r} \int d\psi f_I(|\psi\rangle) p_\psi(k) F(|\psi^k\rangle, |\psi\rangle). \tag{4.5}$$

In this case, the optimal estimation strategy consists on the one maximizing $\bar{F}$, i.e. not only the best measurement apparatus, $\{M_k\}$, should be determined, but also the guesses for each of the outcomes. However, in spite of

this two-step optimization, the calculation of expression (4.5) is often quite easier than (4.4), and this fidelity-approach is simpler. Since the fidelity functions should quantify the resemblance between states, they usually have a geometrical meaning: the smaller the fidelity is, the more distant the states are. For the case of pure states, $F(|\phi\rangle, |\psi\rangle)$ is generically chosen to be the overlap between states, $|\langle\phi|\psi\rangle|^2$, as in apppendix E.

4.3 State estimation

In this section we introduce the main results of the article in appendix E about state estimation. The statement of the problem is simple: a finite number of copies, N, of an unknown state, $|\psi\rangle \in \mathcal{C}^d$, are given, and we have to design the optimal estimation strategy, where the optimality criterion takes the overlap between states as fidelity function. Since there is no a priori information about the incoming state (apart from the fact that it is pure), the unbiased probability distribution of pure states describes our knowledge about it. In this case the average fidelity reads

$$\bar{F}_{ps} = \sum_{k=1}^{r} \int d\psi f_I(|\psi\rangle) \operatorname{tr}(|\psi\rangle\langle\psi|^{\otimes N} M_k) \, |\langle\psi^k|\psi\rangle|^2. \tag{4.6}$$

The authors of [42] derived the optimal fidelity, depending on the number of copies, for the case of two-dimensional systems, $d = 2$, and proved that global measurements over the whole state of N copies, $|\Psi\rangle = |\psi\rangle^{\otimes N}$, are better than any adaptative measurement acting separately on each of the copies. Later, the algorithm for constructing the optimal POVM was also provided in [43], and explicit constructions were found in [44], for the case of spin one half. The optimal fidelity for arbitrary dimension is derived in [45], showing an interesting connection between state estimation and cloning. The expression for this optimal fidelity depends on the dimension d of the system and the number N of copies, and is equal to

$$\bar{F}_{ps}^{opt} = \frac{N+1}{N+d}. \tag{4.7}$$

In the article of appendix E, we extend the results of [44] to arbitrary dimension. The incoming state, $|\Psi\rangle = |\psi\rangle^{\otimes N}$, lives in the totally symmetric

subspace of $\mathcal{C}^{d^N}$, therefore, in the search for the optimal measurement it is enough to restrict us to resolutions of the identity in this subspace. We prove that the optimal fidelity (4.7) is achieved by the following estimation strategy: a resolution of the identity in the totally symmetric subspace of N copies, I^N_{sym}, is built by means of projectors onto symmetric product states $|\Psi_k\rangle = |\psi_k\rangle \otimes \cdots \otimes |\psi_k\rangle$, i.e.

$$I^N_{sym} = \sum_{k=1}^{r} c_k^2 |\Psi_k\rangle\langle\Psi_k|, \tag{4.8}$$

where c_k^2 are positive numbers. When the outcome k is obtained after this measurement, we guess $|\psi_k\rangle$ as the unknown state. Shur's lemma guarantees that this measurement is always possible, although with an infinite number of outcomes ($r \to \infty$). However, this is not an interesting solution from a practical point of view, and we look for explicit contructions of optimal and finite POVMs (4.8), extending the techniques used in [44]. A set of equations to be fulfilled by the generalized Bloch vectors of the pure states appearing in the optimal measurement (4.8) is derived. From these equations we can find the explicit form of the pure states and the coefficients appearing in (4.8), or bounds on the number of projectors, r.

4.4 Entanglement estimation

The analysis of the best strategy for the estimation of the entanglement properties of an unknown pure two-qubit state is the scope of the article in appendix F. As it has been shown in chapter two, all the information about bipartite pure-state entanglement is encoded in the Schmidt coefficients, so we do not want to know about all the parameters specifying a state, but we just focus into its Schmidt coefficients. For the case of two qubits, this implies that we want to determine one of the two Schmidt coefficients, being the other fixed by the normalization condition. We concentrate on the estimation of one of the six real numbers that a generic normalized state $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2$, the global phase having been removed, depends on. Indeed, any pure two-qubit state can be parametrized as

$$|\Psi\rangle = \sqrt{\frac{1+b}{2}}|\vec{a}\rangle|\vec{b}\rangle + \sqrt{\frac{1-b}{2}}e^{i\alpha}|-\vec{a}\rangle|-\vec{b}\rangle, \tag{4.9}$$

where $0 \leq b \leq 1$ is the Bloch vector of the reduced density matrix, $\rho_A \equiv \mathrm{tr}_B(|\Psi\rangle\langle\Psi|)$, $|\vec{a}\rangle$ and $|-\vec{a}\rangle$ are its eigenvectors (and the same for B), that are orthogonal, and $0 \leq \alpha \leq 2\pi$ is a phase factor, that is usually absorbed in the definition of $|-\vec{a}\rangle$ or $|-\vec{b}\rangle$. All the nonlocal properties of this state are specified by the value of b, and this simplifies the problem. Indeed, for this case it is not difficult to compute the average gain of information (4.4), where $D(\vec{p},\vec{q})$ is chosen to be the Kullback information distance. The a priori probability distribution for b comes from the unbiased distribution of pure states in $\mathcal{C}^4$.

A finite number of copies, N, of this unknown state are given, and the measurement that gives us more information about b is studied. We consider the most general strategy, i.e. global measurements over $|\Psi\rangle^{\otimes N}$, but it is proved that the optimal strategy can be performed locally by one of the parties without any amount of classical communication. This means that the optimal gain of information about the nonlocal properties of a state can be achieved locally.[1] Intuitively, no information about b is lost when one of the parties is traced out, since it survives in the eigenvalues (or purity) of the resulting density matrix. Indeed, the best measurement is a coarse graining of the optimal measurement for mixed states given in [46], and it is equivalent to the best estimation of the purity of a density matrix.

4.5 Conclusions

State estimation is the main subject of the articles in appendices E and F. While in the first one we consider the estimation of an unknown pure state belonging to a d-dimensional system, i.e. we want to obtain information about all the parameters needed for its specification, in the latter we focus only on one of the features of the unknown pure two-qubit state, its amount of entanglement. The main results are:

- The optimal measurement strategy for the estimation of N copies of a state belonging to a d-dimensional system can be accomplished by means of a resolution of the identity in the symmetric subspace of $\mathcal{C}^{d^N}$

[1] Note however that the local observer, say A, must perform global measurements over the N copies of his reduced state.

built from projectors onto pure product states which are fully symmetric. After the measurement, our guess is equal to the state corresponding to the resulting outcome.

- The introduction of generalized Bloch vectors simplifies the analysis of the conditions to be satisified by the optimal POVM. We show an explicit construction for spin one and two copies.

- The estimation of the entanglement of a pure two-qubit state, i.e. of its Schmidt coefficients, can be attained locally by one of the observers without loosing optimality. It corresponds to the optimal measurement of the mixing of his local density matrix.

Bibliography

[1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47**, 777 (1935).

[2] J. S. Bell, Physics 1, 195 (1964).

[3] A. Aspect, J. Dalibard and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982); W. Tittel, J. Brendel, H. Zbinden and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998), quant-ph/9806043; G. Weihs, T. Jennewein, C. Simon, H. Weinfurter and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998), quant-ph/9810080; M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe and D. J. Wineland, Nature **409**, 791 (2001).

[4] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[5] J. F. Clauser, M. A. Horne, A. Shimony and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[6] N. Gisin, Phys. Lett. A **154**, 201 (1991).

[7] A. K. Ekert, Phys. Rev. Lett. **70**, 661 (1991).

[8] P. W. Shor, Phys. Rev. A **52**, 2493 (1995).

[9] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).

[10] C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).

[11] B. Schumacher, Phys. Rev. A **51**, 2738 (1995).

[12] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[13] K. Kraus, *States, Effects and Operations: Fundamentals Notions of Quantum Theory*, Lectures Notes in Physics **190**, Springer-Verlag, Berlin, 1983.

[14] G. Vidal, J. Mod. Opt. **47**, 355 (2000), quant-ph/9807077.

[15] E. Schmidt, Math. Ann. **63**, 433 (1907); A. Ekert and P. L. Knight, Am. J. Phys. **63**, 415 (1995).

[16] N. Linden and S. Popescu, Fortsch. Phys. **46**, 567 (1998), quant-ph/9711016.

[17] A. Sudbery, J. Phys. A **34**, 643 (2001), quant-ph/0001116.

[18] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999), quant-ph/9811053.

[19] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999), quant-ph/9902033.

[20] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 3566 (1999), quant-ph/9905071.

[21] C. H. Bennett, H. J. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).

[22] S. Popescu and D. Rohrlich, Phys. Rev. A **56**, R3319 (1997), quant-ph/9610044

[23] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223**, 1 (1996), quant-ph/9605038; P. Horodecki, Phys. Lett. A **232**, 333 (1997), quant-ph/9703004.

[24] M. Lewenstein, D. Bruß, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera and R. Tarrach, J. Mod. Opt. **47**, 2481 (2000), quant-ph/0006064.

[25] D. M. Greenberger, M. A. Horne and A. Zeilinger, *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos, Kluwer Academic, Dordrecht, The Netherlands, 1989; D. M. Greenberger, M. A. Horne, A. Shimony and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).

[26] N. Gisin and H. Bechmann-Pasquinucci, Phys. Lett. A **246**, 1 (1998), quant-ph/9804045.

[27] C. H. Bennett, S. Popescu, D. Rohrlich, J. A. Smolin, A. V. Thapliyal, quant-ph/9908073.

[28] A. Peres, Phys. Lett. A **202**, 16 (1995), quant-ph/9504006.

[29] H. A. Carteret, A. Higuchi and A. Sudbery, J. Math. Phys. **41**, 7932 (2000), quant-ph/0006125.

[30] M. Grassl, PhD Thesis, University of Karlsruhe.

[31] V. Coffman, J. Kundu and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000), quant-ph/9907047.

[32] W. Dür, G. Vidal and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000), quant-ph/0005115.

[33] B. M. Terhal and P. Horodecki, Phys. Rev. A **61**, R040301 (2000), quant-ph/9911117; A. Sanpera, D. Bruß and M. Lewenstein, Phys. Rev. A, R03105PRA (2001), quant-ph/0009109.

[34] A. Di Domenico, Nucl. Phys. B **450**, 293 (1995); A. Bramon and M. Nowalowski, Phys. Rev. Lett. **83**, 1 (1999), hep-ph/9811406; B. Ancochea, A. Bramon and M. Nowakowski, Phys. Rev. D **60**, 094008 (1999), hep-ph/9811404; N. Gisin and A. Go, Am. J. Phys. **69**, 264 (2001), quant-ph/0004063.

[35] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).

[36] A. Peres, Fortsch. Phys. **48**, 531 (2000), quant-ph/9905084.

[37] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam (1982).

[38] J. Anandan, Found. Phys. **21**, 1265 (1991).

[39] D. Petz and C. Sudár, J. Math. Phys. **37**, 2662 (1996); A. Lesniewski and M. B. Ruskai, J. Math. Phys. **40**, 5702 (1999), math-ph/9808016.

[40] A. Peres, Found. Phys. **20**, 1441 (1990).

[41] S. Kullback, *Information theory and statistics*, Wiley, New York (1959).

[42] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).

[43] R. Derka, V. Buzek and A. Ekert, Phys. Rev. Lett. **80**, 1571 (1998), quant-ph/9707028.

[44] J. I. Latorre, P. Pascual and R. Tarrach, Phys. Rev. Lett. **81**, 1351 (1998), quant-ph/9803066.

[45] D. Bruß and C. Macchiavello, Phys. Lett. A **253**, 249 (1999), quant-ph/9812016.

[46] G. Vidal, J. I. Latorre, P. Pascual and R. Tarrach, Phys. Rev. A **60**, 126 (1999), quant-ph/9812068.

List of papers

Articles in this thesis

- *Generalized Schmidt decomposition and classification of three-quantum-bit states*
  A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre and R. Tarrach
  Physical Review Letters **85**, 1560 (2000), quant-ph/0003050.
  See appendix A.

- *Three-qubit pure-state canonical forms*
  A. Acín, A. Andrianov, E. Jané and R. Tarrach
  Submitted to Journal of Physics A, special issue on Quantum Information, quant-ph/0009107.
  See appendix B.

- *Classification of mixed three-qubit states*
  A. Acín, D. Bruss, M. Lewenstein and A. Sanpera
  Submitted to Physical Review Letters, quant-ph/0103025.
  See appendix C.

- *Three-party entanglement from positronium*
  A. Acín, J. I. Latorre and P. Pascual
  Physical Review A **63**, 042107 (2001), quant-ph/0007080.
  See appendix D.

- *Optimal generalized quantum measurements for arbitrary spin systems*
  A. Acín, J.I. Latorre and P. Pascual
  Physical Review A **61**, 22113 (2000), quant-ph/9904056.
  See appendix E.

- *Optimal estimation of two-qubit pure-state entanglement*
  A. Acín, R. Tarrach and G. Vidal
  Physical Review A **61**, 62307 (2000), quant-ph/9911008.
  See appendix F.

Articles not included in this thesis

- *Optimal distillation of a GHZ state*
  A. Acín, E. Jané, W. Dür and G. Vidal
  Physical Review Letters **85**, 4811 (2000), quant-ph/0007042.

- *Optimal estimation of quantum dynamics*
  A. Acín, E. Jané and G. Vidal
  Submitted to Physical Review Letters, quant-ph/0012015.

- *Statistical distinguishability between unitary operations*
  A. Acín
  Submitted to Physical Review Letters, quant-ph/0102064.

Appendices

Appendix A

Generalized Schmidt Decomposition and Classification of Three-Quantum-Bit States

A. Acín,[1] A. Andrianov,[1,3] L. Costa,[2] E. Jané,[1,*] J. I. Latorre,[1] and R. Tarrach[1]

[1]*Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain*
[2]*Departament d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via Corts Catalanes 585, E-08007 Barcelona, Spain*
[3]*Department of Theoretical Physics, St. Petersburg State University, 198904, St. Petersburg, Russia*

(Received 24 March 2000)

We prove for any pure three-quantum-bit state the existence of local bases which allow one to build a set of five orthogonal product states in terms of which the state can be written in a unique form. This leads to a canonical form which generalizes the two-quantum-bit Schmidt decomposition. It is uniquely characterized by the five entanglement parameters. It leads to a complete classification of the three-quantum-bit states. It shows that the right outcome of an adequate local measurement always erases all entanglement between the other two parties.

PACS numbers: 03.67.–a, 03.65.Bz

The Schmidt decomposition [1,2] allows one to write any pure state of a bipartite system as a linear combination of biorthogonal product states or, equivalently, of a nonsuperfluous set of product states built from local bases. For two quantum bits (qubits) it reads

$$|\Psi\rangle = \cos\theta|00\rangle + \sin\theta|11\rangle, \qquad 0 \le \theta \le \pi/4. \quad (1)$$

Here $|ii\rangle \equiv |i\rangle_A \otimes |i\rangle_B$, both local bases $\{|i\rangle\}_{A,B}$ depend on the state $|\Psi\rangle$, the relative phase has been absorbed into any of the local bases, and the state $|00\rangle$ has been defined by carrying the larger (or equal) coefficient. A larger value of θ means more entanglement. The only entanglement parameter, θ, plus the hidden relative phase, plus the two parameters which define each of the two local bases are the six parameters of any two-qubit pure state, once normalization and global phase have been disposed of.

Very many results in quantum information theory have been obtained with the help of the Schmidt decomposition: its simplicity reflects the simplicity of bipartite systems as compared to N-partite systems. Much of its usefulness comes from it not being superfluous: to carry one entanglement parameter one needs only two orthogonal product states built from local bases states, no more, no less.

The aim of this work is to generalize the Schmidt decomposition of (1) to three qubits. It is well known [2] that its straightforward generalization, that is, in terms of triorthogonal product states, is not possible (see also [3]). Nevertheless, having a minimal canonical form in which to cast any pure state, by performing local unitary transformations, will provide a new tool for quantifying entanglement for three qubits, a notoriously difficult problem. It will lead to a complete classification of exceptional states which, as we will see, is much more complex than in the two-qubit case. The generalization to N quantum dits (d-state systems) is not completely straightforward and will be given elsewhere.

Linden and Popescu [4] and Schlienz [5] showed that for any pure three-qubit state the number of entanglement parameters is five and, using repeatedly the two-qubit Schmidt decomposition, proved the existence for any pure state of a reference form in terms of six orthogonal product states built from local bases. The five entanglement parameters are one phase (all others can be absorbed) and four moduli of the six coefficients, so that a further constraint beyond the normalization exists. In other words, exactly as (1) shows that local unitary transformations allow one to make two of the four components vanish (corresponding to $|01\rangle$ and $|10\rangle$) for a two-qubit pure state, Linden and Popescu and Schlienz proved that, also for a three-qubit system two of the, now eight, components can be made zero. However, the set of six states is superfluous in the sense that its coefficients require a constraint to lead to a unique representative of any pure state. It is not clear whether this is the best one can do, i.e., whether the set is minimal. We will now prove that indeed, combining adequately the local changes of bases corresponding to $U(1) \times SU(2) \times SU(2) \times SU(2)$ transformations, one can always do with five terms, which precisely can carry only five entanglement parameters, leading thus to a nonsuperfluous unique representation.

Notice that a straightforward counting of parameters shows that a nonsuperfluous set will have five states, i.e., three vanishing coefficients. There exist three inequivalent sets of five local bases product states

$$\begin{aligned} &\{|000\rangle, |001\rangle, |010\rangle, |100\rangle, |111\rangle\}, \\ &\{|000\rangle, |001\rangle, |110\rangle, |100\rangle, |111\rangle\}, \\ &\{|000\rangle, |100\rangle, |110\rangle, |101\rangle, |111\rangle\}. \end{aligned} \quad (2)$$

Whereas the first set is symmetric under permutation of parties, the other two are not.

The nonequivalence of the three sets follows from the different degrees of orthogonality between the five states within each set. One can also readily check that all three sets can carry exactly five entanglement parameters, four moduli, and one phase, and are thus nonsuperfluous. This is of course no proof that any state can always be written as a linear combination of the five states of one and the same

 0031-9007/00/85(7)/1560(4)$15.00

set. We will now prove that it can always be done for the last two sets, or their versions obtained by permuting parties.

As an introduction let us first present a one-line proof of the Schmidt decomposition of a two-qubit state, Eq. (1). Writing any state in a basis of product states built from any two local bases,

$$|\Psi\rangle = \sum_{i,j} t_{ij}|ij\rangle , \tag{3}$$

calling T the matrix of elements t_{ij}, and recalling that for any T there always exist two unitary matrices which diagonalize it,

$$U_1 T U_2 = D , \tag{4}$$

the Schmidt decomposition follows at once. Note that U_1 and U_2 correspond to the local basis changes necessary for casting the original state into its Schmidt form.

For a three-qubit state the proof goes as follows: from

$$|\Psi\rangle = \sum_{i,j,k} t_{ijk}|ijk\rangle , \tag{5}$$

one introduces the matrices T_0 and T_1 with elements

$$(T_i)_{jk} \equiv t_{ijk} . \tag{6}$$

Consider now the unitary transformation on the first qubit,

$$T_i' = \sum_j u_{ij} T_j , \tag{7}$$

such that

$$\det T_0' = 0 . \tag{8}$$

Notice that (8) has always two solutions. The matrix obtained from T_0' after diagonalization following (4), which corresponds to unitary transformations on the last two qubits, has at least three zeros,

$$(D_0')_{01} = (D_0')_{10} = (D_0')_{11} = 0 . \tag{9}$$

This finishes the proof that any pure state of three qubits can always be written as a linear superposition of the five states of the last set of (2).

The generalization to three qubits of the Schmidt decomposition, i.e., one more zero for one more qubit, thus reads

$$|\Psi\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\varphi}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle \qquad \lambda_i \geq 0,\ 0 \leq \varphi \leq \pi,\ \mu_i \equiv \lambda_i^2,\ \sum_i \mu_i = 1 , \tag{10}$$

where we have chosen the second coefficient to carry the only relevant phase, whose range, to be proven later, is also given. Notice that we have singled out party A in obtaining (10), but we could have chosen any of the three parties.

An immediate and important consequence of this decomposition is that there always exists for any state $|\Psi\rangle$ and any (genderless) party X a state $|0\rangle_X$ such that ${}_X\langle 0|\Psi\rangle$ is a product state of the other two parties (unless party X is not entangled with the other two parties). That is, party X, knowing $|\Psi\rangle$, can perform a local measurement which, for one outcome, allows it to be sure that the other two parties share no entanglement whatsoever. Note that when (8) displays two different solutions, two such states exist. This property suggests some applications to quantum information processing. It also leads to an efficient algorithm for computing the λ's and φ.

There is one small hitch left: as (8) has generically two different solutions, any state can be written in the form of (10) with two different sets of coefficients. Let us dispose generically of this redundancy. Recall that after diagonalization of T_0' we are left with the matrices

$$M_0 \equiv D_0' = \begin{pmatrix} \lambda_0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad M_1 = \begin{pmatrix} e^{i\varphi}\lambda_1 & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}, \tag{11}$$

for one solution of Eq. (8) and

$$\tilde{M}_0 = \begin{pmatrix} \tilde{\lambda}_0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \tilde{M}_1 = \begin{pmatrix} e^{i\tilde{\varphi}}\tilde{\lambda}_1 & \tilde{\lambda}_2 \\ \tilde{\lambda}_3 & \tilde{\lambda}_4 \end{pmatrix}, \tag{12}$$

for the other solution. Of course, both solutions can be related by a U(1) × SU(2) × SU(2) × SU(2) transformation:

$$\begin{aligned} \tilde{M}_0 &= e^{i\omega} U_1 (u_{00} M_0 + u_{01} M_1) U_2 , \\ \tilde{M}_1 &= e^{i\omega} U_1 (-u_{01}^* M_0 + u_{00}^* M_1) U_2 , \end{aligned} \tag{13}$$

and the inverse

$$\begin{aligned} M_0 &= e^{-i\omega} U_1^\dagger (u_{00}^* \tilde{M}_0 - u_{01} \tilde{M}_1) U_2^\dagger , \\ M_1 &= e^{-i\omega} U_1^\dagger (u_{01}^* \tilde{M}_0 + u_{00} \tilde{M}_1) U_2^\dagger . \end{aligned} \tag{14}$$

The condition $\det M_0 = \det \tilde{M}_0 = 0$ leads to

$$u_{00} = -\frac{\det M_1}{\lambda_0 \lambda_4} u_{01} \qquad u_{00}^* = \frac{\det \tilde{M}_1}{\tilde{\lambda}_0 \tilde{\lambda}_4} u_{01} . \tag{15}$$

It is tedious, but straightforward, to solve the previous equations. Here we need only the following results:

$$\lambda_0 \lambda_4 = \tilde{\lambda}_0 \tilde{\lambda}_4, \qquad u_{01}^* = -u_{01} , \tag{16}$$

which, from Eq. (15), imply

$$\det M_1 = (\det \tilde{M}_1)^* . \tag{17}$$

From here it follows that

$$\begin{aligned} 0 < \varphi < \pi \Leftrightarrow \pi < \tilde{\varphi} < 2\pi , \\ 0 < \tilde{\varphi} < \pi \Leftrightarrow \pi < \varphi < 2\pi . \end{aligned} \tag{18}$$

so that one can always choose the solution for which

$$0 \leq \varphi \leq \pi , \tag{19}$$

which explains the range of φ given in Eq. (10).

Let us mention here that by performing a unitary transformation on the third qubit,

$$|0'\rangle = \frac{1}{\sqrt{\mu_1 + \mu_2}} (\lambda_1 e^{i\varphi}|0\rangle + \lambda_2|1\rangle) , \tag{20}$$

the decomposition for the second set of (2) is obtained. In the remainder we will use the first decomposition (10), which is physically and mathematically more convenient.

A generalization of the Schmidt decomposition is thus given by (10); any state can be written in this minimal form, generically in a unique way. The explicit algorithm for constructing this canonical form follows from the set of Eqs. (5)–(8). However, particular states can be obtained for different values of the five entanglement parameters. It is thus useful to have five independent invariants for the classification of states which we will obtain from (10). We will take here the five minimal polynomial invariants of [6].

Defining $\Delta \equiv |\lambda_1\lambda_4 e^{i\varphi} - \lambda_2\lambda_3|^2$ we find

$$\begin{aligned}
&\tfrac{1}{2} \le I_1 \equiv \mathrm{Tr}\rho_A^2 = 1 - 2\mu_0(1 - \mu_0 - \mu_1) \le 1\,,\\
&\tfrac{1}{2} \le I_2 \equiv \mathrm{Tr}\rho_B^2 = 1 - 2\mu_0(1 - \mu_0 - \mu_1 - \mu_2)\\
&\qquad - 2\Delta \le 1\,,\\
&\tfrac{1}{2} \le I_3 \equiv \mathrm{Tr}\rho_C^2 = 1 - 2\mu_0(1 - \mu_0 - \mu_1 - \mu_3)\\
&\qquad - 2\Delta \le 1\,,\\
&\tfrac{1}{4} \le I_4 \equiv \mathrm{Tr}(\rho_A \otimes \rho_B\rho_{AB})\\
&\qquad = 1 + \mu_0(\mu_2\mu_3 - \mu_1\mu_4 - 2\mu_2 - 3\mu_3 - 3\mu_4)\\
&\qquad - (2 - \mu_0)\Delta \le 1\,,\\
&0 \le I_5 \equiv |\mathrm{Hdet}(t_{ijk})|^2 = \mu_0^2\mu_4^2 \le \tfrac{1}{16}\,,
\end{aligned} \tag{21}$$

where

$$\begin{aligned}
\rho_{AB} &\equiv \mathrm{Tr}_C|\Psi\rangle\langle\Psi| \qquad \rho_C \equiv \mathrm{Tr}_{AB}|\Psi\rangle\langle\Psi|\\
\rho_A &\equiv \mathrm{Tr}_B\rho_{AB} \qquad \rho_B \equiv \mathrm{Tr}_A\rho_{AB}\,,
\end{aligned} \tag{22}$$

and Cayley's hyperdeterminant, $\mathrm{Hdet}(t_{ijk})$, can be found in [7] and corresponds to the three-tangle of [6,8].

Although these five invariants are computationally simple and physically meaningful, as they give local information, it can be convenient to trade them, recalling $\sum_i \mu_i = 1$, for algebraically simpler ones:

$$\begin{aligned}
0 \le J_1 &\equiv \Delta \le \tfrac{1}{4}\,,\\
0 \le J_2 &\equiv \mu_0\mu_2 \le \tfrac{1}{4}\,,\\
0 \le J_3 &\equiv \mu_0\mu_3 \le \tfrac{1}{4}\,,\\
0 \le J_4 &\equiv \mu_0\mu_4 \le \tfrac{1}{4}\,,\\
J_5 &\equiv \mu_0(\Delta + \mu_2\mu_3 - \mu_1\mu_4)\,.
\end{aligned} \tag{23}$$

The invariants J_4 and J_5 are symmetric under permutation of parties, while $J_1(J_2, J_3)$ is symmetric under exchange of parties B and C (A and C, A and B).

We can now proceed with the complete classification of nongeneric three-qubit states with the help of Eqs. (10) and (23):

Type 1 (product states): $J_i = 0$ for $i = 1, 2, 3, 4, 5$.

Type 2a (biseparable states): $J_i = 0$ except $J_1(J_2, J_3)$ when party $A(B, C)$ is not entangled with the other two parties. They carry only bipartite entanglement and depend on one parameter.

Type 2b (generalized GHZ states): $J_i = 0$ except J_4. They include the standard GHZ states [9] and depend on one parameter.

Type 3a (tri-Bell states): $\mu_1 = \mu_4 = 0$. It implies $J_4 = 0$, $J_1J_2 + J_1J_3 + J_2J_3 = \sqrt{J_1J_2J_3} = \frac{J_5}{2}$. They depend on two parameters.

Type 3b (extended GHZ states): $\mu_j = \mu_k = 0$, for $j, k \in \{1, 2, 3\}$ and $j \neq k$. It implies $J_j = J_k = J_5 = 0$. They depend on two parameters and correspond to the slice states of [10].

Type 4a: $\mu_4 = 0$. It follows $J_4 = 0$ and $\sqrt{J_1J_2J_3} = \frac{J_5}{2}$. They depend on three parameters.

Type 4b: $\mu_2 = 0$ ($\mu_3 = 0$). Then, $J_2 = J_5 = 0$ ($J_3 = J_5 = 0$). They depend on three parameters.

Type 4c: $\mu_1 = 0$. Then, $J_1(J_2 + J_3 + J_4) + J_2J_3 = \sqrt{J_1J_2J_3} = \frac{J_5}{2}$ and they depend on three parameters.

Notice that the type number indicates how many of the five states of (10) characterize the states of that type. Because of the asymmetric character of the decomposition (10), some of the states included in type 5 can be written in terms of four states, had we singled out party B or C [11]. Notice also that, in some sense, the J_i's are indicators of entanglement: only when all of them vanish there is no entanglement at all, $J_1(J_2, J_3)$ indicate bipartite entanglement, and J_4 indicates GHZ entanglement.

Let us further exploit our previous results. An alternative generalization of the Schmidt decomposition could be writing the state as a superposition of two nonorthogonal product states which are not built from local bases,

$$|\Psi\rangle = \alpha|abc\rangle + \beta|a'b'c'\rangle\,, \tag{24}$$

with α and β real.

Beside the trivial cases of type-1 and type-2a states, this decomposition is always possible except for a familly of states depending on three parameters [12]. Our decomposition allows one to reproduce this result and shows that (24) is not possible when $I_5 = 0$ (corresponding to type-3a and type-4a states). It can be proved that when $I_5 = 0$ the two solutions of (8) coincide. The same happens had we chosen to single out any of the other parties. Therefore, for any party X, there is only one state $|0\rangle_X$ such that ${}_X\langle 0\,|\,\Psi\rangle$ is a product state of the other two parties. Since (24) implies two such states, e.g., $|a_\perp\rangle_A$ and $|a'_\perp\rangle_A$, it follows that type-3a and type-4a states cannot be written as a sum of two nonorthogonal product states. When the decomposition (24) is possible, our results give the constructive method to obtain it. From (10), the second coefficient can be split into two terms,

$$|\Psi\rangle = \left(\lambda_0|000\rangle + \frac{\lambda_1\lambda_4 e^{i\varphi} - \lambda_2\lambda_3}{\lambda_4}|100\rangle\right) + \left(\frac{\lambda_2\lambda_3}{\lambda_4}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle\right). \tag{25}$$

It is easy to see that (25) corresponds to the sum of two nonorthogonal product states as (24) with coefficients

$$\alpha = \frac{1}{\lambda_4}\sqrt{J_1 + J_4}, \qquad \beta = \frac{1}{\lambda_4}\sqrt{\mu_2\mu_3 + \mu_4(\mu_4 + \mu_2 + \mu_3)}. \tag{26}$$

This decomposition is unique. The states that appear in (24) are orthogonal to the ones that allow each party to destroy the entanglement between the other two parties with some nonvanishing probability.

A final consequence of (10) is that, by using the bipartite Schmidt decomposition, any pure state can be written as a superposition of a product state and a biseparable state, i.e.,

$$|\Psi\rangle = \cos\theta|000\rangle + \sin\theta|1\rangle(\cos\omega|0'0''\rangle + \sin\omega|1'1''\rangle), \tag{27}$$

which is the minimal decomposition in terms of orthogonal product states. It exhibits explicitly two of the five entanglement parameters. The other three are hidden in the moduli of the scalar products $\langle 0|0'\rangle$ and $\langle 0|0''\rangle$, and in one phase absorbed by one of the local bases. It is also a nonsuperfluous form, though not built from local bases.

In this work we have found the minimal decomposition of any pure three-qubit state in terms of orthogonal product states built from local bases. It generalizes the Schmidt decomposition and leads to a complete classification of pure three-qubit states, which fine grains the fully inseparable states class of the general entanglement classification of mixed three-qubit states [13]. Our decomposition shows that any party can, performing a clever local measurement, kill the entanglement between the other two parties with nonvanishing probability. A decomposition in terms of the minimal number of orthogonal product states has also been found.

Finally, we have explored whether a pure three-qubit state can be written as a sum of two nonorthogonal product states, which can be thought of as an alternative generalization of the Schmidt decomposition. We have verified that only a subfamily depending on three parameters cannot be expressed in this form [12], corresponding to states with $I_5 = 0$.

The authors thank Guifré Vidal and Sandu Popescu for useful discussions. J. I. L. and R. T. acknowledge financial support by CICYT Project No. AEN 98-0431, CIRIT Project No. 1998SGR-00026, and CEC Project No. IST-1999-11053, A. Andrianov by RFBR 99-01-00736 and CIRIT, PIV-2000, L. C. by PB97-0893, and A. Acín and E. J. by a grant from MEC (AP98 and AP99). Financial support from the ESF is also acknowledged.

*Email address: ejane@ecm.ub.es

[1] E. Schmidt, Math. Ann. **63**, 433 (1907); A. Ekert and P. L. Knight, Am. J. Phys. **63**, 415 (1995).
[2] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academic Publishers, Dordrecht, 1995); A. Peres, Phys. Lett. A **202**, 16 (1995).
[3] A. V. Thapliyal, Phys. Rev. A **59**, 3336 (1999); A. K. Pati, quant-ph/9911073.
[4] N. Linden and S. Popescu, Fortschr. Phys. **46**, 567 (1998).
[5] J. Schlienz and G. Mahler, Phys. Lett. A **224**, 39–44 (1996).
[6] A. Sudbery, quant-ph/0001116.
[7] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants* (Birkhäuser, Boston, 1994). Its explicit form is $\mathrm{Hdet}(t_{ijk}) = t_{000}^2 t_{111}^2 + t_{001}^2 t_{110}^2 + t_{010}^2 t_{101}^2 + t_{100}^2 t_{011}^2 - 2(t_{000}t_{111}t_{011}t_{100} + t_{000}t_{111}t_{101}t_{010} + t_{000}t_{111}t_{110}t_{001} + t_{011}t_{100}t_{101}t_{010} + t_{011}t_{100}t_{110}t_{001} + t_{101}t_{010}t_{110}t_{001}) + 4(t_{000}t_{110}t_{101}t_{011} + t_{111}t_{001}t_{010}t_{100})$.
[8] V. Coffman, J. Kundu, and W. K. Wootters, quant-ph/9907047.
[9] D. M. Greenberger, M. A. Horne, and A. Zeilinger, Phys. Today **46**, No. 8, 24 (1993).
[10] H. A. Carteret and A. Sudbery, quant-ph/0001091.
[11] A. Acín, A. Andrianov, E. Jané, J. I. Latorre, and R. Tarrach (to be published).
[12] J. I. Cirac, W. Dür, and G. Vidal, quant-ph/0005115.
[13] W. Dür, J. I. Cirac, and R. Tarrach, Phys. Rev. Lett. **83**, 3562 (1999).

Appendix B

Three-qubit pure-state canonical forms

A. Acín[†], A. Andrianov[†*], E. Jané[†] and R. Tarrach[†]
[†] *Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain.*
[*] *Department of Theoretical Physics, St. Petersburg State University, 198904, St. Petersburg, Russia.*
e-mail: acin@ecm.ub.es
(April 6, 2001)

In this paper we analyze the canonical forms into which any pure three-qubit state can be cast. The minimal forms, i.e. the ones with the minimal number of product states built from local bases, are also presented and lead to a complete classification of pure three-qubit states. This classification is related to the values of the polynomial invariants under local unitary transformations by a one-to-one correspondence.

PACS Nos. 03.67.-a, 03.65.Bz

I. INTRODUCTION

Non-local quantum correlations or entanglement between space-separated parties is one of the most fertile and thought-generating properties of quantum mechanics. Recently it has become a very useful resource for many of the applications in quantum information theory and this has led to a lot of work devoted to understanding how it can be quantified and manipulated.

Bipartite pure state entanglement is almost completely understood, while many questions are still open for the mixed state case. For pure states, the Schmidt decomposition [1] has proven to be a very useful tool, since it allows to write any pure state shared by two parties A and B in a canonical form, where all the information about the non-local properties of the state is contained in the positive Schmidt coefficients. The non-local properties of quantum states can be also specified by means of other quantities invariant under the action of local unitary transformations. An interesting type of these invariants are given by polynomial combination of the coordinates of the state in a product basis, and the relation between these invariants and the Schmidt coefficients is well known.

Some novel aspects, compared to the bipartite case, appear for entangled systems of more than two parties. In this work we study the canonical forms of three-qubit pure states, extending the results of bipartite systems. First we analyze the forms proposed for generalizing the Schmidt decomposition for three-qubit pure states. Then, we relate one of these decompositions to the polynomial invariants studied in [2–9]. We give a one-to-one correspondence between a canonical form for a three-qubit pure state and a complete set of polynomial invariants describing its entanglement properties. We also classify the different types of canonical forms by means of the minimal number of local bases product states (LBPS), i.e. the minimal number of non-local parameters, needed for the specification of a state. For any three-qubit pure state we give its decomposition with the minimal number of LBPS and the procedure that has to be applied in order to build it. Finally we indicate how to generalize the results to systems of N-qubits, where many difficulties arise.

II. GENERALIZATION OF THE SCHMIDT DECOMPOSITION

The Schmidt decomposition has been a very useful tool for the study of entanglement properties of bipartite systems. For a generic bipartite pure state $|\Phi\rangle \in \mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2}$ it reads

$$|\Phi\rangle = \sum_{i=1}^{l} \alpha_i |ii\rangle, \quad \alpha_i \geq 0, \tag{1}$$

where $l = \min(d_1, d_2)$, $|ii\rangle \equiv |i\rangle_A \otimes |i\rangle_B$, being $|i\rangle$ orthonormal vectors in each subsystem, and α_i are the Schmidt coefficients. It would be very interesting to find for three-qubit pure states a canonical decomposition generalizing the features of the Schmidt decomposition. However, the trivial generalization is not possible [10] and it is not evident how to extend the Schmidt decomposition to the case of N-party systems ($N > 2$). Indeed several forms have been proposed (see for instance [11]).

In recent work [9] we gave a generalization of the Schmidt decomposition for three-qubit pure states, in the sense that the coefficients of this decomposition carry all the information about the non-local properties of the state, and do so minimally and unambiguously, i.e. the decomposition is not superflous. Starting from a generic state shared by three parties, A, B and C,

$$|\Psi\rangle = \sum_{i,j,k} t_{ijk} |ijk\rangle, \tag{2}$$

where $|ijk\rangle \equiv |i\rangle_A \otimes |j\rangle_B \otimes |k\rangle_C$, we look for the local bases that allow to write (2) with the minimal number of LBPS. A simple counting of parameters shows that at least five product states built from local bases are needed in order to specify a generic state belonging to $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$. There

are three inequivalent classes of five LBPS: the first one is the symmetric set

$$\{|000\rangle, |001\rangle, |010\rangle, |100\rangle, |111\rangle\}, \tag{3}$$

the second is weakly asymmetric and corresponds to the three sets of states,

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

and the third one is strongly asymmetric, and corresponds to the three sets

$$\begin{aligned} &\{|000\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\} \\ &\{|000\rangle, |010\rangle, |011\rangle, |110\rangle, |111\rangle\} \\ &\{|000\rangle, |001\rangle, |110\rangle, |101\rangle, |111\rangle\}, \end{aligned} \tag{5}$$

where the three sets of states of (4) are related by permutation of the parties, and the same happens for the sets (5). The non-equivalence between the sets (3), (4) and (5) follows from the different degrees of orthogonality between the five states within each set (see figure 1). In [9] it was proved that any three-qubit state can be written in terms of the product states of any of the asymmetric sets. Let us sketch the procedure.

Starting from a generic state (2), one introduces the matrices T_0 and T_1 with elements

$$(T_i)_{jk} \equiv t_{ijk}. \tag{6}$$

A change of basis on the first qubit transforms these matrices in the following way,

$$\begin{aligned} T_0' &= u_{00}^A T_0 + u_{01}^A T_1 \\ T_1' &= u_{10}^A T_0 + u_{11}^A T_1, \end{aligned} \tag{7}$$

where u_{ij}^A are the elements of a unitary matrix, while the effect of a change of basis in B (C) implies that each T_i is left (right) multiplied by a unitary matrix $U^B (U^C)$. The unitary transformation on party A is chosen such that

$$\det(T_0') = 0. \tag{8}$$

There are always two solutions for this equation since (8) is equivalent to

$$\det(T_0 + xT_1) = 0, \tag{9}$$

where $x \equiv \frac{u_{01}^A}{u_{00}^A}$ is an unbounded complex number. Now we apply two unitary matrices on parties B and C in order to diagonalize T_0'. These operations lead to the matrices

$$\begin{aligned} M_0 \equiv U^B T_0' U^C &= \begin{pmatrix} \lambda_0 & 0 \\ 0 & 0 \end{pmatrix} \\ M_1 \equiv U^B T_1' U^C &= \begin{pmatrix} \lambda_1 e^{i\varphi} & \lambda_2 \\ \lambda_3 & \lambda_4 \end{pmatrix}, \end{aligned} \tag{10}$$

where λ_i are real and positive, since all the phases have been absorbed by phase redefinitions of $|0\rangle_A$, $|1\rangle_A$, $|1\rangle_B$ and $|1\rangle_C$. By means of these unitary transformations we have been able to write the initial state (2) in terms of the products states appearing in the first set of (5), i.e.

$$|\Psi\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\varphi}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle. \tag{11}$$

Equation (9) has generically two different solutions, x and $\bar{x}$, so two different decompositions (11) are possible for the same state $|\Psi\rangle$. By limiting the range of the phase factor to $0 \leq \varphi \leq \pi$ a unique solution is found when $0 < \varphi < \pi$ (see [9] for more details), and then we have a unique canonical form in which to cast almost any three-qubit pure state. For the remaining ones, when $\varphi = 0, \pi$, two canonical forms exist in general; we will break this remaining degeneracy taking, for instance, the form with the smallest λ_1, or, if λ_1 is unique, taking the form with the smallest λ_0. It is important also to note that we have singled out party A in obtaining (11), but we could have chosen any of the three parties.

From (11) and by applying a unitary transformation on the third qubit,

$$|0'\rangle = \frac{1}{\sqrt{\lambda_1^2 + \lambda_2^2}} \left(\lambda_1 e^{i\varphi}|0\rangle + \lambda_2|1\rangle\right) \tag{12}$$

it follows that any state can be written, after removing the phases of four of the coefficients, as,

$$|\Psi\rangle = \eta_0 e^{i\phi}|000\rangle + \eta_1|001\rangle + \eta_2|100\rangle + \eta_3|110\rangle + \eta_4|111\rangle, \tag{13}$$

with η_i real and positive, which corresponds to the first set in (4).

Recently, it has been shown [12] that the symmetric decomposition using the set of states (3) is also possible. The proof is based on the fact that if a given state $|\Psi\rangle$ is written in a basis such that the state $|111\rangle$ is the one that maximizes the overlap of $|\Psi\rangle$ with any product state, i.e.

$$|t_{111}|^2 = \max |\langle\Psi|\alpha\beta\gamma\rangle|^2, \tag{14}$$

the coefficients t_{110}, t_{101} and t_{011} must be zero (otherwise one could find a product state with a larger overlap). Therefore any state can be written as

$$|\Psi\rangle = \kappa_0 e^{i\theta}|000\rangle + \kappa_1|001\rangle + \kappa_2|010\rangle + \kappa_3|100\rangle + \kappa_4|111\rangle, \tag{15}$$

with κ_i real and positive and $0 \leq \theta < \pi$. Nevertheless, the conditions under which the decomposition (15) is unique are not known.

A different decomposition, which can also be thought as an alternative generalization of the Schmidt decomposition for three-qubit states, could be writing the state

as a superposition of two product states, not necessarily orthogonal,

$$|\Psi\rangle = \alpha|000\rangle + \beta e^{i\delta}|\varphi_1\varphi_2\varphi_3\rangle, \tag{16}$$

with α and β positive real numbers. This decomposition is only possible when $J_4 \neq 0$ (see below for the definition of J_4) [9,13], which corresponds to the GHZ-class in [13], and it has been proved very useful for the obtention of the optimal GHZ distillation protocol [14].

III. THE SET OF POLYNOMIAL INVARIANTS

The space of states of three qubits is $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$, which depends on sixteen real parameters (including the norm and the global phase). Two states, $|\Psi_1\rangle$ and $|\Psi_2\rangle$, are equivalent, as far as their entanglement properties are concerned, when they can be transformed one into the other by local unitary transformations. Therefore the action of the elements of the group $U(1) \times SU(2) \times SU(2) \times SU(2)$ define orbits in the space of states, each orbit being the equivalence class of all the states having the same non-local properties. Thus, and as it is well-known, the dimension of a generic orbit for the case of three-qubit pure states is ten [2], so six entanglement parameters should be enough to discriminate between two different orbits. Since the decomposition (11) is unique, it gives six quantities invariant under local unitaries, the five coefficients λ_i and the phase φ, which allow us to check whether two generic states belong to the same orbit, i.e. whether they can be connected applying local unitary transformations. These parameters can be thought of as the entanglement coordinates. An alternative, though two-fold degenerate, set of entanglement parameters is given by polynomial combinations of the coefficients t_{ijk} which are invariant under the group of local unitaries [2–8]. In this section decomposition (11) will be related to these polynomial invariants.

For bipartite pure states, $|\Phi\rangle \in \mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2}$, a complete set of polynomial invariants, which allows to know whether two bipartite states have the same entanglement properties, is given by

$$\mathrm{tr}(\rho_A^l) = \mathrm{tr}(\rho_B^l) \quad l = 1, ..., \min(d_1, d_2), \tag{17}$$

where $\rho_A \equiv \mathrm{tr}_B|\Phi\rangle\langle\Phi|$ and $\rho_B \equiv \mathrm{tr}_A|\Phi\rangle\langle\Phi|$ are the local density matrices. Since the eigenvalues of these matrices correspond to the square of the Schmidt coefficients (1), we know the relation between the polynomial invariants and the Schmidt decomposition [7].

As it has been mentioned above, the space of entanglement parameters of pure three-qubit states has dimension equal to six, so at least six linearly independent polynomial combinations of t_{ijk} invariant under local unitary transformations are needed in order to specify the non-local properties of a state, or the orbit which it belongs to. In [7] the six linearly independent polynomial invariants of minimal degree were found. The norm is a trivial one, so we will not consider it and in the rest of the paper we will restrict ourselves to the space of normalized states, the number of non-local parameters being reduced to five. This implies that we have $\sum_i \lambda_i^2 = 1$ in (11). Apart from the norm, the polynomial invariants given in [7] are

$$\begin{aligned}
&\frac{1}{2} \leq I_1 \equiv \mathrm{tr}(\rho_A^2) \leq 1 \\
&\frac{1}{2} \leq I_2 \equiv \mathrm{tr}(\rho_B^2) \leq 1 \\
&\frac{1}{2} \leq I_3 \equiv \mathrm{tr}(\rho_C^2) \leq 1 \\
&\frac{1}{4} \leq I_4 \equiv \mathrm{tr}(\rho_A \otimes \rho_B \rho_{AB}) \leq 1 \\
&0 \leq I_5 \equiv |\mathrm{Hdet}(t_{ijk})|^2 \leq \frac{1}{16},
\end{aligned} \tag{18}$$

where

$$\begin{aligned}
\rho_A &\equiv \mathrm{tr}_{BC}|\Psi\rangle\langle\Psi| \\
\rho_B &\equiv \mathrm{tr}_{AC}|\Psi\rangle\langle\Psi| \\
\rho_C &\equiv \mathrm{tr}_{AB}|\Psi\rangle\langle\Psi| \\
\rho_{AB} &\equiv \mathrm{tr}_C|\Psi\rangle\langle\Psi|,
\end{aligned} \tag{19}$$

and $\mathrm{Hdet}(t_{ijk})$ is the hyperdeterminant of the coefficients t_{ijk} [15] and corresponds to the three-tangle of [16]. An equivalent set of invariants can be constructed [9]

$$\begin{aligned}
J_1 &\equiv \frac{1}{4}(1 + I_1 - I_2 - I_3 - 2\sqrt{I_5}) \\
J_2 &\equiv \frac{1}{4}(1 - I_1 + I_2 - I_3 - 2\sqrt{I_5}) \\
J_3 &\equiv \frac{1}{4}(1 - I_1 - I_2 + I_3 - 2\sqrt{I_5}) \\
J_4 &\equiv \sqrt{I_5} \\
J_5 &\equiv \frac{1}{4}(3 - 3I_1 - 3I_2 - I_3 + 4I_4 - 2\sqrt{I_5}),
\end{aligned} \tag{20}$$

which, in terms of the parameters of the decomposition (11), are equal to

$$\begin{aligned}
&0 \leq J_1 = |\lambda_1\lambda_4 e^{i\varphi} - \lambda_2\lambda_3|^2 \leq \frac{1}{4} \\
&0 \leq J_2 = \mu_0\mu_2 \leq \frac{1}{4} \\
&0 \leq J_3 = \mu_0\mu_3 \leq \frac{1}{4} \\
&0 \leq J_4 = \mu_0\mu_4 \leq \frac{1}{4} \\
&-\frac{1}{108} \leq J_5 = \mu_0(J_1 + \mu_2\mu_3 - \mu_1\mu_4) \leq \frac{2}{27},
\end{aligned} \tag{21}$$

where $\mu_i \equiv \lambda_i^2$. It can be proved that J_4 and J_5 are invariant under permutation of the parties, because so

are $2I_4 - I_1 - I_2$ and I_5, and J_1, J_2, and J_3 single out parties A, B and C respectively, and transform among themselves under party permutation.

From the above expressions one can prove the tighter bounds

$$\begin{aligned} 0 \leq J_2 + J_3 + J_4 \leq \frac{1}{4} \\ 0 \leq J_1 + J_3 + J_4 \leq \frac{1}{4} \\ 0 \leq J_1 + J_2 + J_4 \leq \frac{1}{4} \\ 0 \leq J_4 + J_5 \leq \frac{1}{4}. \end{aligned} \tag{22}$$

Also the following holds

$$\begin{aligned} J_1 = 0 \Rightarrow J_5 = 0 \\ J_2 = 0 \Rightarrow J_5 = 0 \\ J_3 = 0 \Rightarrow J_5 = 0 \\ J_4 = 0 \Rightarrow \sqrt{J_1 J_2 J_3} = \frac{J_5}{2}. \end{aligned} \tag{23}$$

From (21) and using the normalization condition $\sum_i \mu_i = 1$, it is possible to obtain the value of the set of coefficients $\{\mu_i\}$,

$$\begin{aligned} \mu_0^{\pm} &= \frac{J_4 + J_5 \pm \sqrt{\Delta_J}}{2(J_1 + J_4)} \\ \mu_i^{\pm} &= \frac{J_i}{\mu_0^{\pm}}, \quad i = 2, 3, 4 \\ \mu_1^{\pm} &= 1 - \mu_0^{\pm} - \frac{J_2 + J_3 + J_4}{\mu_0^{\pm}}, \end{aligned} \tag{24}$$

where

$$\Delta_J \equiv (J_4 + J_5)^2 - 4(J_1 + J_4)(J_2 + J_4)(J_3 + J_4) \geq 0, \tag{25}$$

which implies

$$J_4 + J_5 = 0 \Rightarrow J_4 = J_5 = 0. \tag{26}$$

Note that the value of $\cos\varphi$ can be also found from (21),

$$\cos\varphi^{\pm} = \frac{\mu_1^{\pm}\mu_4^{\pm} + \mu_2^{\pm}\mu_3^{\pm} - J_1}{2\lambda_1^{\pm}\lambda_2^{\pm}\lambda_3^{\pm}\lambda_4^{\pm}}, \tag{27}$$

and thus almost all the information about the decomposition can be extracted from the values of the $\{J_i\}$. There remains however some ambiguity in these expressions, since there are two solutions for the coefficients, corresponding to μ_0^+ and μ_0^-, and for each of them, two different angles, $0 \leq \varphi^{\pm} \leq \pi$ and $\bar{\varphi}^{\pm} = 2\pi - \varphi^{\pm}$, coming from (27). Part of this uncertainty is due to the two solutions of (8) and in fact the coefficients $\{\mu_i^+, \varphi^+\}$ and $\{\mu_i^-, \bar{\varphi}^-\}$ describe the same orbit, and the same happens for $\{\mu_i^-, \varphi^-\}$ and $\{\mu_i^+, \bar{\varphi}^+\}$. As it has been said, the solutions associated to $\bar{\varphi}$ are not considered because of the range of the angle. However the set of invariants $\{J_i\}$ (or $\{I_i\}$) does not determine a unique orbit, or equivalently a canonical point representing it. Two candidates are possible, $\{\mu_i^{\pm}, \varphi^{\pm}\}$, so there is still some ambiguity left.

The five polynomial invariants (18) are real, and this means that they can not distinguish among the orbits associated to a given pure three-qubit state $|\Psi\rangle$, with coefficients t_{ijk}, and to $|\Psi\rangle^*$, given by t_{ijk}^*. Indeed,

$$I_i(|\Psi\rangle^*) = I_i(|\Psi\rangle)^* = I_i(|\Psi\rangle), \tag{28}$$

where the second equality comes from the fact that the invariants are real. It is not possible, due to this ambiguity, to individuate a unique canonical state representing an orbit from the invariants (18), or (20). A twelfth degree complex polynomial invariant, I_6, introduced by Grassl [17], solves (albeit redundantly) this problem, just by inspection of the sign of its imaginary part (in other words, the second equality of (28) is not valid for this invariant). The explicit form of Grassl's invariant, using decomposition (11) is

$$I_6 = \mu_0^2\mu_4(\lambda_4(1 - 2(\mu_0 + \mu_1)) + 2\lambda_1\lambda_2\lambda_3 e^{-i\varphi})^2. \tag{29}$$

The set given by (18) and I_6 is complete, it allows to check when two states belong to different orbits, and from their values one can obtain a unique canonical point representing the orbit applying (24-27) and, in the end, using I_6 to discriminate between the two candidates.

This situation is quite different from what happens for pure states of bipartite systems. In this case, a generic state $|\Phi\rangle \in \mathcal{C}^{d_1} \otimes \mathcal{C}^{d_2}$, with coefficients t_{ij}, can be always tranformed into $|\Phi\rangle^*$ by local unitary transformations, as this is clear from the fact that all the Schmidt coefficients are real. In general this is not true for three-qubit systems, although in some cases the state $|\Psi\rangle$ and its complex conjugate $|\Psi\rangle^*$ are in the same orbit. This corresponds to the situations when either

$$|\cos\varphi^+| = |\cos\varphi^-| = 1, \tag{30}$$

or

$$\begin{aligned} \cos\varphi^+ = \cos\varphi^- \\ \mu_i^+ = \mu_i^-. \end{aligned} \tag{31}$$

Equivalent conditions in terms of the invariants $\{J_i\}$ can be obtained, giving

$$\sqrt{J_1 J_2 J_3} = \frac{|J_5|}{2}, \tag{32}$$

for the first case and

$$\Delta_J = 0, \tag{33}$$

for the second. Furthermore in both situations a product basis can be found for which all the coefficients t_{ijk} are real. For the states satisfying the first condition, this basis is the one that gives decomposition (11), since we have $e^{i\varphi} = \pm 1$, while in the second case the proof is a bit more tedious and it is given in the appendix A. From these results, then, it follows that

$$|\Psi\rangle \sim |\Psi\rangle^* \Leftrightarrow \sqrt{J_1 J_2 J_3} = \frac{|J_5|}{2} \text{ or } \Delta_J = 0 \Leftrightarrow |\Psi\rangle \text{ real}, \tag{34}$$

where a pure state belonging to $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$ is said to be real when there exists a product basis where all the coefficients are real.

To summarize, five independent quantities invariant under local unitaries are needed to specify the non-local properties of a generic three-qubit pure state. The coefficients appearing in the decomposition (11) form a complete faithful and minimal set of such invariants, when constrained as explained after (11). The polynomial invariants given in (18) must be completed with I_6 in order to solve the ambiguity between the orbits associated to $|\Psi\rangle$ and $|\Psi\rangle^*$, and from the values of these polynomial invariants one can build a unique canonical point representing the orbit. Also when $|\Psi\rangle$ and $|\Psi\rangle^*$ are in the same orbit there exists a product basis where all the coordinates of $|\Psi\rangle$ are real, as it happens for pure states of bipartite systems.

Let us mention finally that any real state can be written with real coefficients in terms of a set of six LBPS, adding the state $|011\rangle$ to (3) or to the first of (5). This is done by diagonalizing T_0 with two orthogonal matrices.

IV. MINIMAL DECOMPOSITION

We have seen that a generic three-qubit pure state can always be written in terms of five product states from any of the sets of states in (3), (4) or (5). However it is not clear which set should be used to find the minimal decomposition, that is, the one with the least number of non-local parameters. The minimal number of LBPS needed to specify a state $|\Psi\rangle$ will be denoted by $\nu(\Psi)$. We know that in general $\nu = 5$ but now we want to analyze the cases in which $\nu < 5$. In this section we present a complete classification of the three-qubit pure states according to this minimal number of product states. We also give necessary and sufficient conditions written in terms of the invariants $\{J_i\}$ to be satisfied by the states of each class. The number of non-local parameters in each family is $\nu - 1$, since all the coefficients are real. All the families satisfy condition (32).

A. $\nu = 4$

There are several subfamilies of states that allow for a decomposition in terms of four LBPS.

Type 4a: This subfamily is given by the states with $\mu_4 = 0$ in (11). It is easy to prove that this condition is equivalent to $J_4 = 0$ (we will take the rest of invariants different from zero, unless otherwise specified). Condition (32) is also satisfied with $J_5 > 0$, since all the phases can be absorbed.

Type 4b: States with $\mu_2 = 0$ ($\mu_3 = 0$) in (11). The equivalent conditions in term of the invariants are $J_2 = J_5 = 0$ ($J_3 = J_5 = 0$). Let us mention that there is an apparently lack of symmetry in this subfamily, but this is due to the fact that party A has been singled out in the determinations of the decomposition (11). In fact the analogous states with $J_1 = J_5 = 0$ are written with four terms if either party B or C is singled out in (7-10).

Type 4c: States with $\mu_1 = 0$ in (11). It can be proved that the corresponding conditions in terms of the invariants are $J_1 J_4 + J_1 J_2 + J_1 J_3 + J_2 J_3 = \sqrt{J_1 J_2 J_3} = \frac{J_5}{2}$. Again the lack of symmetry is due to the fact that party A is privileged in the calculation of the decomposition (11). Analogous condition can be found interchanging the role of the indices 1, 2 and 3, which means that the minimal decompositions is obtained if one of the other two parties is singled out in (7-10).

Type 4d: States with $\kappa_0 = 0$ in (15). It is proved in appendix B that the corresponding condition, apart from (32), which is always satisfied when $\nu < 5$, is $\Delta_J = 0$.

B. $\nu = 3$

Now we move to the study of those states that can be expressed as a sum of three LBPS.

Type 3a: This subfamily is given by taking $\mu_1 = \mu_4 = 0$ in (11). The equivalent conditions for the invariants are $J_4 = 0$ and $J_1 J_2 + J_1 J_3 + J_2 J_3 = \sqrt{J_1 J_2 J_3} = \frac{J_5}{2}$.

Type 3b: These states correspond to the case $\mu_j = \mu_k = 0$ in (11), for $j, k \in \{1, 2, 3\}$ and $j \neq k$. These conditions expressed in terms of the invariants are $J_j = J_k = J_5 = 0$.

C. $\nu = 2$

The states with two product states built from local bases are just in two classes.

Type 2a: $J_i = 0$ except $J_1(J_2, J_3)$, and these are the states where party A(B,C) is not entangled with the other two parties, so there is not truly three-party entanglement.

Type 2b: $J_i = 0$ except J_4, they include the standard GHZ state.

D. $\nu = 1$

Type1: $J_i = 0$, and these are the product states where there is no correlation between the parties.

E. Summary

All the states belonging to $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$ have been classified in terms of the minimal number, ν, of LBPS required to express the state, and the resulting families of states are shown in table I. Generically five terms are needed, although there are cases where $\nu < 5$. Necessary and sufficient conditions in terms of the set of invariants $\{J_i\}$ are given, which can be used to recognise the subfamily a three-qubit pure state belongs to. Once this has been done, we have provided the procedure that has to be applied in order to find this minimal decomposition with product states.

V. GENERALIZATION TO MORE PARTIES

The decomposition (11), which generalizes the bipartite Schmidt decomposition, has been proved to be very fruitful for the case of three-qubit pure states, so it will be convenient to know the way it can be generalized to more parties. In this section first we will consider with some details the case of four-qubit systems and this will give us insight into the difficulties found when we try to extend our results.

The procedure to be applied for the generalization of decomposition (11) for pure states belonging to $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$, i.e. states $|\Psi\rangle = \sum_{i,j,k,l} t_{ijkl} |ijkl\rangle$ shared by four parties A, B, C and D, will be now described. First we define the two hypermatrices [15]

$$(T_i)_{jkl} \equiv t_{ijkl}, \tag{35}$$

which means that the initial state is interpreted as

$$|\Psi\rangle = |0\rangle|\phi_0\rangle + |1\rangle|\phi_1\rangle, \tag{36}$$

where $|\phi_i\rangle$ are, up to normalization, three-qubit pure states, their coordinates being given by the elements of the corresponding hypermatrix T_i. The effect of the change of local bases is very similar to the one described for three-qubit systems: a unitary transformation on system A mixes the coordinates of the two $|\phi_i\rangle$, while unitary transformations on the rest of subsystems can be used to make zero some of their coefficients. Now we apply the change of local bases on A that gives

$$\mathrm{Hdet}(T'_0) = 0, \tag{37}$$

and afterwards unitary transformation on B, C and D are used to write the new $|\phi'_0\rangle$ in the canonical decomposition found for three-qubit pure states. Since (37) is verified, it is known that $|\phi'_0\rangle$ belongs to, at least, type 4a states, so we will manage to write the initial state $|\Psi\rangle$ in terms of the twelve product states:

$$\begin{aligned} &|0000\rangle, |0100\rangle, |0101\rangle, |0110\rangle, \\ &|1000\rangle, |1001\rangle, |1010\rangle, |1011\rangle, \\ &|1100\rangle, |1101\rangle, |1110\rangle, |1111\rangle. \end{aligned} \tag{38}$$

A simple counting of parameters gives that the minimal number of LBPS needed to specify a state $|\Psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$ is exactly twelve. The decomposition we have found depends on twenty-four non-local parameters but it is known that by phase redefinitions, i.e. acting locally with $U(1)$, five phases can be absorbed (generically, for N parties $N+1$ coefficients can be made real), so the number of non-local parameters is nineteen (including the norm), as it was expected [2].

However some problems arise in this case. Many decompositions in terms of the set of states (38) are possible for the same state. In fact (37) is a fourth degree equation, so four solutions will be found and from these solutions four different decompositions will be derived. For the case of three-qubit pure state there were two solutions for (8), but we managed to obtain a unique decomposition by limiting the range of φ. A similar reasoning seems not to be trivial for this case. Furthermore for pure four-qubit states more inequivalent set of twelve product states appear, and this will difficult the analysis of the minimal decomposition. The generalization of decomposition (11) to N-qubit pure states ($N > 3$) is then quite cumbersome.

Finally, it has to be noted that the algorithm proposed in [12] for the decomposition (15) can be also extended to higher dimensional systems. Let us mention however that, in any case, as the dimension of the space increases, the number of coefficients that can be made equal to zero in any of the decompositions becomes irrelevant.

VI. CONCLUSIONS

In this work we have studied the canonical forms of pure three-qubit states, extending the known results of bipartite systems.

First we show the possible generalizations of the Schmidt decomposition and we relate one of these decompositions (11) to the polynomial invariants of [2–9]. The six linearly independent polynomial invariants of [7] are not able to discriminate betwee the entanglement orbits associated to a state and its complex conjugate in a product basis. An additional polynomial invariant introduced in [17] has to be used, and we have seen how to connect this complete set of polynomial invariants with our generalization of the Schmidt decomposition. Indeed it is shown how to find a canonical point in a generic

orbit described by this complete set of invariants. Let us mention here that a three-qubit pure state $|\Psi\rangle$ and its complex conjugate $|\Psi\rangle^*$ give the same optimal probability of distilling a maximally entangled state of three qubits, in the single-copy case [14].

We have also looked for the decomposition of any state, $|\Psi\rangle$, with the minimal number, $\nu(\Psi)$, of product states built from local bases. Generically this number is equal to five, although many exceptional states have been found with $\nu < 5$. We have been able to give a complete classification of these states by means of a set of necessary and sufficient conditions written in terms of the set of invariants (20). The procedure to be applied in order to build the minimal decomposition for every state has been given too. The classification of the pure three-qubit states in terms of their entanglement properties can be done following alternative criteria to the one described here, which is based on the features observed acting with the group of local unitary transformations. A possible approach is to classify the states looking for their probabilistic conversions under local operations and classical comunication (LOCC) for the single-copy case (see [13] and also [14,18]) or in the asymptotic regime [19]. It would be expected that these classifications are a coarse-graining of the one presented in this work. In fact this is the case for the equivalences classes under LOCC given in [13].

Finally it has been indicated how to extend decomposition (11) to systems of more parties. A simple counting of parameters shows that at least $2^N - N$ product states built from local bases are needed in order to specify a generic N-qubit pure state, and for four qubits we succeeded to find a procedure that makes zero four of the coordinates t_{ijkl}. The decomposition (15) allows for a simpler generalization. However, in all the cases some difficulties arise, related to the uniqueness of the decompositions, and it is not clear whether these generalized Schmidt decompositions are quite useful for composite systems of more than three qubits.

APPENDIX A: REAL STATES

In this appendix we will show that, given a pure three-qubit state $|\psi\rangle \in \mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$, this state is real, i.e. there exists a product basis for which all coefficients are real, if and only if $\sqrt{J_1 J_2 J_3} = \frac{|J_5|}{2}$ or $\Delta_J = 0$.

Consider the case of a state $|\psi\rangle = \sum_{i,j,k} t_{ijk}|ijk\rangle$ where all the t_{ijk} are real. Now we will follow the procedure described by the equations (7-10) that gives us the decomposition (11). Since the initial coordinates are real, from (8) a second degree equation in x with real coefficients is obtained, and this implies that the two solutions, x and $\bar{x}$, satisfy that either they are both real or $x = \bar{x}^*$. In the first case, the calculation of the decomposition can be performed using orthogonal matrices, and since the initial coordinates were real, we will obtain a real decomposition, i.e. $\varphi = 0, \pi$, which is equivalent to (32). For the second case, since $x = \bar{x}^*$, $\mathrm{tr}(T_0'^{\dagger} T_0') = \mathrm{tr}(\bar{T}_0'^{\dagger} \bar{T}_0')$, and then $\mu_0 = \bar{\mu}_0$ and (33) is satisfied.

Now, the inverse has to be proved. For the first case it is clear that all the states verifying (32) take real coordinates when they are expressed in the basis used in decomposition (11). For the second case the proof is not so trivial.

Consider a generic state, $|\phi\rangle$, having Δ_J equal to zero. The parametrization of this family of states is simplified using (16), so let us first mention some facts about this decomposition. As it has been shown, any state with $J_4 \neq 0$ can be written as (16) [9,13] where

$$\begin{aligned} \alpha &= \frac{1}{\lambda_4}\sqrt{J_1 + J_4} \\ \beta &= \frac{1}{\lambda_4}\sqrt{\mu_2\mu_3 + \mu_4(\mu_4 + \mu_2 + \mu_3)} \\ \delta &= \arg(\lambda_1\lambda_4 e^{i\varphi} - \lambda_2\lambda_3), \end{aligned} \tag{39}$$

and, up to unitary transformations,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |\varphi_i\rangle = \begin{pmatrix} \cos\gamma_i \\ \sin\gamma_i \end{pmatrix}, \; i = 1, 2, 3. \tag{40}$$

It can be proved that when $\Delta_J = 0$ the coefficients α and β are equal and then the states to be studied are

$$|\phi\rangle = \alpha\left(|000\rangle + e^{i\delta}|\varphi_1\varphi_2\varphi_3\rangle\right). \tag{41}$$

Recall that for these states the complex conjugate is in the same orbit as the original one, and this means that

$$t^*_{ijk} = \sum v^1_{ia} v^2_{jb} v^3_{kc} t_{abc}, \tag{42}$$

where t_{ijk} are the coordinates in some product basis and v^1_{ia}, v^2_{jb} and v^3_{kc} are the elements of the local unitary matrices, V^1 in A, V^2 in B and V^3 in C, connecting the two states. From (41) it follows that these unitary operators are

$$V^i = e^{-i\delta'} \begin{pmatrix} c_i & s_i \\ s_i & -c_i \end{pmatrix}, \tag{43}$$

where $c_i \equiv \cos\gamma_i$, $s_i \equiv \sin\gamma_i$ and $\delta' \equiv \frac{\delta}{3}$ (actually, the phase factors in the matrices V^i can be given by arbitrary angles δ_i satisfying the constraint $\sum_i \delta_i = \delta$, but we choose these angles for simplicity).

Now we would like to find a product basis for which all the coefficients are real, i.e.

$$t'_{ijk} = \sum w^1_{ia} w^2_{jb} w^3_{kc} t_{abc} = t'^*_{ijk}, \tag{44}$$

and from this condition and using (42), we have

$$V^i = (W^i)^T W^i. \tag{45}$$

The explicit form of each V^i, (43), as a product of a phase factor and a real and symmetric matrix allows to write them as

$$V^i = e^{-i\delta'}(O^i)^T D^i O^i, \tag{46}$$

where O^i are orthogonal matrices and D^i are diagonal matrices with entries ± 1. The change of basis we are looking for then is given by

$$W^i = (D^i)^{\frac{1}{2}} O^i = e^{-i\delta''} \begin{pmatrix} \tilde{c}_i & \tilde{s}_i \\ -i\tilde{s}_i & i\tilde{c}_i \end{pmatrix}, \tag{47}$$

where $\tilde{c}_i \equiv \cos\frac{\gamma_i}{2}$, $\tilde{s}_i \equiv \sin\frac{\gamma_i}{2}$ and $\delta'' \equiv \frac{\delta}{6}$. The new coordinates obtained applying these local change of basis are, up to normalization,

$$\begin{aligned}
t'_{000} &= \tilde{c}_1\tilde{c}_2\tilde{c}_3\cos\frac{\delta}{2} & t'_{001} &= -\tilde{c}_1\tilde{c}_2\tilde{s}_3\sin\frac{\delta}{2} \\
t'_{010} &= -\tilde{c}_1\tilde{s}_2\tilde{c}_3\sin\frac{\delta}{2} & t'_{011} &= -\tilde{c}_1\tilde{s}_2\tilde{s}_3\cos\frac{\delta}{2} \\
t'_{100} &= -\tilde{s}_1\tilde{c}_2\tilde{c}_3\sin\frac{\delta}{2} & t'_{101} &= -\tilde{s}_1\tilde{c}_2\tilde{s}_3\cos\frac{\delta}{2} \\
t'_{110} &= -\tilde{s}_1\tilde{s}_2\tilde{c}_3\cos\frac{\delta}{2} & t'_{111} &= \tilde{s}_1\tilde{s}_2\tilde{s}_3\sin\frac{\delta}{2}.
\end{aligned} \tag{48}$$

This ends the proof.

APPENDIX B: TYPE 4D

In this section we prove that a three-qubit pure state $|\psi\rangle$ can be written as

$$|\psi\rangle = l_1|001\rangle + l_2|010\rangle + l_3|100\rangle + l_4|111\rangle, \tag{49}$$

with real and positive coefficients, if and only if (32) and (33) are verified.

Starting from (49) we can apply the procedure given by (7-10) to obtain (11). It can be seen that all the unitary matrices needed for the determination of this decomposition are real, i.e. they are orthogonal, and since the original coefficients $\{l_i\}$ were also real, we will obtain a real decomposition with (32). Moreover, it can also be proved that the two matrices obtained after (8), T'_0 and $\bar{T}'_0$, corresponding to the two solutions of this equation, x and $\bar{x}$, verify

$$\mathrm{tr}((T'_0)^\dagger T'_0) = \mathrm{tr}((\bar{T}'_0)^\dagger \bar{T}'_0). \tag{50}$$

This condition implies that $\mu_0 = \bar{\mu}_0$, and using (24) we have also (33).

Now we prove the inverse. Consider a state $|\phi\rangle$ satisfying (32) and (33). Because of the latter condition, the state allows for a decomposition as (41). Moreover, since (32) is also satisfied, we have $\varphi = 0, \pi$ in (11), and this implies, using (39), that $\delta = 0, \pi$. The generic expression for a state satisfying both the conditions can be now given,

$$|\phi\rangle = \alpha(|000\rangle \pm |\varphi_1\varphi_2\varphi_3\rangle). \tag{51}$$

If we perform the local change of bases described by (47) it can be seen, using (48) and the fact that $\delta = 0, \pi$, that the state $|\phi\rangle$ is of type 4d. Indeed, the new coordinates are, after absorbing the phases and up to normalization,

$$l_1 = \tilde{s}_1\tilde{s}_2\tilde{c}_3 \quad l_2 = \tilde{s}_1\tilde{c}_2\tilde{s}_3 \quad l_3 = \tilde{c}_1\tilde{s}_2\tilde{s}_3 \quad l_4 = \tilde{c}_1\tilde{c}_2\tilde{c}_3, \tag{52}$$

for $\delta = 0$, and

$$l_1 = \tilde{c}_1\tilde{c}_2\tilde{s}_3 \quad l_2 = \tilde{c}_1\tilde{s}_2\tilde{c}_3 \quad l_3 = \tilde{s}_1\tilde{c}_2\tilde{c}_3 \quad l_4 = \tilde{s}_1\tilde{s}_2\tilde{s}_3, \tag{53}$$

for $\delta = \pi$. Note that the local bases that appear in (49) are the ones that diagonalize the local density matrices. This gives the procedure to be applied in order to find the minimal decomposition without performing the maximization of (14), which is generically a more difficult calculation.

ACKNOWLEDGMENTS

We thank G. Vidal, A. Sudbery and M. Grassl for useful discussion. R. T. acknowledges financial support by CICYT project AEN 98-0431, CIRIT project 1998SGR-00026 and CEC project IST-1999-11053, A. Andrianov by RFBR 99-01-00736 and CIRIT, PIV-2000, A. Acín and E. J. by a grant from MEC (AP98 and AP99). Financial support from the ESF is also acknowledged. This work was partially performed at the 2000 Benasque Center for Science.

[1] E. Schmidt, Math. Ann. **63** (1907) 433; A. Ekert and P. L. Knight, Am. J. Phys. **63** (1995) 415; A. Peres, "Quantum theory: concepts and methods", Kluwer Academic Publishers, Dordrecht 1995.

[2] N. Linden and S. Popescu, Fortsch. Phys. **46** (1998) 567, quant-ph/9711016.

[3] E. M. Rains, "Polynomial invariants of quantum codes", quant-ph/9704042.

[4] M. Grassl, M. Roetteler and T. Beth, Phys. Rev. A **58** (1998) 1833, quant-ph/9712040.

[5] N. Linden, S. Popescu and A. Sudbery, Phys. Rev. Lett. **83** (1999) 243, quant-ph/9801076.

[6] J. Kempe, Phys. Rev. A **60** (1999) 910, quant-ph/9902036.

[7] A. Sudbery, "On local invariants of pure three-qubit states", quant-ph/0001116.

[8] Y. Makhlin, "Nonlocal properties of two-qubit gates and mixed states and optimization of quantum computations", quant-ph/0002045.

[9] A. Acín, A. Andrianov, L. Costa, E. Jané, J.I. Latorre and R. Tarrach, Phys. Rev. Lett **85** (2000) 1560, quant-ph/0003050.

[10] A. Peres, Phys. Lett. A **202** (1995) 16, quant-ph/9504006.

[11] T. A. Brun and O. Cohen, "Parametrization and distillability of three-qubit entanglement", quant-ph/0005124.

[12] A. Higuchi and A. Sudbery, "How entangled can two couples get?", quant-ph/0005013; H. A. Carteret, A. Higuchi, A. Sudbery, "Multipartite generalisation of the Schmidt decomposition", quant-ph/0006125.

[13] W. Dür, G. Vidal and J. I. Cirac, "Three qubits can be entangled in two inequivalent ways", quant-ph/0005115.

[14] A. Acín, E. Jané, W. Dür and G. Vidal, "Optimal distillation of a GHZ state", quant-ph/0007042.

[15] I. M. Gelfand, M. M. Kapranov and A. V. Zelevinsky, "Discriminants, resultants and multidimensional determinants", Birkhäuser Boston 1994. Its explicit form is: $\mathrm{Hdet}(t_{ijk}) = t_{000}^2 t_{111}^2 + t_{001}^2 t_{110}^2 + t_{010}^2 t_{101}^2 + t_{100}^2 t_{011}^2 - 2(t_{000}t_{111}t_{011}t_{100} + t_{000}t_{111}t_{101}t_{010} + t_{000}t_{111}t_{110}t_{001} + t_{011}t_{100}t_{101}t_{010} + t_{011}t_{100}t_{110}t_{001} + t_{101}t_{010}t_{110}t_{001}) + 4(t_{000}t_{110}t_{101}t_{011} + t_{111}t_{001}t_{010}t_{100})$.

[16] V. Coffman, J. Kundu, W. K. Wootters, Phys. Rev. A **61** 052306, quant-ph/9907047.

[17] Markus Grassl, private communication.

[18] T.A. Brun and O. Cohen, "Distillation of GHZ states by selective information manipulation", Phys. Rev. Lett. **84** (2000) 5908, quant-ph/0001084.

[19] C.H. Bennett, S. Popescu, D. Rohrlich, J.A. Smolin and A.V. Thapliyal, "Exact and asymptotic measures of multipartite pure state entanglement", quant-ph/9908073; N. Linden, S. Popescu, B. Schumacher and M. Westmoreland, "Reversibility of local transformations of multiparticle entanglement", quant-ph/9912039; G. Vidal, W. Dür and J.I. Cirac, Phys. Rev. Lett. **85** (2000) 658, quant-ph/0004009; S. Wu and Y. Zhang, "Multipartite pure-state entanglement and the generalized GHZ states", quant-ph/0004020.

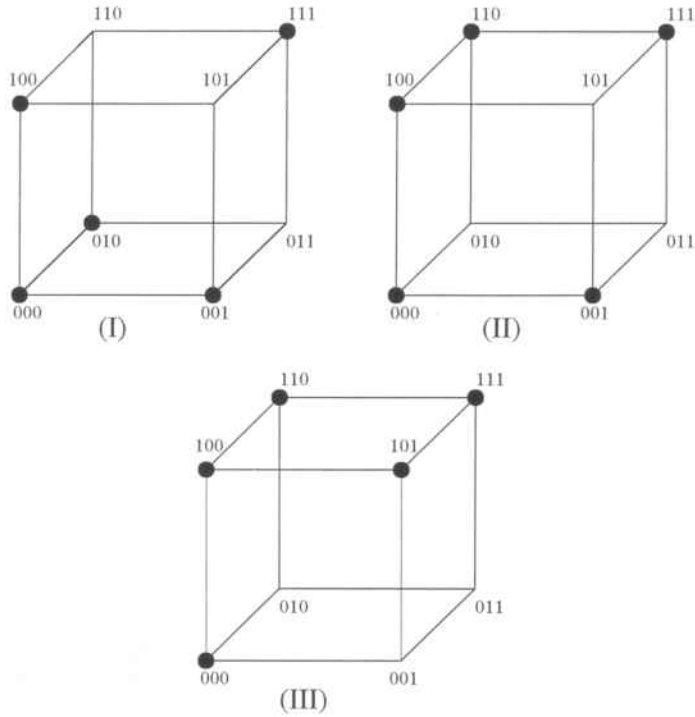


FIG. 1. The figure depicts the three inequivalent sets of states given by (3), (4) and (5).

Type	Conditions	States
4a	$J_4 = 0, \sqrt{J_1 J_2 J_3} = \frac{J_5}{2}$	$\|000\rangle, \|100\rangle, \|101\rangle, \|110\rangle$
4b	$J_2 = J_5 = 0$	$\|000\rangle, \|100\rangle, \|110\rangle, \|111\rangle$
4c	$J_1 J_4 + J_1 J_2 + J_1 J_3 + J_2 J_3 = \sqrt{J_1 J_2 J_3} = \frac{J_5}{2}$	$\|000\rangle, \|101\rangle, \|110\rangle, \|111\rangle$
4d	$\Delta_J = 0, \sqrt{J_1 J_2 J_3} = \frac{\|J_5\|}{2}$	$\|001\rangle, \|010\rangle, \|100\rangle, \|111\rangle$
3a	$J_1 J_2 + J_1 J_3 + J_2 J_3 = \sqrt{J_1 J_2 J_3} = \frac{J_5}{2}, J_4 = 0$	$\|000\rangle, \|101\rangle, \|110\rangle$
3b	$J_1 = J_2 = J_5 = 0$	$\|000\rangle, \|110\rangle, \|111\rangle$
2a	All $J_i = 0$ apart from J_1	$\|000\rangle, \|011\rangle$
2b	All $J_i = 0$ apart from J_4	$\|000\rangle, \|111\rangle$
1	$J_i = 0$	$\|000\rangle$

TABLE I. Classification of three-quantum-bit states. For the types of states denoted by 4b, 4c, 3b and 2a, there exist analogous condition interchanging the roles of the invariants J_1, J_2, J_3, and consequently the product states used in the minimal decomposition.

Appendix C

Classification of mixed three–qubit states

A. Acín[1], D. Bruß[2], M. Lewenstein[2], and A. Sanpera[2]
[1] *Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, 08028 Barcelona, Spain*
[2] *Institut für Theoretische Physik, Universität Hannover, 30167 Hannover, Germany*
(Received March 8, 2001)

We introduce a classification of mixed three–qubit states, in which we define the classes of separable, biseparable, W– and GHZ–states. These classes are successively embedded into each other. We show that contrary to pure W–type states, the mixed W–class is not of measure zero. We construct witness operators that detect the class of a mixed state. We discuss the conjecture that all entangled states with positive partial transpose (PPTES) belong to the W–class. Finally, we present a new family of PPTES "edge" states with maximal ranks.

03.65.Bz, 03.67.-a,03.65.Ca, 03.67.Hk

The rapidly increasing interest in quantum information processing has motivated the detailed study of entanglement. Whereas entanglement of pure bipartite systems is well understood, the classification of mixed states according to the degree and character of their entanglement is still a matter of intensive research (see [1]). It was soon realised, that the entanglement of pure tripartite quantum states is not a trivial extension of the entanglement of bipartite systems [2,3]. Recently, the first results concerning the entanglement of pure tripartite systems have been achieved [4–6]. There, the main goal has been to generalize the concept of the Schmidt decomposition to three-party systems [4,5], and to distinguish classes of locally inequivalent states [6]. The knowledge of mixed tripartite entanglement is much less advanced (see, however, [7–9]).

In this Letter we introduce a classification of the whole space of mixed three–qubit states into different entanglement classes. We provide a method to determine to which class a given state belongs (tripartite witnesses). We also discuss the characterization of entangled states that are positive under partial transposition (PPTES). Finally, we introduce a new family of PPTES for mixed tripartite qubits.

Our proposal to classify mixed tripartite–qubit states is done by specifying compact convex subsets of the space of all states, which are embedded into each other. This idea vaguely resembles the classification of bipartite systems by their Schmidt number [9–11]. However, as shown later our classification does *not* follow the Schmidt number [9]. Also in this respect, entanglement of tripartite systems differs genuinely from the one of bipartite quantum systems.

Before presenting our results concerning mixed states, we briefly review some of the recent results on pure three–qubit states. Any three–qubit vector (pure state) can be written as

$$|\psi_{GHZ}\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\theta}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle\,, \qquad (1)$$

where $\lambda_i \geq 0$, $\sum_i \lambda_i^2 = 1$, $\theta \in [0,\pi]$, and $\{|0\rangle,|1\rangle\}$ denotes an orthonormal basis in Alice's, Bob's and Charlie's space, respectively [4]. Apart from separable and biseparable pure states, there exist also two different types of locally inequivalent entangled vectors; the so-called GHZ–type [2] and W–type [6]. Vectors belonging to GHZ– and W–types cannot be transformed into each other by local operations and classical communication (LOCC). Generically, a vector described by Eq.(1) is of the GHZ–type, while W–vectors can be written as

$$|\psi_W\rangle = \lambda_0|000\rangle + \lambda_1|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle. \qquad (2)$$

W–vectors form a set of measure zero among all pure states [6]. Also, given a W–vector one can always find a GHZ–vector as close to it as desired by adding an infinitesimal λ_4–term to the RHS of Eq.(2) [12]. Furthermore, the so-called tangle, τ, introduced in [13], can be used to detect the type, since $\tau(|\psi_W\rangle) = 0$ [6].

Mixed states of three–qubit systems can be classified generalizing the classification of pure states. To this aim we define (see Fig.1):

- the class S of separable states, i.e. those that can be expressed as a convex sum of projectors onto product vectors;
- the class B of biseparable states, i.e. those that can be expressed as a convex sum of projectors onto product and bipartite entangled vectors (A–BC, B–AC and C–AB);
- the class W of W–states, i.e. those that can be expressed as a convex sum of projectors onto product, biseparable and W–type vectors;
- the class GHZ of GHZ–states, i.e. the set of all physical states.

All these sets are convex and compact, and satisfy $S \subset B \subset W \subset GHZ$. States in S are not entangled. No genuine three–party entanglement is needed to prepare entangled states in the subset $B \setminus S$. The formation of entangled states in $W \setminus B$ requires W–type vectors with three–party entanglement, but zero tangle, which is an

Classification of mixed three–qubit states

A. Acín[1], D. Bruß[2], M. Lewenstein[2], and A. Sanpera[2]
[1] *Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, 08028 Barcelona, Spain*
[2] *Institut für Theoretische Physik, Universität Hannover, 30167 Hannover, Germany*
(Received March 8, 2001)

We introduce a classification of mixed three–qubit states, in which we define the classes of separable, biseparable, W– and GHZ–states. These classes are successively embedded into each other. We show that contrary to pure W–type states, the mixed W–class is not of measure zero. We construct witness operators that detect the class of a mixed state. We discuss the conjecture that all entangled states with positive partial transpose (PPTES) belong to the W–class. Finally, we present a new family of PPTES "edge" states with maximal ranks.

03.65.Bz, 03.67.-a,03.65.Ca, 03.67.Hk

The rapidly increasing interest in quantum information processing has motivated the detailed study of entanglement. Whereas entanglement of pure bipartite systems is well understood, the classification of mixed states according to the degree and character of their entanglement is still a matter of intensive research (see [1]). It was soon realised, that the entanglement of pure tripartite quantum states is not a trivial extension of the entanglement of bipartite systems [2,3]. Recently, the first results concerning the entanglement of pure tripartite systems have been achieved [4–6]. There, the main goal has been to generalize the concept of the Schmidt decomposition to three-party systems [4,5], and to distinguish classes of locally inequivalent states [6]. The knowledge of mixed tripartite entanglement is much less advanced (see, however, [7–9]).

In this Letter we introduce a classification of the whole space of mixed three–qubit states into different entanglement classes. We provide a method to determine to which class a given state belongs (tripartite witnesses). We also discuss the characterization of entangled states that are positive under partial transposition (PPTES). Finally, we introduce a new family of PPTES for mixed tripartite qubits.

Our proposal to classify mixed tripartite–qubit states is done by specifying compact convex subsets of the space of all states, which are embedded into each other. This idea vaguely resembles the classification of bipartite systems by their Schmidt number [9–11]. However, as shown later our classification does *not* follow the Schmidt number [9]. Also in this respect, entanglement of tripartite systems differs genuinely from the one of bipartite quantum systems.

Before presenting our results concerning mixed states, we briefly review some of the recent results on pure three–qubit states. Any three–qubit vector (pure state) can be written as

$$|\psi_{GHZ}\rangle = \lambda_0|000\rangle + \lambda_1 e^{i\theta}|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle + \lambda_4|111\rangle\,, \qquad (1)$$

where $\lambda_i \geq 0$, $\sum_i \lambda_i^2 = 1$, $\theta \in [0,\pi]$, and $\{|0\rangle,|1\rangle\}$ denotes an orthonormal basis in Alice's, Bob's and Charlie's space, respectively [4]. Apart from separable and biseparable pure states, there exist also two different types of locally inequivalent entangled vectors; the so-called GHZ–type [2] and W–type [6]. Vectors belonging to GHZ– and W–types cannot be transformed into each other by local operations and classical communication (LOCC). Generically, a vector described by Eq.(1) is of the GHZ–type, while W–vectors can be written as

$$|\psi_W\rangle = \lambda_0|000\rangle + \lambda_1|100\rangle + \lambda_2|101\rangle + \lambda_3|110\rangle. \qquad (2)$$

W–vectors form a set of measure zero among all pure states [6]. Also, given a W–vector one can always find a GHZ–vector as close to it as desired by adding an infinitesimal λ_4–term to the RHS of Eq.(2) [12]. Furthermore, the so-called tangle, τ, introduced in [13], can be used to detect the type, since $\tau(|\psi_W\rangle) = 0$ [6].

Mixed states of three–qubit systems can be classified generalizing the classification of pure states. To this aim we define (see Fig.1):

- the class S of separable states, i.e. those that can be expressed as a convex sum of projectors onto product vectors;
- the class B of biseparable states, i.e. those that can be expressed as a convex sum of projectors onto product and bipartite entangled vectors (A–BC, B–AC and C–AB);
- the class W of W–states, i.e. those that can be expressed as a convex sum of projectors onto product, biseparable and W–type vectors;
- the class GHZ of GHZ–states, i.e. the set of all physical states.

All these sets are convex and compact, and satisfy $S \subset B \subset W \subset GHZ$. States in S are not entangled. No genuine three–party entanglement is needed to prepare entangled states in the subset $B \setminus S$. The formation of entangled states in $W \setminus B$ requires W–type vectors with three–party entanglement, but zero tangle, which is an

entanglement monotone decreasing under LOCC [6]. Finally, the class GHZ contains all types of entanglement, and in particular, GHZ–type vectors are needed to prepare states from $GHZ \setminus W$. The introduced classes are invariant under local unitary or invertible non-unitary operations, while local POVM's [12] can only transform states from a "higher" to a "lower" class.

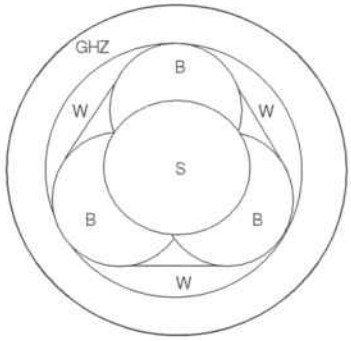


FIG. 1. Schematic structure of the set of all three–qubit states. S: separable class; B: biseparable class (convex hull of biseparable states with respect to any partition); W–class and GHZ–class.

Notice that since GHZ–vectors can be expressed as the sum of only two product vectors, i.e. $|GHZ\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$, whereas the minimum number of product terms forming a W–vector is three [4,6], as in the state $|W\rangle = (|100\rangle + |010\rangle + |001\rangle)/\sqrt{3}$, our scheme may seem somehow counterintuitive. Indeed, for bipartite systems, states with lower Schmidt number, i.e. lower number of product terms in the Schmidt decomposition, are embedded into the set of states with higher Schmidt number [10]. One is tempted to extend this classification to tripartite systems as $S \subset B \subset GHZ \subset W$, where now W is the set of all states. However, such generalization is evidently wrong, because the the set of GHZ–states in such classification cannot be closed [12].

Having established the structure of the set of mixed three–qubit states, we show how to determine to which class a given state ρ belongs. To this aim, we use the approach developed previously in the construction and optimisation of witness operators [11,14,15].

We denote the range of ρ by $R(\rho)$, its rank by $r(\rho)$, its kernel by $K(\rho)$, and the dimension of $K(\rho)$ by $k(\rho)$. Following the approach of the best separable approximation (BSA) [16], one can decompose any state ρ as a convex combination of a W–class state and a remainder δ,

$$\rho = \lambda_W \rho_W + (1 - \lambda_W)\delta \ , \tag{3}$$

where $0 \leq \lambda_W \leq 1$, and $R(\delta)$ does not contain any W–vector. Maximization of λ_W leads to the best W–approximation of ρ. Notice that only for ρ belonging to the $GHZ \setminus W$–class, this decomposition is non-trivial, i.e. $\lambda_W \neq 1$. Also, $r(\delta) = 1$, since any subspace spanned by two linearly independent GHZ–vectors contains at least one pure state with zero tangle. In fact, given $|\psi_1\rangle$ and $|\psi_2\rangle$ with $\tau(|\psi_1\rangle)$ and $\tau(|\psi_2\rangle)$ not equal zero, it is always possible to find some $\tilde{\alpha}, \tilde{\beta}$ such that $|\psi(\tilde{\alpha}, \tilde{\beta})\rangle = \tilde{\alpha}|\psi_1\rangle + \tilde{\beta}|\psi_2\rangle$ is normalized, and its tangle is zero. Therefore, any W–approximation must have the form:

$$\rho = \lambda_W \rho_W + (1 - \lambda_W)|\psi_{GHZ}\rangle\langle\psi_{GHZ}| \ . \tag{4}$$

Similarly, one can express ρ in the best biseparable approximation as:

$$\rho = \lambda_B \rho_B + (1 - \lambda_B)\delta \ , \tag{5}$$

where now $R(\delta)$ must not contain any biseparable states, i.e. $r(\delta) < 4$, since any N–dimensional subspace of the $2 \times N$ space contains at least one product vector [17].

We use the above decompositions to construct operators that detect the desired subset (see [15]). In analogy to entanglement witnesses and Schmidt witnesses we term these operators tripartite witnesses. The existence of witness operators is a consequence of the Hahn-Banach theorem, which states that a point outside a convex compact set is separated from that set by a hyper-plane. The equation $\mathrm{Tr}(\mathcal{W}\rho) = 0$ describes such a hyper-plane, and one calls $\mathcal{W}$ a witness operator. For example, in our setting, a W–witness is an operator $\mathcal{W}_W$ such that $\mathrm{Tr}(\mathcal{W}_W \rho_B) \geq 0$ holds $\forall \rho_B \in B$, but for which there exists a $\rho_W \in W \setminus B$ such that $\mathrm{Tr}(\mathcal{W}_W \rho_W) < 0$.

Any GHZ–witness (W–witness) has the canonical form $\mathcal{W} = Q - \epsilon \mathbb{1}$, where Q is a positive operator which has no W–type (B–type) vectors in its kernel; thus $k(Q) = 1$ ($k(Q) < 4$) [11,15]. An example of a GHZ–witness is

$$\mathcal{W}_{GHZ} = \frac{3}{4}\mathbb{1} - P_{GHZ} \ , \tag{6}$$

where P_{GHZ} is the projector onto $|GHZ\rangle$. The value 3/4 corresponds to the maximal squared overlap between $|GHZ\rangle$ and a W–vector. This construction guarantees that $\mathrm{Tr}(\mathcal{W}_{GHZ}\rho_W) \geq 0$ for any W–state, and since $\mathrm{Tr}(\mathcal{W}_{GHZ}P_{GHZ}) < 0$, there is a GHZ $\setminus$ W–state which is detected by $\mathcal{W}_{GHZ}$. The maximal overlap is obtained as follows: due to the symmetry of $|GHZ\rangle$ we only need to consider W–vectors that are symmetric under the exchange of any of the three qubits [18]. Therefore, we have to consider all local trilateral rotations of $|\psi_W\rangle = \kappa_0|000\rangle + \kappa_1(|100\rangle + |010\rangle + |001\rangle)$, where κ_0, κ_1 are real and $\kappa_0^2 + 3\kappa_1^2 = 1$. Due to the symmetry, such rotations can be parametrised for all parties as $|0\rangle \to \alpha|0\rangle + \beta|1\rangle$, $|1\rangle \to \beta^*|0\rangle - \alpha^*|1\rangle$, with $|\alpha|^2 + |\beta|^2 = 1$. Thus, the overlap $\langle GHZ|\psi_W\rangle$ is a function of six parameters with two constraints, and can be maximized using Lagrange multipliers. An optimal choice of parameters is $\kappa_0 = 0$, $\kappa_1 = 1/\sqrt{3}$, and $\beta = -\alpha = 1/\sqrt{2}$. This leads to $|\langle GHZ|\psi_W\rangle|^2_{max} = 3/4$.

Analogously, we can construct a W–witness as

$$\mathcal{W}_{W_1} = \frac{2}{3}\mathbb{1} - P_W \ , \tag{7}$$

where P_W is now the projector onto a vector $|W\rangle$, and $2/3$ corresponds to the maximal squared overlap between $|W\rangle$ and a B–vector. Another example of a W–witness is

$$\mathcal{W}_{W_2} = \frac{1}{2}\mathbb{1} - P_{GHZ}, \tag{8}$$

where now $1/2$ is the maximal squared overlap between $|GHZ\rangle$ and a B–type vector [19]. The W–vector that has maximal overlap with $|GHZ\rangle$ is detected by $\mathcal{W}_{W_2}$.

The tripartite witness $\mathcal{W}_{W_2}$ allows to prove that the class of mixed W $\setminus$ B–states is not of measure zero: consider the family of states in $\mathcal{C}^2 \otimes \mathcal{C}^2 \otimes \mathcal{C}^2$ given by the convex sum of the identity and a projector onto a W–state,

$$\rho = \frac{1-p}{8}\mathbb{1} + pP_W \ . \tag{9}$$

Obviously, the states (9) belong at most to W. The range for the parameter p, in which $\mathcal{W}_{W_2}$ detects ρ, i.e. $\mathrm{Tr}(\mathcal{W}_{W_2}\rho) < 0$, is found to be $3/5 < p \leq 1$, and is bigger than the one found by using $\mathcal{W}_{W_1}$. Taking any p which has a finite distance to the border of this interval, i.e. $p - 3/5 > \Delta$ and $1 - p > \Delta$, it is always possible to find a finite region around ρ which still belongs to the $W \setminus B$–class. This can be seen by considering

$$\tilde{\rho} = (1-\epsilon)\left[\frac{1-p}{8}\mathbb{1} + pP_W\right] + \epsilon\sigma \ , \tag{10}$$

where σ is an *arbitrary* density matrix, which covers all directions of possible deviations from ρ in the operator space. In the worst case σ is orthogonal to P_{GHZ}, so that $\mathrm{Tr}(P_{GHZ}\sigma) = 0$, and therefore $\mathrm{Tr}(\mathcal{W}_{W_2}\tilde{\rho}) = (1-\epsilon)\mathrm{Tr}(\mathcal{W}_{W_2}\rho) + \epsilon/2$. As long as the relation $\epsilon < (5p-3)/(5p+1)$ holds, the corresponding state $\tilde{\rho}$ is still detected by $\mathcal{W}_{W_2}$. Moreover, one can also find a finite ϵ' such that if $\epsilon < \epsilon'$, then $\tilde{\rho}$ is in the W–class. The bound ϵ' is obtained, for instance, by demanding that $(1-\epsilon')(1-p)\mathbb{1}/8 + \epsilon'\sigma$ is biseparable. The intersection of the two intervals gives a finite range for ϵ where the state $\tilde{\rho}$ is in the $W \setminus B$–class. This proves that the set of mixed W $\setminus$ B–states contains a ball, i.e. is not of measure zero.

We discuss now some possible consequences of our results for PPTES of three qubits, for which the partial transposes ρ^{T_A}, ρ^{T_B} and ρ^{T_C} are positive. Any of these states can be decomposed as:

$$\rho = \lambda_S \rho_S + (1-\lambda_S)\delta \ , \tag{11}$$

where ρ_S is a separable state and δ is an edge state [20]. We conjecture that *PPTES cannot belong to the GHZ $\setminus$ W–class*, i.e. they are at most in the W–class. This conjecture is rigorous for states that have edge states with low ranks in the above decomposition. It was shown in [17] that for bipartite systems in $\mathcal{C}^2 \otimes \mathcal{C}^N$, the rank of PPTES must be larger than N, and if $r(\rho) \leq N$ and $\rho^{T_A} \geq 0$, then the state ρ is separable. Thus, any PPTES of three–qubits with $r(\rho) \leq 4$ is biseparable with respect to any partition; an example of such states are the UPB–states from Ref. [7].

For the case of higher ranks we can only give some support for our conjecture. We proceed as in [11], and observe first that it suffices to prove the conjecture for the edge states. For these states, the sum of ranks satisfies $r(\delta) + r(\delta^{T_A}) + r(\delta^{T_B}) + r(\delta^{T_C}) \leq 28$ [20]. Any PPT entangled state can only be detected by a non-decomposable entanglement witness, which in the case of tripartite systems has the canonical form $\mathcal{W}_{nd} = \mathcal{W}_d - \epsilon\mathbb{1}$ where $\mathcal{W}_d = P + \sum Q_X^{T_X}$ is a decomposable operator with $P, Q_X \geq 0$, $R(P) = K(\delta)$, $R(Q_X) = K(\delta^{T_X})$ for some edge state δ, and $X = A, B, C$ [20]. We restrict ourselves to edge states with the maximal sum of ranks, i.e. states δ with $(r(\delta), r(\delta^{T_A}), r(\delta^{T_B}), r(\delta^{T_C})) = (8,8,7,5), (8,8,6,6), (8,7,7,6), (7,7,7,7)$ and permutations. Indeed, if the conjecture is true for these states, it will be true for all edge states, and thus for all PPTES, since the edge states with maximal sum of ranks are dense in the set of all edge states [11]. We conjecture that for the case of edge states with maximal sum of ranks it is always possible to find a pure W–type vector, $|\phi_W\rangle$, such that for any non-decomposable witness $\mathcal{W}_{nd}$ of δ, $\langle\phi_W|\mathcal{W}_d|\phi_W\rangle \leq 0$, so that $\langle\phi_W|\mathcal{W}_{nd}|\phi_W\rangle < 0$. That means $\mathcal{W}_{nd}$ *cannot* be a GHZ–witness, so the edge state δ belongs to the W–class. If this holds for any δ it implies that all PPTES belong to the W–class.

Any W–vector can be obtained by local invertible operations applied to $|W\rangle$ i.e. can be written as $|\phi_W\rangle = \alpha_A|e_2, f_1, g_1\rangle + \alpha_B|e_1, f_2, g_1\rangle + \alpha_C|e_1, f_1, g_2\rangle$. We denote $|\Phi_A\rangle = |e_2^*, f_1, g_1\rangle$, $|\Psi_A\rangle = \alpha_B|e_1^*, f_2, g_1\rangle + \alpha_C|e_1^*, f_1, g_2\rangle$, $|\Phi_B\rangle = |e_1, f_2^*, g_1\rangle$, $|\Psi_B\rangle = \alpha_A|e_2, f_1^*, g_1\rangle + \alpha_C|e_1, f_1^*, g_2\rangle$, $|\Phi_C\rangle = |e_1, f_1, g_2^*\rangle$, $|\Psi_C\rangle = \alpha_A|e_2, f_1, g_1^*\rangle + \alpha_B|e_1, f_2, g_1^*\rangle$. In order to fulfill the condition $\langle\phi_W|\mathcal{W}_d|\phi_W\rangle \leq 0$ we demand that $Q_X|\Phi_X\rangle = 0$; $P|\phi_W\rangle = 0$, and $Q_X|\Psi_X\rangle = 0$ for $X = A, B, C$. The latter 4 conditions form 4 linear homogeneous equations for the α_X's, whose solutions exist if two 3×3 determinants vanish. Together with the first 3 conditions this gives at most 5 equations in the case $r(\delta) < 8$, and 6 equations in the worst case $r(\delta) = 8$, for the 6 complex parameters characterizing $|e_i\rangle, |f_i\rangle$, and $|g_i\rangle$, with $i = 1, 2$. For $r(\delta) < 8$ ($r(\delta) = 8$) one expects here a one complex parameter (finite, but large) family of solutions. At the same time $\langle\phi_W|\mathcal{W}_d|\phi_W\rangle = 2\,\mathrm{Re}\sum_X \alpha_X\langle\Psi_X^{*_X}|Q_X^{T_X}|\Phi_X^{*_X}\rangle$, (where $|\Phi^{*_X}\rangle$ denotes partial complex conjugation with respect to X) i.e. is a hermitian form of α_X's, whose diagonal elements vanish, since $|\Psi_X\rangle$ does not depend on α_X. Employing the freedom of choosing the solutions from the family, one expects to find at least one with $\langle\phi_W|\mathcal{W}_d|\phi_W\rangle \leq 0$. In this way we obtain the W–vector we were looking for. For the cases $(6,8,8,6)$ and $(5,8,8,7)$, a similar argu-

ment indeed shows that there should exist a biseparable state, $|\psi_B\rangle$, such that $\langle\psi_B|\mathcal{W}_{nd}|\psi_B\rangle < 0$. Note that the above method of searching $|\psi_W\rangle$ ($|\psi_B\rangle$) for a given δ, if successful, provides a sufficient condition for δ to belong to the W–class (B–class).

Finally, we present an example for a PPTES entangled edge state with ranks (7,7,7,7). We introduce

$$\rho = \frac{1}{n}\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & a & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & c & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{c} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{b} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{a} & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \tag{12}$$

with $a, b, c > 0$ and $n = 2 + a + 1/a + b + 1/b + c + 1/c$. The basis is $\{000, 001, 010, 011, 100, 101, 110, 111\}$. This density matrix has a positive partial transpose with respect to each subsystem. One sees immediately that $r(\rho) = r(\rho^{T_A}) = r(\rho^{T_B}) = r(\rho^{T_{AB}}) = 7$. In order to check that ρ is a PPT entangled edge state, one has to prove that it is impossible to find a product vector $|\phi\rangle \in R(\rho)$, such that at the same time $|\phi^{*_X}\rangle \in R(\rho^{T_X})$ for $X = A, B, C$. This, indeed, is not possible, as one readily concludes by looking at the kernels directly: one cannot find a product vector $|\phi\rangle$ that is orthogonal to $|000\rangle - |111\rangle$, whereas at the same time $|\phi^{*_A}\rangle \perp |011\rangle - c|100\rangle$, $|\phi^{*_B}\rangle \perp |010\rangle - b|101\rangle$, and $|\phi^{*_C}\rangle \perp |001\rangle - a|110\rangle$, unless the condition $ab = c$ is fulfilled. Thus, for generic a, b, c we have found a family of bound PPT entangled edge states of three qubits with maximal sum of ranks. By direct inspection we observe that ρ fulfills our conjecture, and is biseparable with respect to any partition. It can be written e.g. as a sum of separable projectors and a B–state acting in the 2×2 subspace spanned by Alice's space and the vectors $|00\rangle$ and $|11\rangle$ in Bob's–Charlie's space.

To summarize, we show that the set of density matrices for three qubits has an "onion" structure (see Fig.1) and contains convex compact subsets of states belonging to the separable S, biseparable B, W– and GHZ–class, respectively. We provide the canonical way of constructing witness operators for the GHZ– and W–class, and give the first examples of such witnesses. The study of the family of tripartite states given in Eq. (9) allows us to prove that the W–class is not of measure zero. We conjecture and give some evidence that all PPTES of three–qubit systems do not require GHZ–type pure states for their formation. We formulate a sufficient condition which allows to check constructively if a state belongs to the W–class (B–class). Finally, we present a family of PPT entangled edge states of three qubits with maximal sum of ranks.

This work has been supported by DFG (SFB 407 and Schwerpunkt "Quanteninformationsverarbeitung"), the ESF-Programme PESC, and the EU IST-Programme EQUIP. AA thanks the University of Hannover for hospitality, E. Jané for useful comments and the Spanish MEC (AP-98) for financial support.

[1] M. Horodecki, P. Horodecki and R. Horodecki in "Quantum Information - Basic Concepts and Experiments", Eds. G. Alber and M. Weiner, in print (Springer, Berlin, 2001); M. Lewenstein *et al.*, J. Mod. Phys. **47**, 2481 (2000), quant-ph/0006064.

[2] D.M. Greenberger, M. Horne and A. Zeilinger, *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, Ed. M. Kafatos (Kluwer, Dordrecht, 1989).

[3] D. Bouwmeester, A. Ekert, and A. Zeilinger (Eds.), "The Physics of Quantum Information", (Springer, Heidelberg, 2000), chapter 6 and references therein.

[4] A. Acín *et al.*, Phys. Rev. Lett. **85**, 1560 (2000), quant-ph/0003050; A. Acín *et al.*, quant-ph/0009107.

[5] H. A. Carteret, A. Higuchi and A. Sudbery, J. Math. Phys. **41**, 7932 (2000), quant-ph/0006125.

[6] W. Dür, G. Vidal and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000), quant-ph/0005115.

[7] C. H. Bennett *et al.*, Phys. Rev. Lett. **82**, 5385 (1999).

[8] S. L. Braunstein *et al.*, Phys. Rev. Lett. **83**, 1054 (1999); W. Dür and J. I. Cirac, Phys. Rev. A **61**, 042314 (2000); M. Horodecki, P. Horodecki, and R. Horodecki, quant-ph/0006071; M. Plenio and V. Vedral, quant-ph/0010080; T. Eggeling and R. F. Werner, quant-ph/0010096.

[9] J. Eisert and H.-J. Briegel, quant-ph/0007081.

[10] B. M. Terhal and P. Horodecki, Phys. Rev. A **61**, R040301 (2000), quant-ph/9911117.

[11] A. Sanpera, D. Bruß, M. Lewenstein, Phys. Rev. A, R03105PRA (2001), quant-ph/0009109.

[12] This implies that a GHZ–vector can be *approximately* transformed by LOCC into a W–vector with some probability, although the contrary is, in general, not possible.

[13] V. Coffman, J. Kundu and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).

[14] B. Terhal, Phys. Lett. A **271**, 319 (2000).

[15] M. Lewenstein *et al.*, Phys. Rev. A **62**, 052310 (2000), quant-ph/0005014; M. Lewenstein *et al.*, quant-ph/0005112.

[16] M. Lewenstein and A. Sanpera, Phys. Rev. Lett. **80**, 2261 (1998).

[17] B. Kraus *et al.*, Phys. Rev. A **61**, 062302 (2000), quant-ph/9912010.

[18] One can always symmetrize an asymmetric state without diminishing the overlap.

[19] The same overlaps have been found numerically by W. Dür.

[20] S. Karnas, PhD Thesis, Universität Hannover; S. Karnas and M. Lewenstein, quant-ph/0102115.

Appendix D

Three-party entanglement from positronium

A. Acín,* J. I. Latorre, and P. Pascual
Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain
(Received 18 August 2000; published 19 March 2001)

The decay of orthopositronium into three photons produces a physical realization of a pure state with three-party entanglement. Its quantum correlations are analyzed using recent results on quantum information theory, looking for the final state that has the maximal amount of Greenberger, Horne, and Zeilinger like correlations. This state allows for a statistical dismissal of local realism stronger than the one obtained using any entangled state of two spin one-half particles.

DOI: 10.1103/PhysRevA.63.042107 PACS number(s): 03.65.Ta, 03.67.−a, 12.20.−m

I. INTRODUCTION

Entanglement or quantum correlations between many space-separated subsystems has been recognized as one of the most intrinsic properties of quantum mechanics and provides the basis for many genuine applications of quantum information theory. It is, then, quite natural to look for physical situations in which quantum entangled states are obtained. Most of the theoretical and experimental effort has so far been devoted to unveil physical realizations of quantum states describing two quantum correlated subsystems. The search for physical systems displaying clean three-party entanglement is not simple. In this paper, we shall analyze decays of particles as a natural scenario for fulfilling such a goal. More precisely, we shall show that the decay of orthopositronium into three photons corresponds to a highly entangled state. Let us now review what entanglement can be used for and why it is interesting to look for quantum correlation between more than two particles.

In 1935 Einstein, Podolsky, and Rosen [1], starting from three reasonable assumptions of locality, reality, and completeness that every physical theory must satisfy, argued that quantum mechanics (QM) is an incomplete theory. They did not question quantum mechanics predictions but rather quantum mechanics interpretation [2]. Their argument was based on some inconsistencies between quantum mechanics and their local-realistic premises (LR) that appear for quantum states of bipartite systems, $|\psi\rangle \in \mathcal{H}_{d_1} \otimes \mathcal{H}_{d_2}$. It was in 1964 when Bell [3] showed that any theory compatible with LR assumptions cannot reproduce some of the statistical predictions of QM, using a gedankenexperiment proposed in Ref. [4] with two quantum correlated spin-$\frac{1}{2}$ particles in the singlet state

$$|s\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \tag{1}$$

In his derivation, as it is well-known, quantum correlations or entanglement have a crucial role. Actually, the singlet state is known to be the maximally entangled state between two particles. The conflict between LR and QM arises since the latter violates some experimentally verifiable inequalities, called Bell inequalities, that any theory according to the local-realistic assumptions ought to satisfy. It is then possible to design real experiments testing QM against LR (for a detailed discussion see Ref. [5]). Correlations of linear polarizations of pair of photons were measured in 1982 showing strong agreement with quantum mechanics predictions and violating Bell inequalities [6]. Nowadays, Bell inequalities have been tested thoroughly in favor of QM [7].

More recently, it has been pointed out that some predictions for quantum systems having quantum correlations between more than two particles give a much stronger conflict between LR and QM than any entangled state of two particles. The maximally entangled state between three spin-$\frac{1}{2}$ particles, the so-called Greenberger, Horne, and Zeilinger (GHZ) state [8]

$$|\mathrm{GHZ}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{2}$$

shows some perfect correlations incompatible with any LR model (see Ref. [2] and also Ref. [9] for more details). It is then of obvious relevance to obtain these GHZ-like correlations. Producing experimentally a GHZ state has turned out to be a real challenge yet a controlled instance has been produced in a quantum optics experiment [10].

Entanglement is then important for our basic understanding of quantum mechanics. Recent developments on quantum information have furthermore shown that it is also a powerful resource for quantum information applications. For instance, teleportation [11] uses entanglement in order to obtain surprising results, which are impossible in a classical context. A lot of work has been performed trying to know how entanglement can be quantified and manipulated. Our aim in this paper consists on looking for GHZ-like correlations, which are truly three-party pure state entanglement, in the decay of orthopositronium to three photons. The choice of this physical system has been motivated mainly by several reasons. First, decay of particles seems a very natural source of entangled particles. Indeed, positronium decay to two photons was one of the physical systems proposed a long time ago as a source of two entangled space-separated particles [12]. On a different line of thought, some experiments for testing quantum mechanics have been recently proposed using correlated neutral kaons coming from the decay of a ϕ meson [13]. In the case of positronium, three entangled pho-

*Email address: acin@ecm.ub.es

tons are obtained in the final state, so it offers the opportunity of analyzing a quantum state showing three-party correlations similar to other experiments in quantum optics.

The structure of the paper goes as follows. We first review the quantum states emerging in both para- and orthopositronium decays. Then, we focus on their entanglement properties and proceed to a modern analysis of the three-photon decay state of orthopositronium. Using techniques developed in the context of quantum information theory, we show that this state allows in principle for an experimental test of QM finer than the ones based on the use of the singlet state. We have tried to make the paper self-contained and easy to read for both particle physicists and quantum information physicists. The former can find a translation of some of the quantum information ideas to a well-known situation, that is, the positronium decay to photons, while the latter can see an application of the very recent techniques obtained for three-party entangled states, which allow to design a QM vs LR test for a three-particle system in a situation different from the GHZ state.

II. POSITRONIUM DECAYS

A. Positronium properties

Let us start remembering some basic facts about positronium. Positronium corresponds to a e^+e^- bound state. These two spin-$\frac{1}{2}$ particles can form a state with total spin equal to zero, parapositronium (p-Ps), or equal to one, orthopositronium (o-Ps). Depending on the value of its angular momentum, it can decay to an even or an odd number of photons as we shall see shortly.

Positronium binding energy comes from the Coulomb attraction between the electron and the positron. In the nonrelativistic limit, its wave function is [14]

$$\Psi(r)=\frac{1}{\sqrt{\pi a^3}}e^{-(r/a)}$$

$$=\int\frac{d^3p}{(2\pi)^{3/2}}e^{i\vec{p}\cdot\vec{r}}\tilde{\Psi}(\vec{p})$$

$$=\int\frac{d^3p}{(2\pi)^{3/2}}e^{i\vec{p}\cdot\vec{r}}\frac{\sqrt{8a^3}}{\pi(1+a^2p^2)^2}, \qquad (3)$$

where $a=2/(m\alpha)$, i.e., twice the Bohr radius of atomic hydrogen, and m is the electron mass. Note that the wave function takes significant values only for three momenta such that $p\lesssim 1/a\ll m$, which is consistent with the fact that the system is essentially nonrelativistic.

The parity and charge conjugation operators are equal to

$$U_P=(-1)^{L+1},\quad U_C=(-1)^{L+S}, \qquad (4)$$

where L and S are the orbital and spin angular momentum. Positronium states are then classified according to these quantum numbers so that the ground states are ${}^1S_0$, with $J^{PC}=0^{-+}$, for the p-Ps and ${}^3S_1+{}^3D_1$, having $J^{PC}=1^{--}$, for the o-Ps.

Positronium is an unstable bound state that can decay to photons. Since a n-photon state transforms as $U_C|n\gamma\rangle=(-1)^n|n\gamma\rangle$ under charge conjugation, which is an exact discrete symmetry for any QED process such as the decay of positronium, we have that the ground state of p-Ps (o-Ps) decays to an even (odd) number of photons [15]. The analysis of the decay of positronium to photons can be found in a standard QED textbook [14]. Parapositronium lifetime is about 0.125 ns, while for the case of orthopositronium the lifetime is equal to approximately 0.14 μs [16].

The computation of positronium decays is greatly simplified due to the following argument. The scale that controls the structure of positronium is of the order of $|\vec{p}|\sim\alpha m$. On the other hand, the scale for postrinomium annihilation is of the order of m. Therefore, it is easy to prove that positronium decays are only sensitive to the value of the wave function at the origin. As a consequence, it is possible to factor out the value of the wave function from the tree-level QED final-state computation [14]. A simple computation of Feymann diagrams will be enough to write the precise structure of momenta and polarizations that describe the positronium decays. Furthermore, only tree-level amplitudes need to be computed since higher corrections are suppressed by one power of α. Let us now proceed to analyze the decays of p-Ps and o-Ps in turn.

B. Parapositronium decay

Parapositronium ground state decays into two photons. Because of the argument mentioned above, the determination of the two-photon state coming from the p-Ps decay is simply given by the lowest-order Feynmann diagram of $e^+e^-\rightarrow\gamma\gamma$. Since positronium is a nonrelativistic particle to a very good approximation, the three momenta of e^+ and e^- are taken equal to zero, and the corresponding spinors are replaced by a two-component spin. This implies that the tree-level calculation of the annihilation of p-Ps into two photons is equal to, up to constants,

$$\mathcal{M}(e^+e^-\rightarrow\gamma\gamma)\sim\chi_+^{c\dagger}M_2\chi_-, \qquad (5)$$

where (see Ref. [14] for more details) $\chi_\pm$ is the two-component spinor describing the fermions, $\chi^{c\dagger}\equiv\chi^T i\sigma_2$, and M_2 gives

$$M_2=\sum_{perm}(\vec{\epsilon}_1^{\,*}\times\vec{\epsilon}_2^{\,*})\cdot\hat{k}I_{2\times2}\equiv A(\hat{k}_1,\lambda_1;\hat{k}_2,\lambda_2)I_{2\times2}, \qquad (6)$$

where $\vec{\epsilon}_i^{\,*}\equiv\vec{\epsilon}^{\,*}(\hat{k}_i,\lambda_i)$ stands for the circular polarization vector associated to the outgoing photon i and $I_{2\times2}$ is the 2×2 identity matrix. More precisely, for a photon having the three-momentum vector $\vec{k}=|\vec{k}|\hat{k}=|\vec{k}|(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$, the polarization vectors can be chosen

$$\vec{\epsilon}(\hat{k},\lambda)=-\frac{\lambda}{\sqrt{2}}(\cos\theta\cos\phi-i\lambda\sin\phi,\cos\theta\sin\phi + i\lambda\cos\phi,-\sin\theta), \tag{7}$$

where $\lambda=\pm 1$ and they obey

$$\hat{k}\cdot\vec{\epsilon}(\hat{k},\lambda)=0,\quad \hat{k}\times\vec{\epsilon}(\hat{k},\lambda)=-i\lambda\vec{\epsilon}(\hat{k},\lambda),$$

$$\vec{\epsilon}(\hat{k}_i,\lambda_i)\cdot\vec{\epsilon}(\hat{k}_j,\lambda_j)=-\tfrac{1}{2}(1-\lambda_i\lambda_j\hat{k}_i\cdot\hat{k}_j). \tag{8}$$

From the expressions of the polarizaton vectors and the three-momentum and energy conservation, it follows that the scalar term A is

$$A(\hat{k},\lambda_1;-\hat{k},\lambda_2)=-\frac{i}{2}(\lambda_1+\lambda_2), \tag{9}$$

and it verifies

$$A(\hat{k},+1;-\hat{k},+1)=-A(\hat{k},-1;-\hat{k},-1),$$

$$A(\hat{k},+1;-\hat{k},-1)=-A(\hat{k},+1;-\hat{k},-1)=0. \tag{10}$$

The two fermions in the parapositonium ground state are in the singlet state, $|S=0,S_z=0\rangle=1/\sqrt{2}(|\frac{1}{2},-\frac{1}{2}\rangle-|-\frac{1}{2},\frac{1}{2}\rangle)$, and then, using the previous relations for A and Eq. (5), the two-photon state results of the p-Ps desintegration is

$$|\psi_p\rangle=\frac{1}{\sqrt{2}}(|++\rangle-|--\rangle). \tag{11}$$

The two-photon state resulting from p-Ps decay is thus equivalent to a maximally entangled state of two spin-$\frac{1}{2}$ particles. This is a well-known result and was, actually, one of the physical system first proposed as a source of particles having the quantum correlations needed to test QM vs LR [12].

C. Orthopositronium decay

The ground state of orthopositronium has $J^{PC}=1^{--}$ and, due to the fact that charge conjugation is conserved, decays to three photons. Repeating the treatment performed for the p-Ps annihilation, the determination of the three-photon state resulting from the o-Ps decay requires the simple calculation of the tree-level Feynmann diagrams corresponding to $e^+e^-\rightarrow\gamma\gamma\gamma$. Its tree-level computation gives, up to constants,

$$\mathcal{M}(e^+e^-\rightarrow\gamma\gamma\gamma)\sim\chi_+^{c\dagger}M_3\chi_-, \tag{12}$$

and the 2×2 matrix M_3 is equal to [14]

$$M_3=\sum_{\text{cyclic perm.}}[(\vec{\epsilon}_2^{\,*}\cdot\vec{\epsilon}_3^{\,*}-\vec{\delta}_2\cdot\vec{\delta}_3)\vec{\epsilon}_1^{\,*} + (\vec{\epsilon}_2^{\,*}\cdot\vec{\delta}_3+\vec{\epsilon}_3^{\,*}\cdot\vec{\delta}_2)\vec{\delta}_1]\cdot\vec{\sigma}, \tag{13}$$

where

$$\vec{\delta}_i=\vec{k}_i\times\vec{\epsilon}_i^{\,*}. \tag{14}$$

Using Eq. (8) we can rewrite M_3 in the following way:

$$M_3\equiv\vec{\sigma}\cdot\vec{V}(\hat{k}_1,\lambda_1;\hat{k}_2,\lambda_2;\hat{k}_3,\lambda_3), \tag{15}$$

where

$$\vec{V}=\{(\lambda_1-\lambda_2)(\lambda_2+\lambda_3)\,\vec{\epsilon}^{\,*}(\hat{k}_1,\lambda_1)[\vec{\epsilon}^{\,*}(\hat{k}_2,\lambda_2)\cdot\vec{\epsilon}^{\,*}(\hat{k}_3,\lambda_3)] + (\lambda_2-\lambda_3)(\lambda_3+\lambda_1)\vec{\epsilon}^{\,*}(\hat{k}_2,\lambda_2)[\vec{\epsilon}^{\,*}(\hat{k}_3,\lambda_3)\cdot\vec{\epsilon}^{\,*}(\hat{k}_1,\lambda_1)] + (\lambda_3-\lambda_1)(\lambda_1+\lambda_2)\,\vec{\epsilon}^{\,*}(\hat{k}_3,\lambda_3) \times[\vec{\epsilon}^{\,*}(\hat{k}_1,\lambda_1)\cdot\vec{\epsilon}^{\,*}(\hat{k}_2,\lambda_2)]\}. \tag{16}$$

Notice that the helicity coefficient $(\lambda_i-\lambda_j)(\lambda_j+\lambda_k)$ for the cyclic permutations of ijk explicitly enforces the vanishing of the $(+++)$ and $(---)$ polarizations,

$$\vec{V}(\hat{k}_1,+;\hat{k}_2,+;\hat{k}_3,+)=\vec{V}(\hat{k}_1,-;\hat{k}_2,-;\hat{k}_3,-)=0. \tag{17}$$

Furthermore, it is easy to see that

$$\vec{V}(\hat{k}_1,-;\hat{k}_2,+;\hat{k}_3,+)=2\vec{\epsilon}^{\,*}(\hat{k}_1,-)(1-\hat{k}_2\cdot\hat{k}_3),$$

$$\vec{V}(\hat{k}_1,+;\hat{k}_2,-;\hat{k}_3,-)=2\vec{\epsilon}^{\,*}(\hat{k}_1,+)(1-\hat{k}_2\cdot\hat{k}_3), \tag{18}$$

and similar expressions for the other cyclic terms.

The original e^+e^- in the orthopositronium could be in any of the three triplet states. It can be shown, using Eqs. (12) and (15), that when the initial positronium state is $|S=1,S_z=1\rangle=|\frac{1}{2},\frac{1}{2}\rangle$, the decay amplitude is proportional to V_1+iV_2, while the same argument gives $-V_1+iV_2$ for $|S=1,S_z=-1\rangle=|-\frac{1}{2},-\frac{1}{2}\rangle$ and $-\sqrt{2}V_3$ for $|S=1,S_z=0\rangle=1/\sqrt{2}(|\frac{1}{2},-\frac{1}{2}\rangle+|-\frac{1}{2},\frac{1}{2}\rangle)$. Now, considering the explicit expressions of the polarization vectors (7), with $\theta=\pi/2$ without loss of generality, and Eq. (18), it is easy to see that the three-photon state coming from the o-Ps decay is, up to normalization,

$$|\psi_0(\hat{k}_1,\hat{k}_2,\hat{k}_3)\rangle=(1-\hat{k}_1\cdot\hat{k}_2)(|++-\rangle+|--+\rangle) + (1-\hat{k}_1\cdot\hat{k}_3)(|+-+\rangle+|-+-\rangle) + (1-\hat{k}_2\cdot\hat{k}_3)(|-++\rangle+|+--\rangle), \tag{19}$$

when the third component of the orthopositronium spin S_z, is equal to zero, and

$$|\psi_1(\hat{k}_1,\hat{k}_2,\hat{k}_3)\rangle=(1-\hat{k}_1\cdot\hat{k}_2)(|++-\rangle-|--+\rangle) + (1-\hat{k}_1\cdot\hat{k}_3)(|+-+\rangle-|-+-\rangle) + (1-\hat{k}_2\cdot\hat{k}_3)(|-++\rangle-|+--\rangle) \tag{20}$$

when $S_z=\pm 1$.

The final state of the o-Ps decay is, thus, an entangled state of three photons, whose quantum correlations depend on the angles among the momenta of the outgoing three photons. For the rest of the paper we will consider the first family of states ($S_z=0$) although equivalent conclusions are valid for the second one. In the next sections we will analyze the entanglement properties of the states $|\psi_0(\hat{k}_1,\hat{k}_2,\hat{k}_3)\rangle$, using some of the quantum information techniques and comparing them to the well-known cases of the singlet and GHZ state.

III. ENTANGLEMENT PROPERTIES

The quantum correlations of the three-photon entangled state obtained from the o-Ps annihilation depend on the position of the photon detectors, i.e., on the photon directions we are going to measure. Our next aim will be to choose from the family of states given by Eq. (19), the one that, in some sense, has the maximum amount of GHZ-like correlations. In order to do this, we first need to introduce some recent results on the study of three-party entanglement.

The set of states $|\psi_0(\hat{k}_1,\hat{k}_2,\hat{k}_3)\rangle$ form a six-parameter dependent family in the Hilbert space $\mathcal{H}_2\otimes\mathcal{H}_2\otimes\mathcal{H}_2$, so that each of its components is equivalent to a state describing three spin-$\frac{1}{2}$ particles or three qubits (a qubit, or quantum bit, is the quantum version of the classical bit and corresponds to a spin-$\frac{1}{2}$ particle). Two pure states belonging to a generic composite system $\mathcal{H}_d^{\otimes N}$, i.e., N parties each having a d-dimensional Hilbert space, are equivalent as far as their entanglement properties go when they can be transformed one into another by local unitary transformations. This argument gives a lower bound for the entanglement parameters a generic state $|\phi\rangle\in\mathcal{H}_2^{\otimes N}$ depends on. Since the number of real parameters for describing it is 2^{N+1}, and the action of an element of the group of local unitary transformations $\mathrm{U}(2)^{\otimes N}$ is equivalent to the action of $\mathrm{U}(1)\times\mathrm{SU}(2)^{\otimes N}$, which depends on $3N+1$ real parameters, the number of entanglement parameters is bounded by $2^{N+1}-(3N+1)$. For our case this counting of entanglement parameters gives six, since we have $N=3$, and it can be proved that this is indeed the number of nonlocal parameters describing a state in $\mathcal{H}_2\otimes\mathcal{H}_2\otimes\mathcal{H}_2$ [17].

The above arguments imply that six independent quantities invariant under the action of the group of local unitary transformations will be enough, up to some discrete symmetry, to describe the entanglement properties of any three-qubit pure state. Given a generic state $|\phi\rangle\in\mathcal{H}_2^{\otimes 3}$:

$$|\phi\rangle=\sum_{i,j,k} t_{ijk}|ijk\rangle,\quad i,j,k=1,2, \tag{21}$$

where $|i\rangle,|j\rangle,|k\rangle$ are the elements of a basis in each subsystem, A, B, and C, the application of three local unitary transformations U^A, U^B, and U^C transforms the coefficients t_{ijk} into

$$t'_{ijk}=\sum U^A_{i\alpha}U^B_{j\beta}U^C_{k\gamma}t_{\alpha\beta\gamma}. \tag{22}$$

From this expression it is not difficult to build polynomial combinations of the coefficient t_{ijk}, which are invariant under local unitary transformations [17,18]. These quantities are good candidates for being an entanglement parameter. For example, one of these invariants is

$$\sum t_{i_1j_1k_1}t^*_{i_1j_2k_2}t_{i_2j_2k_2}t^*_{i_2j_1k_1}=\mathrm{tr}(\rho_A^2), \tag{23}$$

where $\rho_A=\mathrm{tr}_{BC}(|\phi\rangle\langle\phi|)$ is the density matrix describing the local quantum state of A (and the same happens for B and C). In Ref. [18] the six linearly independent polynomial invariants of minor degree were found (a trivial one is the norm) and a slightly modified version of these quantities was also proposed in Ref. [19]. In the rest of the paper we will not consider the norm, so the space of entanglement parameters of the normalized states belonging to $\mathcal{H}_2\otimes\mathcal{H}_2\otimes\mathcal{H}_2$ has dimension equal to five.

A particularly relevant polynomial invariant is the square concurrence, τ, introduced in [20]. There is strong evidence that somehow it is a measure of the amount of GHZ state character of a state [19–22]. It corresponds to the modulus of the hyperdeterminant of the hypermatrix given by the coefficients t_{ijk} [23], which from Eq. (21) corresponds to

$$\begin{aligned}\tau(|\phi\rangle)&=|\mathrm{Hdet}(t_{ijk})|\\&=\Big|\sum \epsilon_{i_1i_2}\epsilon_{i_3i_4}\epsilon_{j_1j_2}\epsilon_{j_3j_4}\epsilon_{k_1k_3}\epsilon_{k_2k_4}\\&\quad\times t_{i_1j_1k_1}t_{i_2j_2k_2}t_{i_3j_3k_3}t_{i_4j_4k_4}\Big|,\end{aligned} \tag{24}$$

where $\epsilon_{00}=\epsilon_{11}=0$ and $\epsilon_{01}=-\epsilon_{10}=1$. This quantity can be shown to be symmetric under permutation of the indices i,j,k.

Because of the interpretation of the square concurrence as a measure of the GHZ-like correlations, we will choose the position of the photon detectors, from the set of states (19), the ones that are associated with a maximum square concurrence. In Fig. 1 is shown the variation of the square concurrence with the position of the detectors. It is not difficult to see that the state of Eq. (19) with maximum square concurrence corresponds to the case $\hat{k}_1\cdot\hat{k}_2=\hat{k}_1\cdot\hat{k}_3=\hat{k}_2\cdot\hat{k}_3=-\frac{1}{2}$, i.e., the most symmetric configuration. The normalized state obtained from Eq. (19) for this geometry is

$$\begin{aligned}|\psi\rangle=\frac{1}{\sqrt{6}}(&|++-\rangle+|--+\rangle+|+-+\rangle+|-++\rangle\\&+|-++\rangle+|+--\rangle).\end{aligned} \tag{25}$$

Note that the GHZ state has an square concurrence equal to $\frac{1}{4}$, while the value of the square concurrence of (25) is lower,

$$\tau(|\psi\rangle)=\tfrac{1}{12}. \tag{26}$$

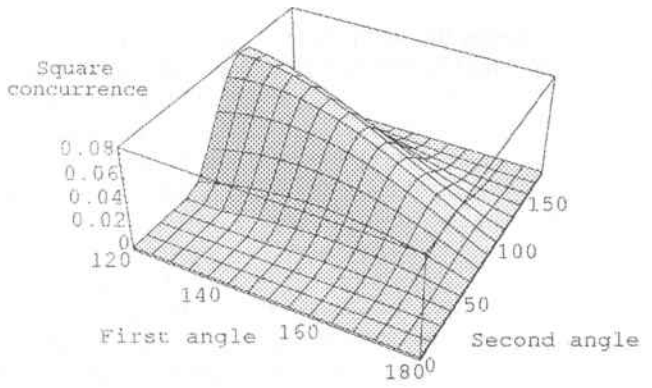


FIG. 1. Variation of the square concurrence with the position of the photon detectors, that are represented by two angles (in degrees), the third one has to sum up to 360°. We have taken $\tau=0$ when the position of the detectors, i.e., the photon trajectories, are incompatible with momentum conservation.

It is arguable that the most symmetric geometry was naturally expected to produce a maximum square concurrence state. Indeed, GHZ-like quantum correlations do not singularize any particular qubit.

Let us also mention that the state we have singled out has some nice properties from the point of view of group theory. It does correspond to the sum of two of the elements of the coupled basis resulting from the tensor product of three spin-$\frac{1}{2}$ particles, $\frac{1}{2}\otimes\frac{1}{2}\otimes\frac{1}{2}$, [24]

$$|\psi\rangle=1/\sqrt{2}(|\tfrac{3}{2},+\tfrac{1}{2}\rangle+|\tfrac{3}{2},-\tfrac{1}{2}\rangle), \tag{27}$$

where

$$|\tfrac{3}{2},+\tfrac{1}{2}\rangle=1/\sqrt{3}(|++-\rangle+|+-+\rangle+|-++\rangle),$$

$$|\tfrac{3}{2},-\tfrac{1}{2}\rangle=1/\sqrt{3}(|--+\rangle+|-+-\rangle+|+--\rangle). \tag{28}$$

The quantum correlations of Eq. (25) will be now analyzed.

IV. USEFUL DECOMPOSITIONS

In this section, the state (25) will be rewritten in some different forms that will help us to understand better its nonlocal properties. First, let us mention that for any generic three-qubit pure state and by performing change of local bases, it is possible to make zero at least three of the coefficients t_{ijk} of Eq. (21) [19,25]. A simple counting of parameters shows that this is in fact the expected number of zeros. This means that by a right choice of the local bases, any state can be written with the minimum number of coefficients t_{ijk}, i.e., we are left with all the nonlocal features of the state, having removed all the "superfluous" information due to local unitary tranformations. For the case of the state (25) it is easy to prove [26] that it can be expressed as

$$|\psi\rangle=\frac{1}{2\sqrt{3}}(|001\rangle+|010\rangle+|100\rangle)+\frac{\sqrt{3}}{2}|111\rangle, \tag{29}$$

which is the minimum decomposition in terms of product states built from local bases (four of the coefficients t_{ijk} are made equal to zero).

An alternative decomposition, that will prove to be fruitful for the rest of the paper, consists of writing the state as a sum of two product states. This decomposition is somewhat reminiscent of the form of the GHZ state, which is a sum of just two product states, and is only possible when the square concurrence is different from zero [19,21] as it happens for our state [see (26)]. The state then can be written as

$$|\psi\rangle=\frac{2}{3}\left[\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}+\begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix}\otimes\begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix}\right]$$

$$\equiv\alpha(|000\rangle+|aaa\rangle), \tag{30}$$

where

$$|0\rangle\equiv\begin{pmatrix}1\\0\end{pmatrix}$$

and

$$a\equiv\begin{pmatrix}\frac{1}{2}\\\frac{\sqrt{3}}{2}\end{pmatrix}.$$

We omit the details for the explicit computation of this expression since they can be found in Refs. [19,21]. It is worth noticing that o-Ps decay is hereby identified to belonging to an interesting type of states already classified in quantum information theory [21].

The above decomposition allows for an alternative interpretation of the initial state as an equally weighted sum of two symmetric product states. Note that the Bloch vector, $\hat{n}=(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$, representing the first local spinor appearing in Eq. (30) is pointing to the z axis, i.e., $\hat{n}_1=(0,0,1)$, while the second is located in the XZ plane with an angle of 120° with the z axis, i.e., $\hat{n}_2=(\sqrt{3}/2,0,-(1/2))$. By performing a new unitary transformation, Eq. (30) can be written as

$$|\psi\rangle=\frac{2}{3}\left[\begin{pmatrix}c\\s\end{pmatrix}\otimes\begin{pmatrix}c\\s\end{pmatrix}\otimes\begin{pmatrix}c\\s\end{pmatrix}+\begin{pmatrix}s\\c\end{pmatrix}\otimes\begin{pmatrix}s\\c\end{pmatrix}\otimes\begin{pmatrix}s\\c\end{pmatrix}\right], \tag{31}$$

where $c=\cos 15°$, and $s=\sin 15°$. Now, the two Bloch vectors are in the XZ plane, pointing to the $\theta=30°$ and $\theta=150°$ directions. The GHZ state corresponds to the particular case $c=1$ and $s=0$.

V. QUANTUM MECHANICS VS LOCAL REALISM

The quantum correlations present in some three-qubit pure states show, as it was mentioned in the Introduction, a much stronger disagreement with the predictions of a local-realistic model than any two-qubit entangled state. In fact, contrary to the case of the singlet state, no LR model is able to reproduce all the perfect correlations predicted for the maximally entangled state of three qubits [2]. The state (25) emerging from o-Ps decay is not a GHZ state, although it has been chosen as the one with the maximum tangle in order to maximize GHZ-like correlations. In this section we will show how to use it for testing quantum mechanics against local-realistic models, and then we will compare its performance against existing tests for the maximally entangled states of two and three spin-$\frac{1}{2}$ particles. We start reviewing some of the consequences derived from the arguments proposed in Ref. [1].

A. QM vs LR conflict

Given a generic quantum state of a composite system shared by N parties, there should be an alternative LR theory that reproduces all its statistical predictions. In this LR model, a state denoted by λ will be assigned to the system specifying all its elements of physical reality. In particular, the result of a measurement depending on a set of parameters $\{n\}$ performed locally by one of the parties, say A, will be specified by a function $a_\lambda(\{n\})$. The same will happen for each of the space-separated parties and, since there is no causal influence among them, the result measured on A cannot modify the measurement on B. For example, if the measurement is of the Stern-Gerlach type, the parameters labeling the measurement are given by a normalized vector $\hat{n}$ and $a_\lambda(\hat{n})\equiv a$ are the LR functions describing the outcome.

The LR model can be very general provided that some conditions must be satisfied. Consider a generic pure state belonging to $\mathcal{H}_2\otimes\mathcal{H}_2\otimes\mathcal{H}_2$ shared by three observers A, B, and C, which are able to perform Stern-Gerlach measurements in any direction. Since the outcomes of a Stern-Gerlach measurement are only ± 1, it is easy to check that for any pair of measurements on each subsystem, described by the LR functions a and a', b and b', c and c', and for all their possible values, it is always verified

$$a'bc+ab'c+abc'-a'b'c'=\pm 2. \tag{32}$$

It follows from this relation that

$$-2\leqslant\langle a'bc+ab'c+abc'-a'b'c'\rangle\leqslant 2. \tag{33}$$

This constraint is known as the Mermin inequality [27] and has to be satisfied by any LR model describing three space-separated systems.

Let us now take the GHZ state (2). It is quite simple to see that if the observables a and a' are equal to σ_y and σ_x (the same for parties B and C), the value of Eq. (33) is -4, so an experimental condition is found that allows to test quantum mechanics against local realism. Note that this is the maximal violation of inequality (33). Moreover, the GHZ state also satisfies that $a'bc=ab'c=abc'=-a'b'c'=-1$ and no LR model is able to take into account this perfect correlation result because of Eq. (32) [2]. This is a new feature that does not appear for the case of a two maximally entangled state of two spin-$\frac{1}{2}$ particles. In this sense it is often said that a most dramatic contrast between QM and LR emerges for entanglement between three subsystems.

Let us go back to the state given by the orthopositronium decay (25). Our aim is to design an experimental situation where a conflict between QM and LR appears, so we will look for the observables that give a maximal violation of Eq. (33). Such observables will extremize that expression. Using the decomposition (31), the expectation value of three local observables is

$$\begin{aligned}\langle abc\rangle&=\langle\psi|(\hat{n}_a\cdot\vec{\sigma})\otimes(\hat{n}_b\cdot\vec{\sigma})\otimes(\hat{n}_c\cdot\vec{\sigma})|\psi\rangle\\&=\frac{4}{9}\Bigg(\prod_{i=a,b,c}(\bar{c}\cos\theta_i+\bar{s}\sin\theta_i\cos\phi_i)\\&\quad+\prod_{i=a,b,c}(-\bar{c}\cos\theta_i+\bar{s}\sin\theta_i\cos\phi_i)\\&\quad+\prod_{i=a,b,c}\sin\theta_i(c^2e^{-i\phi_i}+s^2e^{i\phi_i})\\&\quad+\prod_{i=a,b,c}\sin\theta_i(c^2e^{i\phi_i}+s^2e^{-i\phi_i})\Bigg),\end{aligned} \tag{34}$$

where $\bar{c}\equiv c^2-s^2$ and $\bar{s}\equiv 2sc$. Because of the symmetry of the state under permutation of parties, the Stern-Gerlach directions are taken satisfying $\hat{n}_a=\hat{n}_b=\hat{n}_c=(\sin\theta\cos\phi,\sin\theta\sin\phi,\cos\theta)$ and $\hat{n}_{a'}=\hat{n}_{b'}=\hat{n}_{c'}=(\sin\theta'\cos\phi',\sin\theta'\sin\phi',\cos\theta')$. Substituting this expression in Eq. (33), we get the explicit function $f(\theta,\phi,\theta',\phi')$ to be extremized. For the case of the GHZ state described above, the extreme values were obtained using two observables with $\theta=\theta'=\pi/2$, i.e., in the XY plane. Since Eq. (31) is the GHZ-like decomposition of the initial state, we take $\theta=\theta'=\pi/2$ and it is easy to check that in this case

$$\left.\frac{\partial f}{\partial\theta}\right|_{\theta=\theta'=\pi/2}=\left.\frac{\partial f}{\partial\theta'}\right|_{\theta=\theta'=\pi/2}=0,\quad\forall\phi,\phi'.$$

Mantaining the parallelism with the GHZ case, it can be seen that all the partial derivatives vanish when it is also imposed $\phi=\pi/2$ and $\phi'=0$. In our case the calculation of Eq. (33) gives -3, so a conflict between local-realistic models and quantum mechanics again appears, and then the three-photon state coming from the orthopositronium decay can be used, in principle, to test QM vs LR with the set of observables given by the normalized vectors

$$\hat{n}_a=\hat{n}_b=\hat{n}_c=(0,1,0),\quad\hat{n}_{a'}=\hat{n}_{b'}=\hat{n}_{c'}=(1,0,0). \tag{35}$$

There is an alternative set of angles ϕ and ϕ' that makes zero all the partial derivatives of f: the combination of local observables (33) is equal to ≈ -3.046 for

$$\phi' = \arctan\left(-\frac{\sqrt{17+27\sqrt{41}}}{10}\right) \approx 126^\circ,$$

$$\phi = \frac{1}{2}\arctan\left(\frac{2\sqrt{17+27\sqrt{41}}}{25}\right) \approx 24^\circ. \tag{36}$$

This second set of parameters will be seen to produce in the end a weaker dismissal of LR.

Our next step will be to carry over the comparison of this QM vs LR test against the existent ones for the maximally entangled states of three and two spin-$\frac{1}{2}$ particles, i.e., the GHZ and singlet state. It is quite evident that the described test should be worse than that obtained for the GHZ state. It is less obvious how this new situation will compare with the singlet case.

B. Comparison with the maximally entangled states of two and three spin-$\frac{1}{2}$ particles

We will now estimate the "strength" of the QM vs LR test proposed above, being the "strength" measured by the number of trials needed to rule out local realism at a given confidence level, as Peres did in Ref. [28]. A reasoning anologous to the one given in Ref. [28] will be done here for the state (25) and the observables (35).

Imagine a local-realistic physicist who does not believe in quantum mechanics. He assigns prior subjective probabilities to the validity of LR and QM, p_r and p_q, expressing his personal belief. Take for instance $p_r/p_q = 100$. His LR theory is not able to reproduce exactly all the QM statistical results of some quantum states. Consider the expectation value of some observable $\mathcal{O}$ with two outcomes ± 1 such that $\langle \mathcal{O} \rangle = E_q$ is predicted for some quantum state, while LR gives $\langle \mathcal{O} \rangle = E_r \neq E_q$. Since the value of the two possible outcomes are ± 1, the probablity of having $\mathcal{O} = +1$ is $q = (1 + E_q)/2$ for QM and $r = (1 + E_r)/2$ for LR. An experimental test of the observable $\mathcal{O}$ now is performed n times yielding m times the result $+1$. The prior probabilities p_q and p_r are modified according to the Bayes theorem and their ratio has changed to

$$\frac{p_r'}{p_q'} = \frac{p_r}{p_q}\frac{p(m|_{\mathrm{LR}})}{p(m|_{\mathrm{QM}})}, \tag{37}$$

where

$$p(m|_{\mathrm{LR}}) = \binom{n}{m} r^m (1-r)^{n-m} \tag{38}$$

is the LR probability of having m times the outcome $+1$, and we have the same for $p(m|_{\mathrm{QM}})$, being r replaced by q. Following Peres [28], the *confidence depressing factor* is defined

$$D \equiv \frac{p(m|_{\mathrm{QM}})}{p(m|_{\mathrm{LR}})} = \left(\frac{q}{r}\right)^m \left(\frac{1-q}{1-r}\right)^{n-m}, \tag{39}$$

which accounts for the change in the ratio of the probabilities of the two theories, i.e., it reflects how the LR belief changes with the experimental results. Like in a game, our aim is to destroy as fast as we can, the LR faith of our friend by choosing an adequate experimental situation. It can be said, for example, that he will give up when, for example, $D = 10^4$. Since the world is quantum, $m = qn$, and the number of experimental tests needed to obtain $D = 10^4$ is equal to

$$n_D(q,r) \equiv \frac{4}{q\log_{10}\left(\frac{q}{r}\right) + (1-q)\log_{10}[(1-q)/1-r]} = \frac{4}{K(q,r)}, \tag{40}$$

being $K(q,r)$ the information distance [29] between the QM and LR binomial distribution for the outcome $+1$. The more separate the two probability distributions are, measured in terms of the information distance, the fewer the number of experiments n_D is.

Let us come back to the three-party entangled state coming from the orthopositronium decay (25) under the local measurements described by Eq. (35). As it has been shown above, a contradiction with any LR model appears for the combination of the observables given by the Mermin inequality. In our case quantum mechanics gives the following predictions:

$$\langle a'bc \rangle = \langle ab'c \rangle = \langle abc' \rangle = -\tfrac{2}{3}, \quad \langle a'b'c' \rangle = +1, \tag{41}$$

and this implies that $q_1 = \mathrm{prob}(a'bc = +1) = \mathrm{prob}(ab'c = +1) = \mathrm{prob}(abc' = +1) = \frac{1}{6}$ and $q_2 = \mathrm{prob}(a'b'c' = +1) = 1$. This is the QM data that our LR friend has to reproduce as well as possible. Because of the symmetry of the state he will assign the same probability r_1 to the events $a'bc = +1$, $ab'c = +1$, and $abc' = +1$ and r_2 to $a'b'c' = +1$. However, his model has to satisfy the constraint given by Eq. (33), so the best he can do is to saturate the bound and then

$$3r_1 = r_2 \Rightarrow 0 \leq r_1 \leq \tfrac{1}{3}. \tag{42}$$

Now, according to the probabilities r_1 and r_2 his LR model predicts, we choose the experimental test that minimizes Eq. (40), i.e., we consider the event $a'bc = +1$ $(a'b'c' = +1)$ when $n_D(q_1,r_1) < n_D(q_2,r_2)$ $[n_D(q_1,r_1) > n_D(q_2,r_2)]$, and the experimental results will destroy his LR belief after $n_D(q_1,r_1)$ $[n_D(q_2,r_2)]$ trials. The best value our LR friend can assign to r_1 is the solution to

$$n_D(q_1,r_1) = n_D(q_2,r_2), \tag{43}$$

with the constraint (42), and this condition means that $r_1 \approx 0.315$ and $n_D \approx 161$ trials are needed to have a depressing factor equal to 10^4. Repeating the same calculation for the observables given by Eq. (36), the number of trials slightly increases, $n_D \approx 166$, despite the fact that the violation of the inequality is greater than the obtained for Eq. (35).

TABLE I. Comparison of the strength of the QM vs LR test, which can be performed for the maximally entangled states of two and three spin-$\frac{1}{2}$ particles and for the three-photon entangled state reulting from the orthopositronium annihilation.

State	Number of trials
GHZ	≈ 32
Positronium state (25)	≈ 161
Singlet	≈ 200

In Ref. [28] the same reasoning was applied to the maximally entangled state of two and three spin-$\frac{1}{2}$ particles, showing that $n_D \approx 200$ in the first case, and $n_D \approx 32$ for the latter (see Table I). Our result then implies that the three-photon entangled state produced in the orthopositronium decay has, in some sense, more quantum correlations than any entangled state of two spin-$\frac{1}{2}$ particles.

C. Generalization of the results

It is easy to generalize some of the results obtained for the entangled state resulting from the o-Ps decay. As it has been mentioned, this state can be understood as an equally weighted sum of two symmetric product states, since it can be written as Eq. (31). The Bloch vectors of the two local states appearing in this decomposition form an angle of 120°. It is clear that the conclusions seen above depend on the angle between these vectors, i.e., with their degree of nonorthogonality. The family of states to be analyzed can be parametrized in the following way:

$$|\psi(\delta)\rangle = \alpha_\delta \left[\begin{pmatrix} c_\delta \\ s_\delta \end{pmatrix} \otimes \begin{pmatrix} c_\delta \\ s_\delta \end{pmatrix} \otimes \begin{pmatrix} c_\delta \\ s_\delta \end{pmatrix} + \begin{pmatrix} s_\delta \\ c_\delta \end{pmatrix} \otimes \begin{pmatrix} s_\delta \\ c_\delta \end{pmatrix} \otimes \begin{pmatrix} s_\delta \\ c_\delta \end{pmatrix} \right], \tag{44}$$

where δ is the angle between the two local Bloch vectors, $c_\delta \equiv \cos(\pi - \delta/4)$ and $s_\delta \equiv \sin(\pi - \delta/4)$, and α_δ is a positive number given by the normalization of the state. An alternative parametrization of this family is, using Eq. (29) and defining $\delta' \equiv \delta/4$,

$$|\psi(\delta)\rangle = 2\alpha_\delta [\sin^2\delta' \cos\delta' (|001\rangle + |010\rangle + |100\rangle) + \cos^3\delta' |111\rangle]. \tag{45}$$

The expectation value of three local observables for this set of states follows trivially from Eq. (34). Using this expression it is easy to see that the combination of the expectation values of Eq. (33) has all the partial derivatives equal to zero for the set of observables given in Eq. (35) independently of δ. For these observables, the dependence of expression (33) with the degree of orthogonality between the two product states is given in Fig. 2. There is no violation of the Mermin inequality for the case in which $\delta \lesssim 85°$. In this situation one can always find a LR model able to reproduce the QM statistical prediction given by Eq. (33) and the observables (35). We can now repeat all the steps made in order to determine the number of trials needed to rule out local realism as a function of the angle δ. In Fig. 3 we have summarized the results. We have shown only the cases where the number of trials is less than 200, since this is the value obtained for the singlet. Note that the case $\delta = 120°$, which corresponds to Eq. (25), is very close to the region where there is no improvement compared to the maximally entangled state of two qubits.

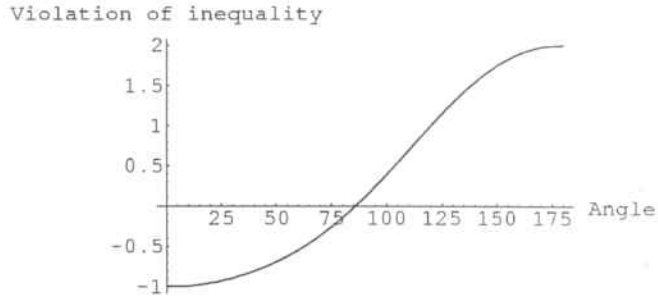


FIG. 2. Violation of the Mermin inequality (33) with the angle δ (in degrees) for the family of states (44). We have substracted 2 to the combination of the expected values of Eq. (33), so a positive value means that a conflict between QM and LR appears.

All these results can be understood in the following way: the smaller the angle between the two local states, δ, the higher the overlap of the state $|\psi(\delta)\rangle$ with the product state having each local Bloch vector pointing in the direction of the x axis, which corresponds to the state $|111\rangle$ in Eq. (45). This means that the quantum state we are handling is too close to a product state [25], and thus, no violation of the Mermin inequality can be observed.

VI. CONCLUDING REMARKS

In this paper we have analyzed the three-particle quantum correlations of a physical system given by the decay of the orthopositronium into a three-photon pure state. After obtaining the state describing the polarization of the three photons (25), some of the recent techniques developed for the study of three-party entanglement have been applied. The particular case where the three photons emerge in the most symmetric configuration corresponds to the state with the maximum square concurrence. We have shown that this state

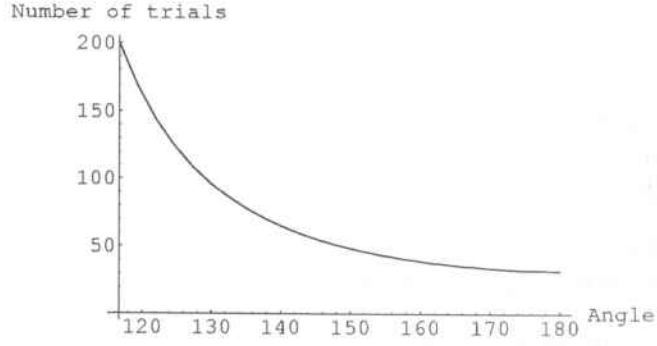


FIG. 3. Number of trials needed to rule out local realism as a function of the angle δ (in degrees) for the family of states (44). Values greater than 200 are not shown since in these cases there always exists a two-qubit entangled state that gives the same result, i.e., it has the same "strength" for ruling out local realism.

allows *a priori* for a QM vs LR test, which is stronger than any of the existing ones that use the singlet state. In this sense, orthopositronium decays into a state which carries stronger quantum correlations than any entangled state of two spin-$\frac{1}{2}$ particles.

Bose symmetrization has played a somewhat negative role in reducing the amount the GHZ-ness of the o-Ps decay state. Indeed, the natural GHZ combination $|+\,+\,-\rangle+|-\,-\,+\rangle$ emerging from the computation of Feynmann diagrams has been symmetrized due to the absence of photon tagging to our state $|+\,+\,-\rangle+|+\,-\,+\rangle+|-\,+\,+\rangle+|-\,-\,+\rangle+|-\,+\,-\rangle+|+\,-\,-\rangle$, inducing a loss of tangle. The quantum optics realization of the GHZ state does avoid symmetrization through a geometric tagging [10]. It is, thus, reasonable to look for pure GHZ states in decays to distinct particles, so that tagging would be carried by other quantum numbers, as, e.g., charge. It is, on the other hand, peculiar to note that symmetrization in the $K^0\bar{K}^0$ system is responsible for its entanglement ($|+-\rangle+|-+\rangle$) [13].

Let us briefly discuss the experimental requirements needed for testing quantum mechanics as it has been described in this paper. The preparation of positronium in a given polarization state can be performed using magnetic mixing as it has been described in Ref. [30]. The circular polarizations of the three photons resulting from an orthopositronium decay have to be measured. The positions of the three detectors are given by the maximization of the square concurrence and their clicks have to detect the coincidence of the three photons. The energy of these photons is of the order of 1 Mev. Polarization analyzers with a good efficiency would allow us to acquire statistical data showing quantum correlations that would violate the Mermin inequality discussed above. Unfortunately, as far as we know, no such analyzers exist for this range of energies (this is not the case for optic photons). A possible way out might be to use Compton scattering to measure the photon polarizations [31]. However, the Compton effect just gives a statistical pattern depending on the photon and electron polarizations, which is not a direct measurement of the polarizations. Further work is needed to modify our analysis of QM vs LR to accommodate for such indirect measurements. Finally, it is hard to see how to implement a switching procedure in the measuring apparatus in order to rule out the locality loophole, although it is thought that this loophole has been closed by recent experiments [32]. The detection loophole cannot be closed, so one has to assume the fair sampling hypothesis.

To summarize, orthopositronium decay provides, without using any postselection procedure, an entangled state of three space-separated photons with more quantum correlations than any entangled state of two particles. Indeed it can be used in principle to test quantum mechanics against local realism, although many experimental difficulties have yet to be overcome. The techniques shown in this paper can be easily extended to the analysis of the entanglement properties of different three-particle entangled states obtained in other experimental settings [perhaps the same state, due to its nice properties from the point of view of group theory (27)].

ACKNOWLEDGMENTS

We acknowledge J. Bernabeu for suggesting positronium as a source of three entangled particles and reading carefully the paper. We also thank A. Czarnecki, D. W. Gidley, M. A. Skalsey, and V. L. Telegdi for comments about the measurement of the photon polarizations in the orthopositronium decay. We acknowledge financial support by CICYT Project No. AEN 98-0431, CIRIT Project No. 1998SGR-00026, and CEC Project No. IST-1999-11053, A.A. by a grant from MEC (AP98). Financial support from the ESF is also acknowledged. This work was concluded during the 2000 session of the Benasque Center for Science, Spain.

[1] A. Einstein, B. Podolsky, and N. Rosen, Phys. Rev. **47**, 777 (1935).
[2] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, Am. J. Phys. **58**, 1131 (1990).
[3] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1964).
[4] D. Bohm and Y. Aharonov, Phys. Rev. **108**, 1070 (1957).
[5] J. F. Clauser and A. Shimony, Rep. Prog. Phys. **41**, 1881 (1978).
[6] A. Aspect, J. Dalibard, and G. Roger, Phys. Rev. Lett. **49**, 1804 (1982).
[7] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998); G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, *ibid.* **81**, 5039 (1998).
[8] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, The Netherlands, 1989), pp. 73–76.
[9] N. D. Mermin, Am. J. Phys. **58**, 731 (1990).
[10] D. Bouwmeester, J. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **82**, 1345 (1999); e-print quant-ph/9810035.
[11] C. H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).
[13] See, for instance, A. Di Domenico, Nucl. Phys. B **450**, 293 (1995); B. Ancochea, A. Bramon, and M. Nowakowski, Phys. Rev. D **60**, 094008 (1999); e-print hep-ph/9811404; F. Benatti and R. Floreanini, Eur. Phys. J. C **13**, 267 (2000); e-print hep-ph/9912348.
[14] C. Itzykson and J. Zuber, *Quantum Field Theory* (McGraw-Hill, New York, 1980).
[15] L. Wolfenstein and D. G. Ravenhall, Phys. Rev. **88**, 279 (1952).
[16] Andrzej Czarnecki, Acta Phys. Pol. B **30**, 3837 (1999); e-print hep-ph/9911455.
[17] N. Linden and S. Popescu, Fortschr. Phys. **46**, 567 (1998); e-print quant-ph/9711016.
[18] A. Sudbery, e-print quant-ph/0001116.
[19] A. Acín, A. Andrianov, L. Costa, E. Jané, J. I. Latorre, and R. Tarrach, Phys. Rev. Lett. **85**, 1560 (2000); e-print quant-ph/0003050.

[20] V. Coffman, J. Kundu, and W. K. Wootters, Phys. Rev. A **61**, 052306 (2000).
[21] W. Dür, G. Vidal, and J. I. Cirac, Phys. Rev. A **62**, 062314 (2000).
[22] T. A. Brun and O. Cohen, e-print quant-ph/0005124.
[23] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants* (Birkhäuser, Boston, 1994). Its explicit form is

$$\begin{aligned}\mathrm{Hdet}(t_{ijk}) = {} & t_{000}^2 t_{111}^2 + t_{001}^2 t_{110}^2 + t_{010}^2 t_{101}^2 + t_{100}^2 t_{011}^2 \\ & - 2(t_{000}t_{111}t_{011}t_{100} + t_{000}t_{111}t_{101}t_{010} \\ & + t_{000}t_{111}t_{110}t_{001} + t_{011}t_{100}t_{101}t_{010} \\ & + t_{011}t_{100}t_{110}t_{001} + t_{101}t_{010}t_{110}t_{001}) \\ & + 4(t_{000}t_{110}t_{101}t_{011} + t_{111}t_{001}t_{010}t_{100}).\end{aligned}$$

[24] S. Rai and J. Rai, e-print quant-ph/0006107.
[25] A. Higuchi and A. Sudbery, e-print quant-ph/0005013; H. A. Carteret, A. Higuchi, and A. Sudbery, e-print quant-ph/0006125.
[26] A. Acín, A. Andrianov, E. Jané, and R. Tarrach, e-print quant-ph/0009107.
[27] N. D. Mermin, Phys. Rev. Lett. **65**, 1838 (1990).
[28] A. Peres, Fortschr. Phys. **48**, 531 (2000).
[29] S. Kullback, *Information Theory and Statistics* (Wiley, New York, 1959).
[30] M. Skalsey, Mod. Phys. Lett. A **7**, 2251 (1992).
[31] B. K. Arbic, S. Hatamian, M. Skalsey, J. Van House, and W. Zheng, Phys. Rev. A **37**, 3189 (1988).
[32] N. Gisin and H. Zbinden, Phys. Lett. A **264**, 103 (1999); e-print quant-ph/9906049.

Appendix E

PHYSICAL REVIEW A, VOLUME 61, 022113

Optimal generalized quantum measurements for arbitrary spin systems

A. Acín, J. I. Latorre, and P. Pascual
Departament d'Estructura i Constituents de la Matèria and IFAE, Facultat de Física, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain
(Received 15 April 1999; published 14 January 2000)

Positive-operator-valued measurements on a finite number of N identically prepared systems of arbitrary spin J are discussed. Pure states are characterized in terms of Bloch-like vectors restricted by a SU$(2J+1)$ covariant constraint. This representation allows for a simple description of the equations to be fulfilled by optimal measurements. We explicitly find the minimal positive-operator-valued measurement for the $N=2$ case, a rigorous bound for $N=3$, and set up the analysis for arbitrary N.

PACS number(s): 03.65.Bz, 03.67.−a

I. INTRODUCTION

A measurement on a quantum-mechanical system only provides partial information on the measured state. Even in the case where N identical copies of the system are available, the information which can be retrieved remains bounded. This fact can be quantified using the averaged fidelity based on the following general idea. Given N identical copies of a system, we may consider a two-step procedure to rate the fidelity of a measuring apparatus. First, we set up a generalized quantum-mechanical measurement [or positive-operator-valued measurement (POVM) [1,2]]. Upon performing a measurement, its outcome provides the basis for a best guess about the incoming state. The averaged fidelity quantifies how close the final guess is from the original state averaging over the latter. For any finite number N of copies of a spin J pure state system, the average fidelity is proven to be bounded by [3]

$$\bar{f}(N,J)=\frac{N+1}{N+2J+1}. \tag{1}$$

The issue at stake remains to devise the optimal and minimal measuring strategy for any quantum system.

Explicit constructions of optimal and minimal generalized quantum-mechanical measurements of spin-$\frac{1}{2}$ systems have been presented recently in Refs. [4–8]. The detailed construction is subtle and depends on whether the original system is in a pure or mixed state. The simplest case corresponds to measuring a spin-$\frac{1}{2}$ system known to be in a pure state. A generalized measurement can be constructed as a resolution of the identity made with rank-1 Hermitian operators, which are in turn built from the direct product of a given state,

$$I=\sum_{r=1}^{n} c_r^2 |\Psi_r\rangle^N {}^N\langle\Psi_r|, \tag{2}$$

where I is then the identity in the maximal spin subspace. The important—and of possible future practical relevance—result is that the maximum averaged fidelity is attained with a finite number of operators [6]. Upon a case-by-case analysis, it is found that the minimum number, n, of such operators is a function of N and is given in the table:

N	1	2	3	4	5
n	2	4	6	10	12

The explicit form of Eq. (2) for the above cases can be found in Ref. [7].

The far more involved case of spin-$\frac{1}{2}$ mixed states has also been worked out in Ref. [8]. At variance with the pure state case, the closed expression for the maximum averaged fidelity depends on what the unbiased *a priori* distribution of density matrices is. Yet, explicit solutions for optimal measurements are found. Some remarkable properties emerge along the new construction. Let us briefly mention a few. Optimal measurements turn out to be structured using projectors on total spin eigenspaces and, within each eigenspace, on maximal spin component is some direction. This allows for a reuse of minimal and optimal results from the pure state case. Also, beyond two copies, some projectors are not of rank 1.

Explicit constructions of optimal minimal measurements are so far restricted to spin-$\frac{1}{2}$ systems, either pure or mixed. It is the purpose of this paper to extend this analysis for arbitrary spin pure states. A number of nontrivial issues must be faced at the outset. For instance, progress in the spin-$\frac{1}{2}$ case was triggered by the appropriate use of the Bloch vector labeling of density matrices associated to spinors. We shall resort to a similar representation in the case of arbitrary spin states, using representations of SU$(2J+1)$. The equivalent of a Bloch vector will be shown to obey a covariant restriction. This extra work will allow for a unified general setting of the problem of optimal measurements of arbitrary spins.

Finding explicit minimal optimal measurements remains a matter of case-by-case analysis. We shall provide explicit bounds for the minimal number of projectors, n, in POVMs. The case of $N=2$ will be fairly complete. Higher number of copies still need further ingenuity to get rigorous bounds.

II. AVERAGED FIDELITY

Consider a spin J particle which is in an unknown pure state $|\Psi\rangle$,

$$|\Psi\rangle=\begin{pmatrix} x_1+iy_1 \\ x_2+iy_2 \\ \cdots \\ x_D+iy_D \end{pmatrix}, \tag{3}$$

where $D=2J+1$ and the normalization of the state imposes $\Sigma_{i=1,\ldots,D}(x_i^2+y_i^2)=1$. Of course, we may use a different parametrization, e.g.,

$$|\Psi\rangle=\begin{pmatrix} \cos\phi \\ \sin\phi(x_2+iy_2) \\ \cdots \\ \sin\phi(x_D+iy_D) \end{pmatrix}, \tag{4}$$

with $0\leq\phi\leq\pi/2$ and $\Sigma_{i=2,\ldots,D}(x_i^2+y_i^2)=1$. Using this second parametrization and following Ref. [9] it is possible to prove that the volume element in the space of these states is

$$dV_D=4(\sin\phi)^{2D-3}\cos\phi\, d\phi\, dS_{2D-3}, \tag{5}$$

where dS_{2D-3} corresponds to the standard volume element on S_{2D-3}. The total volume is

$$V_D=\frac{4\pi^{D-1}}{(D-1)!}. \tag{6}$$

Given N identical copies of the arbitrary spin state, we have

$$|\Psi\rangle^N\equiv|\Psi\rangle\otimes|\Psi\rangle\otimes\cdots^N\cdots\otimes|\Psi\rangle. \tag{7}$$

A measurement on this enlarged system will bring richer information on $|\Psi\rangle$ than N separate measures on its respective copies [10].

Setting a generalized quantum measurement consists in providing a resolution of the identity of the type

$$\sum_{i=1}^{n} c_r^2|\Psi_r\rangle^N\,{}^N\langle\Psi_r|+P_N=I, \tag{8}$$

where P_N is the projector on the space different from the one spanned from states of the form given in Eq. (7). We already have all the necessary elements to define and compute the averaged fidelity. Upon measuring $|\Psi\rangle^N$ with the above POVM, a given outcome labeled by r will result with probability $|^N\langle\Psi|\Psi_r\rangle^N|^2$. The natural guess for the initial pure state is, then, $|\Psi_r\rangle$ (this is only the best strategy if the initial state is known to be pure; the best guess for a mixed state is not the same state as the outcome of the POVM [8]). The overlap of this guess with the original state is just $|\langle\Psi|\Psi_r\rangle|^2$. The averaged or mean fidelity is defined as the product of the probability for r being triggered times the overlap between the ensuing guess and the original state, averaged over all possible initial unknown states,

$$\bar{f}(N,J)\equiv\frac{1}{V_{2J+1}}\sum_{r=1}^{n} c_r^2\int_0^{\pi/2} d\phi(\sin\phi)^{4J-1}\cos\phi \times\int dS_{4J-1}|^N\langle\Psi|\Psi_r\rangle^N|^2|\langle\Psi|\Psi_r\rangle|^2. \tag{9}$$

To evaluate the above expression, it is convenient to use the freedom to choose the integration variables to set each individual $|\Psi_r\rangle$ as a spinor with only a nonvanishing first component. Then,

$$\bar{f}(N,J)=\frac{1}{V_{2J+1}}\sum_{r=1}^{n} c_r^2\int_0^{\pi/2} d\phi(\sin\phi)^{4J-1} \times(\cos\phi)^{2N+3}S_{4J-1}. \tag{10}$$

We finally get

$$\bar{f}(N,J)=\frac{(2J)!(N+1)!}{(2J+N+1)!}\sum_{r=1}^{n} c_r^2. \tag{11}$$

This sum is easily calculated. It is just the dimension of the space spanned by the totally symmetric tensor of order N whose indices can take $2J+1$ values,

$$\sum_{r=1}^{n} c_r^2=\frac{(2J+N)!}{N!(2J)!}. \tag{12}$$

Thus,

$$\bar{f}(N,J)=\frac{N+1}{N+2J+1}, \tag{13}$$

which corresponds to Eq. (1) and was obtained in Ref. [3] using different techniques.

III. GENERALIZED BLOCH FORM OF ARBITRARY SPIN PURE STATES

It is sometimes useful to represent the state of a spin-$\frac{1}{2}$ system using the Bloch representation,

$$\rho=\frac{1}{2}I+\frac{1}{2}\vec{b}\cdot\vec{\sigma}, \tag{14}$$

where $\vec{b}$ is a vector existing within the unit sphere. Pure states correspond to the surface of the sphere, that is, $\vec{b}^2=1$. A similar but more complicated construction is possible for arbitrary spin particles.

Consider a pure state of a spin J particle. One may represent it using, e.g., Eq. (3). Alternatively we may construct its associated density matrix and write

$$\rho=\frac{1}{2J+1}I+\sqrt{\frac{J}{2J+1}}n_a\lambda_a, \quad a=1,\ldots,4J(J+1), \tag{15}$$

where λ_a are the generators of the SU$(2J+1)$ normalized by

$$\mathrm{Tr}(\lambda_a\lambda_b)=2\,\delta_{ab}, \tag{16}$$

and $\hat{n}$ is the normalized vector that plays the role of a generalized Bloch vector. The coefficients in Eq. (15) are chosen in such a way that $\mathrm{Tr}\,\rho=\mathrm{Tr}\,\rho^2=1$.

A simple counting of degrees of freedom shows that a spin J pure state is described by $4J$ real parameters whereas the generalized Bloch vector carries $4J(J+1)-1$. A mismatch appears for $J>\frac{1}{2}$, which implies that severe constraints must limit the subspace of valid vectors $\hat{n}$. Indeed, pure states must verify $\rho=\rho^2$, which translates into

$$d_{abc}n_an_b=\frac{2J-1}{\sqrt{J(2J+1)}}n_c \tag{17}$$

when Eq. (15) is used and where d_{abc} are the completely symmetric symbols associated to SU($2J+1$), defined through the anticommutator of the generators of the group [11],

$$\{\lambda_a,\lambda_b\}=\frac{4}{2J+1}\delta_{ab}I+2\,d_{abc}\lambda_c, \tag{18}$$

which verify

$$d_{abb}=0,\quad d_{abc}d_{dbc}=\frac{(2J-1)(2J+3)}{2J+1}\delta_{ad}. \tag{19}$$

Some useful properties of the vectors $\hat{n}$ follow from the above general covariant constraint (17),

$$\begin{aligned} d_{abc}n_an_bn_c&=\frac{2J-1}{\sqrt{J(2J+1)}},\\ d_{abe}d_{cde}n_an_bn_cn_d&=\frac{(2J-1)^2}{J(2J+1)}, \end{aligned} \tag{20}$$

where it is clear that for spin $J=\frac{1}{2}$ the simple structure of SU(2) causes the d symbols to vanish and the right-hand side to be identically zero.

We can also deduce the useful constraint which follows from the positivity of the square of the scalar product of two arbitrary spin J pure states, which reads

$$|\langle\Psi|\Psi'\rangle|^2=\mathrm{Tr}(\rho\rho')=\frac{1}{2J+1}(1+2J\hat{n}\cdot\hat{n}')\geq 0. \tag{21}$$

Generalized Bloch vectors are thus constrained to have scalars products bounded by

$$\hat{n}\cdot\hat{n}'\geq-\frac{1}{2J}. \tag{22}$$

Two pure states are orthogonal then when the scalar product of their generalized Bloch vectors satisfies the equality in Eq. (22).

Let us illustrate the construction of a Bloch vector for the $J=1$ example. In this case, the density matrix representing the system can be connected to the standard spinorlike representation. For instance, taking $J=1$ it is easy to see that the generalized Bloch vector corresponds to Eq. (3) if

$$\begin{aligned} n_1&=\sqrt{3}(x_1x_2+y_1y_2),\quad n_2=\sqrt{3}(x_1y_2-x_2y_1),\\ n_4&=\sqrt{3}(x_1x_3+y_1y_3),\quad n_5=\sqrt{3}(x_1y_3-x_3y_1),\\ n_6&=\sqrt{3}(x_2x_3+y_2y_3),\quad n_7=\sqrt{3}(x_2y_3-x_3y_2),\\ n_3&=\frac{\sqrt{3}}{2}[x_1^2+y_1^2-(x_2^2+y_2^2)],\quad n_8=\frac{1}{2}[1-3(x_3^2+y_3^2)], \end{aligned} \tag{23}$$

and λ_a are taken in the Gell-Mann representation of SU(3) [11]. Note that symmetric and antisymmetric combinations of the spinor components build the raising and lowering generators, whereas the Casimir combinations correspond to diagonal ones. Generalization of this construction for arbitrary spin J based on the SU($2J+1$) group is straightforward.

The advantage of using a generalized Bloch representation for arbitrary spin pure states will become apparent shortly, when all our equations will be manifestly SU($2J+1$) covariant and real. This is equivalent to note that the difference between working with spinors, which exist in the fundamental representation of the group, or with Bloch vectors, which exist in the adjoint representation, is that the second is real.

IV. OPTIMAL MEASUREMENTS FOR A SINGLE COPY OF A SYSTEM

Let us go back to the construction of a generalized quantum measurement of arbitrary spin systems. We basically need to solve for the minimal set of $|\Psi_r\rangle$ states such that Eq. (8) is fulfilled. We have found it convenient to project out the P_N piece using

$$\sum_{r=1}^{n}c_r^2|^N\langle\Psi|\Psi_r\rangle^N|^2=1,\ \ \forall\ |\Psi\rangle. \tag{24}$$

This equation can also be written in the Bloch representation as

$$\sum_{r=1}^{n}c_r^2\frac{1}{(2J+1)^N}\left(1+2J\sum_a n_an_a(r)\right)^N=1, \tag{25}$$

where every $\hat{n}(r)$ corresponds to a pure state in the POVM and $\hat{n}$ to the original pure state.

It is clear that the simplest situation we may face corresponds to having a single copy of the unknown state. The optimal and minimal measurement for such a case is, of course, known to correspond to a von Neumann measurement. We shall, however, proceed in a more general way and set the *modus operandi* for the more elaborate cases as devised in Ref. [7].

Equation (24) with $N=1$ can be demonstrated (with a little effort) to be equivalent to

$$\sum_{r=1}^{n} c_r^2[x_j(r)x_k(r)+y_j(r)y_k(r)]=\delta_{jk},$$

$$\sum_{r=1}^{n} c_r^2[x_j(r)y_k(r)-x_k(r)y_j(r)]=0, \quad j,k=1,\ldots,2J+1. \tag{26}$$

Using the insight given by Eq. (25) and the result of Eq. (12), this set of $(2J+1)^2$ independent equations can be rewritten in terms of the Bloch vector as

$$\sum_{r=1}^{n} c_r^2=2J+1,$$

$$\sum_{r=1}^{n} c_r^2 n_a(r)=0, \tag{27}$$

where it is important to remember the constraints limiting $\hat{n}(r)$. For instance, scalar products between any pair $\hat{n}(r)\cdot\hat{n}(s)\geq -1/(2J)$, thus

$$\sum_{r\neq s} c_r^2\left(\frac{1}{2J}+\hat{n}(r)\cdot\hat{n}(s)\right)\geq 0. \tag{28}$$

Using the set of equations (27), the above inequality can be transformed into

$$1-c_s^2\geq 0, \quad \forall\ s=1,\ldots,n. \tag{29}$$

Summing over all s, we get

$$n\geq 2J+1. \tag{30}$$

This bound is indeed saturated by a von Neumann measurement, that is,

$$n_{\min}=2J+1,$$

$$c_s^2=1\ \ \forall\ \ s, \quad \hat{n}(r)\cdot\hat{n}(s)=-\frac{1}{2J},\ \ \forall\ r\neq s. \tag{31}$$

The explicit standard construction for $J=1$ is recovered as the solution to this $N=1$ POVM,

$$|\Psi_1\rangle=\begin{pmatrix}1\\0\\0\end{pmatrix}, \quad |\Psi_2\rangle=\begin{pmatrix}0\\1\\0\end{pmatrix}, \quad |\Psi_3\rangle=\begin{pmatrix}0\\0\\1\end{pmatrix}. \tag{32}$$

Or, alternatively,

$$\hat{n}(1)=\left(0,0,\frac{\sqrt{3}}{2},0,0,0,0,\frac{1}{2}\right),$$

$$\hat{n}(2)=\left(0,0,-\frac{\sqrt{3}}{2},0,0,0,0,\frac{1}{2}\right), \tag{33}$$

$$\hat{n}(3)=(0,0,0,0,0,0,0,-1).$$

We are now in a position to appreciate the advantage of resorting to a Bloch-like parametrization. It is easier to deal with Eq. (27) than with Eq. (26). The use of $\hat{n}(r)$ introduces a simple covariant, yet constrained, formulation. Some extra subtleties will play a relevant role in the more complicated cases.

V. OPTIMAL MEASUREMENTS FOR THE $N=2$ CASE

Let us face the case where $N=2$ identical copies of the system are at our disposal. Following the same reasoning as before, we start by writing Eq. (24) in terms of the basic spinor representation. This leads to

$$\sum_{r=1}^{n} c_r^2[x_i(r)x_j(r)+y_i(r)y_j(r)][x_k(r)x_l(r)+y_k(r)y_l(r)]$$

$$=\frac{1}{4}(2\,\delta_{ij}\delta_{kl}+\delta_{ik}\delta_{jl}+\delta_{il}\delta_{jk}),$$

$$\sum_{r=1}^{n} c_r^2[x_i(r)y_j(r)-x_j(r)y_i(r)][x_k(r)y_l(r)-x_l(r)y_k(r)]$$

$$=\frac{1}{4}(\delta_{ik}\delta_{jl}-\delta_{il}\delta_{jk}),$$

$$\sum_{r=1}^{n} c_r^2[x_i(r)x_j(r)+y_i(r)y_j(r)][x_k(r)y_l(r)-x_l(r)y_k(r)]$$

$$=0. \tag{34}$$

The system is now quadratic in the basic structures appearing linearly in the $N=1$ case. Using the Bloch vector representation, these $(2J+1)^2(2J^2+2J+1)$ equations can be recast into

$$\sum_{r=1}^{n} c_r^2=(2J+1)(J+1)\equiv B,$$

$$\sum_{r=1}^{n} c_r^2 n_a(r)=0, \tag{35}$$

$$\sum_{r=1}^{n} c_r^2 n_a(r)n_b(r)=B\frac{1}{4J(J+1)}\delta_{ab}.$$

A general pattern is emerging. Higher N optimal measurements demand a finer grained resolution of the identity. The Bloch vectors are required to satisfy isotropy conditions in $SU(2J+1)$ group space. The determination of the factor $1/[4J(J+1)]$ has been done using the fact that $\hat{n}$ is a normalized vector and Eq. (12). It is easy to verify that the set of

equations (35) provides a solution for Eq. (25).

From the above basic set of equations, it is easy to get

$$\sum_{r\neq s}^{n} c_r^2 = B - c_s^2,$$

$$\sum_{r\neq s}^{n} c_r^2 \hat{n}(r)\cdot\hat{n}(s) = -c_s^2, \tag{36}$$

$$\sum_{r\neq s}^{n} c_r^2 [\hat{n}(r)\cdot\hat{n}(s)]^2 = B\frac{1}{4J(J+1)} - c_s^2.$$

Then we may argue that

$$\sum_{r\neq s} c_r^2 [b + \hat{n}(r)\cdot\hat{n}(s)]^2 \geq 0, \tag{37}$$

which is extremized by $b = c_s^2/(B - c_s^2)$ leading to

$$n \geqslant (2J+1)^2, \quad c_s^2 \leqslant \frac{J+1}{2J+1}, \quad \forall\ s. \tag{38}$$

For $J=\frac{1}{2}$ this bound agrees with the known solution of the tetrahedron (see the Introduction and Ref. [7]) and generalizes it in the following sense. The solution $n=(2J+1)^2$ also forces all scalar products to be $\hat{n}(r)\cdot\hat{n}(s) = -1/[4J(J+1)]$. This corresponds to a hypertetrahedron in $(2J+1)^2 - 1$ dimensions, exactly those of the adjoint representation of SU$(2J+1)$. Let us just write the explicit solution for $J=1$,

$$\hat{n}(1) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}, 0,0,0,0,0,0\right),$$

$$\hat{n}(2) = \left(\frac{1}{2}, -\frac{\sqrt{3}}{4}, \frac{3}{4}, 0,0,0,0,0\right),$$

$$\hat{n}(3) = \left(\frac{1}{2}, -\frac{\sqrt{3}}{4}, -\frac{3}{4}, 0,0,0,0,0\right),$$

$$\hat{n}(4) = \left(-\frac{1}{4}, 0,0,0, \frac{\sqrt{6}}{4}, \frac{\sqrt{3}}{4}, -\frac{\sqrt{6}}{4}, 0\right),$$

$$\hat{n}(5) = \left(-\frac{1}{4}, 0,0, \frac{3\sqrt{2}}{8}, -\frac{\sqrt{6}}{8}, \frac{\sqrt{3}}{4}, \frac{\sqrt{6}}{8}, -\frac{3\sqrt{2}}{8}\right), \tag{39}$$

$$\hat{n}(6) = \left(-\frac{1}{4}, 0,0, -\frac{3\sqrt{2}}{8}, -\frac{\sqrt{6}}{8}, \frac{\sqrt{3}}{4}, \frac{\sqrt{6}}{8}, \frac{3\sqrt{2}}{8}\right),$$

$$\hat{n}(7) = \left(-\frac{1}{4}, 0,0,0, \frac{\sqrt{6}}{4}, -\frac{\sqrt{3}}{4}, \frac{\sqrt{6}}{4}, 0\right),$$

$$\hat{n}(8) = \left(-\frac{1}{4}, 0,0, -\frac{3\sqrt{2}}{8}, -\frac{\sqrt{6}}{8}, -\frac{\sqrt{3}}{4}, -\frac{\sqrt{6}}{8}, -\frac{3\sqrt{2}}{8}\right),$$

$$\hat{n}(9) = \left(-\frac{1}{4}, 0,0, \frac{3\sqrt{2}}{8}, -\frac{\sqrt{6}}{8}, -\frac{\sqrt{3}}{4}, -\frac{\sqrt{6}}{8}, \frac{3\sqrt{2}}{8}\right).$$

There is still the need to perform the nonobvious step of finding out whether this solution does correspond to a set of spin-1 states. For completeness we give this final form of the solution, that is, the explicit states $|\Psi_1\rangle$ through $|\Psi_9\rangle$ which form the POVM,

$$|\Psi_1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |\Psi_2\rangle = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \\ 0 \end{pmatrix}, \quad |\Psi_3\rangle = \begin{pmatrix} \frac{1}{2} \\ -\frac{\sqrt{3}}{2} \\ 0 \end{pmatrix},$$

$$|\Psi_4\rangle = \begin{pmatrix} \frac{1}{2} \\ i\frac{1}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \quad |\Psi_5\rangle = \begin{pmatrix} \frac{1}{2} \\ i\frac{1}{2} \\ -\frac{1}{2\sqrt{2}} + i\frac{\sqrt{3}}{2\sqrt{2}} \end{pmatrix},$$

$$|\Psi_6\rangle = \begin{pmatrix} \frac{1}{2} \\ i\frac{1}{2} \\ -\frac{1}{2\sqrt{2}} - i\frac{\sqrt{3}}{2\sqrt{2}} \end{pmatrix}, \tag{40}$$

$$|\Psi_7\rangle = \begin{pmatrix} \frac{1}{2} \\ -i\frac{1}{2} \\ \frac{1}{\sqrt{2}} \end{pmatrix}, \quad |\Psi_8\rangle = \begin{pmatrix} \frac{1}{2} \\ -i\frac{1}{2} \\ -\frac{1}{2\sqrt{2}} + i\frac{\sqrt{3}}{2\sqrt{2}} \end{pmatrix},$$

$$|\Psi_9\rangle = \begin{pmatrix} \frac{1}{2} \\ -i\frac{1}{2} \\ -\frac{1}{2\sqrt{2}} - i\frac{\sqrt{3}}{2\sqrt{2}} \end{pmatrix}.$$

Note that all the spinors have scalar products with modulus equal to $\frac{1}{2}$.

VI. OPTIMAL MEASUREMENTS FOR THE $N=3$ CASE

The systematics of our approach are already set. It is, however, in the case of three copies where a major difference between spin $\frac{1}{2}$ and higher spin systems appears. Following an analogous reasoning to that in the preceding sections, we get

$$\sum_{r=1}^{n} c_r^2 = \frac{(2J+3)!}{3!(2J)!} \equiv C,$$

$$\sum_{r=1}^{n} c_r^2 n_a(r) = 0,$$

$$\sum_{r=1}^{n} c_r^2 n_a(r) n_b(r) = C \frac{1}{4J(J+1)} \delta_{ab}, \tag{41}$$

$$\sum_{r=1}^{n} c_r^2 n_a(r) n_b(r) n_c(r) = C \frac{1}{4J(J+1)(2J+3)} \times \left(\frac{2J+1}{J}\right)^{1/2} d_{abc}.$$

We have used Eqs. (12), (19), and (20) for determining the factor $1/[4J(J+1)(2J+3)][(2J+1)/J]^{1/2}$. Again it is easy to prove that Eqs. (41) verify Eq. (25).

For the first time the right-hand side of one of the equations displays a tensor structure based on the d symbol. Such a term would vanish for $J=\frac{1}{2}$ due to the simpler structure of SU(2), but is expected for higher spins [note that the conditions (20) are zero for spin $\frac{1}{2}$].

A bound on the number of projectors appearing in a optimal POVM can be obtained following the by now standard procedure of investigating manifestly positive combinations. In this case, starting from

$$\sum_{r \neq s} \left(\frac{1}{2J} + \hat{n}(r) \cdot \hat{n}(s)\right) [b + \hat{n}(r) \cdot \hat{n}(s)]^2 \geq 0, \tag{42}$$

one gets

$$n \geq (J+1)(2J+1)^2 \tag{43}$$

and $c_s^2 \leq (2J+3)/[3(2J+1)]$. That is, $n \geq 6$ for spin $\frac{1}{2}$ (which agrees with the known result in Ref. [7]), $n \geq 18$ for spin 1, $n \geq 40$ for spin $\frac{3}{2}$, etc. Saturating this bound is impossible for certain cases as implied by the following simple argument. If the bound were to be saturated, then Eq. (42) would become a restricting condition for all scalar products. Indeed, $\hat{n}(r) \cdot \hat{n}(s)$ is either $-1/(2J)$ or else $(2J-1)/[2J(2J+3)]$ for any pair $r \neq s$. If we fix any s and assume that the minimal solution carries p scalar products of the first type and q of the second, it follows that Eq. (41) imposes $p = \frac{1}{2}J(2J+1)^2$ and $q = \frac{1}{2}J(2J+3)^2$. For any J half-integer or even this causes no problem but for odd integer values of the spin this leads to noninteger pairs, which is absurd. Thus, in such a case, the bound cannot be saturated.

VII. CONCLUSIONS

We have presented explicit solutions for minimal optimal POVMs acting on arbitrary spin J systems for the case when two copies are available. For $N=3$ we have provided a rigorous bound. The key idea to simplify the analysis consists in using Bloch representation for pure arbitrary spin states. These vectors do not span a naive $(2J+1)^2-1$ sphere, but rather an intricate subspace defined through covariant restrictions. The power of such covariance makes the set of equations simple,

$$\sum_{r=1}^{n} c_r^2 = \frac{(2J+N)!}{N!(2J)!},$$

$$\sum_{r=1}^{n} c_r^2 n_a(r) = 0,$$

$$\sum_{r=1}^{n} c_r^2 n_a(r) n_b(r) = \frac{(2J+N)!}{N!(2J)!} \frac{1}{4J(J+1)} \delta_{ab}, \tag{44}$$

$$\sum_{r=1}^{n} c_r^2 n_a(r) n_b(r) n_c(r) = \frac{(2J+N)!}{N!(2J)!} \frac{1}{4J(J+1)(2J+3)} \times \left(\frac{2J+1}{J}\right)^{1/2} d_{abc},$$

$$\ldots.$$

In order to analyze a given case with N copies of the spin J particle, it is necessary to retain

$$\frac{[4J(J+1)+N]!}{N![4J(J+1)]!} \tag{45}$$

equations in the system, that is, as many rows in Eq. (44) as $N+1$.

Our results confirm the expected increase of needed projectors to build a POVM as the spin of the system increases. The instances analyzed, that is, $N=1,2,3$, seem to point at a dependence of the type

$$n_{\min} \sim J^N. \tag{46}$$

ACKNOWLEDGMENTS

We are grateful to R. Tarrach and G. Vidal for continuously sharing their insight with us. Financial support from CICYT, Contract No. AEN95-0590, and from CIRIT, Contract No. 1996GR00066 is acknowledged. A.A. acknowledges a grant from MEC.

[1] M. A. Neumark, C. R. Acad. Sci. URSS **41**, 359 (1943).
[2] A. Peres, Found. Phys. **20**, 1441 (1990).
[3] D. Bruß and C. Macchiavello, e-print quant-ph/9812016.
[4] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[5] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[6] R. Derka, V. Buzek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998); e-print quant-ph/9707028.
[7] J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. Lett. **81**, 1351 (1998); e-print quant-ph/9803066.
[8] G. Vidal, J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. A **60**, 126 (1999); e-print quant-ph/9812068.
[9] R. Schack, G. M. D'Ariano, and C. M. Caves, Phys. Rev. E **50**, 972 (1994).
[10] A. Peres and W. K. Wootters, Phys. Rev. Lett. **66**, 1119 (1991).
[11] P. Pascual and R. Tarrach, *QCD: Renormalization for the Practitioner* (Springer-Verlag, Berlin, 1984).

Appendix F

PHYSICAL REVIEW A, VOLUME 61, 062307

Optimal estimation of two-qubit pure-state entanglement

Antonio Acín, Rolf Tarrach, and Guifré Vidal
Departament d'Estructura i Constituents de la Matèria, Universitat de Barcelona, Diagonal 647, E-08028 Barcelona, Spain
(Received 3 November 1999; published 16 May 2000)

We present optimal measuring strategies for an estimation of the entanglement of unknown two-qubit pure states and of the degree of mixing of unknown single-qubit mixed states, of which N identical copies are available. The most general measuring strategies are considered in both situations, to conclude in the first case that a local, although collective, measurement suffices to estimate entanglement, a nonlocal property, optimally.

PACS number(s): 03.67.−a, 03.65.Bz

I. INTRODUCTION

Plenty of work has been performed in recent years on optimal quantum measurements, i.e., on measurements which provide the maximum possible information about an unknown quantum-mechanical pure [1–5] or mixed [6] state, of which N identical copies are available. These works focused mainly on a determination of the unknown state as a whole, and consequently any of its properties is also estimated, although maybe not in an optimal way.

On the other hand, recent developments on the field of quantum information theory stressed the importance of the quantum correlations—or entanglement—displayed by some states of composite systems. In the simplest of such composite systems, the two-qubit case, all nonlocal properties of pure states depend upon only one single parameter. Such a nonlocal parameter is the only relevant quantity invariant under local unitary transformations on each qubit, and plays a central role in the quantification and optimal manipulation of entanglement [7–11].

In this work we analyze and solve the problem of optimally estimating the entanglement of an unknown pure state of two qubits. This problem was also independently addressed by Sancho and Huelga in a recent work [12], where only a restricted class of measuring strategies is considered. Here, on the contrary, we will consider most general quantum measurements on N identical copies of the state. Their quality will be assessed through the gain of information they provide about the nonlocal parameter of the state. After presenting and proving the solution, we will conclude that the optimal measuring strategies so defined are not equivalent to the ones used to fully reconstruct the unknown state. As a matter of fact, *all* information about some relative phase of the unknown state turns out to be irreversibly erased as the entanglement is estimated.

An estimation of the degree of mixing of an unknown mixed state is a different but very much related topic that we shall also consider here. For the single-qubit case the amount of mixing is again specified by just one parameter, the modulus of the corresponding Bloch vector, whereas in order to completely specify the state two more parameters, namely, the direction of the Bloch vector, are also required. We shall show that in this case the optimal measuring strategy on any number N of qubits prepared in the same mixed state can be made compatible with an optimal estimation of the direction of its Bloch vector.

Finally, we will show that a possible way of optimally determining the entanglement of an unknown, two-qubit pure state consists precisely of estimating, also optimally, the degree of mixture of any of its two reduced density matrices. Therefore, in this simple bipartite case it turns out that the optimal estimation of a nonlocal parameter can be done through a local measurement.

The paper is structured as follows. Section II is devoted to background material. We introduce a convenient parametrization of two-qubit pure states, and consider their isotropic distribution. We also review some basic aspects on parameter estimation and on quantum measurements. In Sec. III we pose the problem of entanglement estimation on firmer grounds and announce the main result of this paper: its optimal performance. Section IV, which is rather technical and could well be skipped in a first reading, is devoted to a computation of some effective density matrix $\rho^{(N)}(b)$, an object which plays a central role in deriving the optimal strategy for estimating entanglement. In Sec. V the $N=1$, 2, and 3 cases are presented in more detail in order to illustrate the general case. Optimal estimation of the degree of mixing is discussed and solved in Sec. VI, and finally Sec. VII contains a discussion relating estimation of both entanglement and mixing, and some concluding remarks.

II. PRELIMINARIES

Here we will consider a two-party scenario. Alice and Bob will share N copies of a completely unknown two-qubit pure state $|\psi\rangle$, and their aim will be to obtain as much information as possible about its entanglement. The sense in which the state is *unknown*, the mechanisms for *extracting* information from the system, and the scheme for *evaluating* the extracted information will be briefly reviewed in what follows.

A. Homogeneous distribution

All that is initially known about the state of each pair of qubits is that it is pure. This corresponds to the unbiased distribution on the Hilbert space $\mathcal{H}_4=\mathcal{H}_2\otimes\mathcal{H}_2$ of two qubits, that is, to the only probability distribution invariant under arbitrary unitary transformations on $\mathcal{H}_4$. It is convenient to

express the unknown state $|\psi\rangle \in \mathcal{H}_2 \otimes \mathcal{H}_2$, which depends on six parameters, in its Schmidt-like decomposition

$$|\psi\rangle = \sqrt{\frac{1+b}{2}}|\hat{a}\rangle|\hat{b}\rangle + \sqrt{\frac{1-b}{2}}e^{i\alpha}|-\hat{a}\rangle|-\hat{b}\rangle, \quad (1)$$

where the phase $e^{i\alpha}$, which is usually absorbed by one of the kets it goes with, has been left explicit. The nonlocal parameter $b \in [0,1]$ characterizes the entanglement of $|\psi\rangle$. Only for $b=1$ is $|\psi\rangle$ a product state $|\hat{a}\rangle \otimes |\hat{b}\rangle$, and thus unentangled. For $b<1$ the state contains quantum correlations $b=0$ corresponding to a maximally entangled state. Recall that this parameter is the modulus of the Bloch vector of the reduced density matrix ρ_A on Alice's side,

$$\rho_A \equiv tr_B|\psi\rangle\langle\psi| = \frac{1+b}{2}|\hat{a}\rangle\langle\hat{a}| + \frac{1-b}{2}|-\hat{a}\rangle\langle-\hat{a}|, \quad (2)$$

and equivalently for ρ_B. The other four parameters correspond to the two directions $\hat{a}$ and $\hat{b}$ of the Bloch vectors of ρ_A and ρ_B. Then the unbiased distribution of pure states corresponds [13] to the isotropic distribution of $\hat{a}$ in S^2, $\hat{b}$ in S^2, α in S^1, and the quadratic distribution of b in $[0,1]$, which is actually also a flat distribution, as b^2 is just the Jacobian corresponding to going from Cartesian to spherical coordinates:

$$\int_{S^2}\frac{d\hat{a}}{4\pi}\int_{S^2}\frac{d\hat{b}}{4\pi}\int_{S^1}\frac{d\alpha}{2\pi}\int_0^1 db\, 3b^2 = 1. \quad (3)$$

B. General measurements and information gain

The parties are thus provided with N copies of a pure state $|\psi\rangle$ as in Eq. (1), i.e., with the state $|\psi\rangle^{\otimes N}$, and our aim is to construct the most informative measurement on the collective, $2N$-qubit system for the estimation of the parameter b. The optimality criterion to be used is based on the Kullback or mutual information $K[f',f]$ [14], a functional of two probability distributions f' and f that is interpreted as the gain of information in replacing the latter distribution with the former one [15]. In our case, for instance, the prior, unbiased density function for the parameter b is given by Eq. (3), so we have $f(b)=3b^2$. A generic measurement, allowing for the most general manipulation of the system, is represented by a resolution of the identity by means of a set of positive operators:

$$\sum_k M^{(k)} = I. \quad (4)$$

After the above positive operator valued measurement (POVM) has been performed, giving the outcome k with probability $\mathrm{tr}(M^{(k)}\rho^{\otimes N})$, where $\rho=|\psi\rangle\langle\psi|$, we compute the posterior density function for b, $f(b|k)$, through the Bayes formula

$$f_k(b) \equiv f(b|k) = \frac{p(k|b)f(b)}{p(k)}, \quad (5)$$

where $p(k)$ is given by

$$p(k) = \int_0^1 dbf(b)p(k|b), \quad (6)$$

and the conditional probability of obtaining outcome k when the state's nonlocal parameter has value b, $p(k|b)$ will be shown later. The gain of information resulting from obtaining the outcome k after the measurement is quantified by the Kullback information corresponding to the prior and posterior probability density functions:

$$K[f_k,f] = \int dbf(b|k)\ln\left(\frac{f(b|k)}{f(b)}\right). \quad (7)$$

This expression has to be averaged over all the possible outcomes of the measurement, so that the expected gain of information reads

$$\bar{K}[f_k,f] = \sum_k p(k)K[f_k,f], \quad (8)$$

using Eq. (5), this expression can be written as

$$\bar{K}[f_k,f] = \sum_k \int dbf(b)p(k|b)\ln\left(\frac{p(k|b)}{p(k)}\right). \quad (9)$$

Let us note here that the value of $K[f_k,f]$ in Eq. (7) would remain unchanged if we decided to characterize the entanglement of $|\psi\rangle$ by another parameter $b=h(b)$ [where $h(b)$ is any bijective function of the original parameter b]. Consequently, the gain of information we compute for b also applies to any of the measures of entanglement so far proposed, such as the entanglement of formation [7],

$$-\sqrt{\frac{1+b}{2}}\log_2\sqrt{\frac{1+b}{2}} - \sqrt{\frac{1-b}{2}}\log_2\sqrt{\frac{1-b}{2}}, \quad (10)$$

for the asymptotic regime, or the monotone [10]

$$\sqrt{\frac{1-b}{2}} \quad (11)$$

for the single-copy case.

III. OPTIMAL MEASUREMENTS FOR ENTANGLEMENT ESTIMATION

We are looking for a measurement of the form of Eq. (4), such that the expected gain of information [Eq. (9)] is maximized. Here and in Sec. V we will present and explain such optimal measurements, whereas their explicit construction is mainly contained in Sec. IV.

A. Local and global strategies

Before we proceed we comment on four classes of measurements Alice and Bob may consider in order to learn about b [12]:

(i) *Local* measurements on only, say, Alice's side, i.e., on the N qubits supporting the local state $\rho_A^{\otimes N}$, would be the most restrictive class of the hierarchy.

(ii) *Uncorrelated bilocal* measurement, in which each party measures their local N-qubit part independently, is one type of intermediate strategy.

(ii) *Classically correlated bilocal* measurement, with classical communication between Alice and Bob, is a less restrictive intermediate strategy.

(iv) *Global* measurements on the $2N$ qubits constitute the most general case.

Global measurements are in principle the most informative ones. But as the parameter b, which quantifies the entanglement of $|\psi\rangle$, also completely quantifies the mixing of ρ_A (and ρ_B), it could well happen that local measurements, or bilocal measurements on the two parties, optimal for the determination of the mixing, are as informative as the global ones with respect to entanglement. In fact, in reducing $|\psi\rangle\langle\psi|$ to $\rho_A\otimes\rho_B$ only the relative phase α is lost, and the dependence on directions $\hat{a}$ and $\hat{b}$ and on the entanglement b is preserved. We have found the optimal global and local measurement of b. The results obtained following the two strategies are the same, as we will discuss in Sec. VII, so all the extractable information about the entanglement is preserved under the partial trace operation, and the four classes considered above turn out to be equivalent for entanglement estimation.

B. Effective mixed state

Note that all the dependence on the measuring strategy (4) in Eq. (9) is contained in the probability $p(k|b)$ of outcome k conditioned on the entanglement of the state being some given b,

$$p(k|b)=\int_{S^2}\frac{d\hat{a}}{4\pi}\int_{S^2}\frac{d\hat{b}}{4\pi}\int_{S^1}\frac{d\alpha}{2\pi}\mathrm{tr}(M^{(k)}\rho^{\otimes N}), \tag{12}$$

where the sum over the rest of the parameters reflects the fact that we are only interested in the entanglement. This expression can also be written as

$$p(k|b)=\mathrm{tr}[M^{(k)}\rho^{(N)}(b)], \tag{13}$$

where the mixed state $\rho^{(N)}(b)$ is

$$\rho^{(N)}(b)\equiv\int_{S^2}\frac{d\hat{a}}{4\pi}\int_{S^2}\frac{d\hat{b}}{4\pi}\int_{S^1}\frac{d\alpha}{2\pi}|\psi\rangle\langle\psi|^{\otimes N}. \tag{14}$$

Equation (13) allows for an alternative interpretation to our problem: a $2N$-qubit mixed state $\rho^{(N)}(b)$ is drawn randomly with prior probability distribution $f(b)=3b^2$, and we want to determine it by estimating b.

We will compute $p(k|b)$ on a basis that diagonalizes $\rho^{(N)}(b)$, which will crucially turn out to be independent of b. Let us denote the positive eigenvalues of $\rho^{(N)}(b)$ by $\lambda_1(b),\ldots,\lambda_m(b)$, and their multiplicity by $n_1,\ldots,n_m$. From the normalization of Eq. (14) the relation $\Sigma_{j=1}^m n_j\lambda_j=1$ follows. The sum $n\equiv\Sigma_j n_j$ of multiplicities of (nonvanishing) eigenvalues equals the dimension of the space which supports $|\psi\rangle\langle\psi|^{\otimes N}$. This is the symmetric subspace of $\mathcal{H}_4^{\otimes N}$, and thus [5]

$$n=\frac{(N+3)!}{3!N!}=\frac{(N+3)(N+2)(N+1)}{6}. \tag{15}$$

With this notation Eq. (13) reads

$$p(k|b)=\lambda_1(b)\sum_{i=1}^{n_1}M_{ii}^{(k)}+\lambda_2(b)\sum_{i=n_1+1}^{n_1+n_2}M_{ii}^{(k)}+\cdots$$
$$+\lambda_m(b)\sum_{i=n-n_m+1}^{n}M_{ii}^{(k)}\equiv\sum_{j=1}^{m}\lambda_j(b)q_j^{(k)}. \tag{16}$$

By substituting this expression into Eq. (9), and using the inequality [16]

$$(x_1+x_2)\ln\left(\frac{x_1+x_2}{y_1+y_2}\right)\leq x_1\ln\left(\frac{x_1}{y_1}\right)+x_2\ln\left(\frac{x_2}{y_2}\right), \tag{17}$$

where $x_i,y_i\geq 0$, along with the fact that the POVM is a resolution of the identity in the symmetric subspace of $\mathcal{H}_4^{\otimes N}$, i.e. $\Sigma_k q_j^{(k)}=n_j$, it follows that the average gain of information is bounded by

$$\bar{K}[f_k,f]\leq\int dbf(b)\sum_{j=1}^{m}n_j\lambda_j(b)\ln\left(\frac{\lambda_j(b)}{\int dbf(b)\lambda_j(b)}\right). \tag{18}$$

C. Minimal most informative measuring strategy

Bound (18) can be minimally saturated through a measurement with m outcomes, where each $M^{(k)}$ is the n_k-dimensional projector over the subspace corresponding to the eigenvalue λ_k of $\rho^{(N)}(b)$, then having $p(k|b)=n_k\lambda_k(b)$. Therefore, the construction of the optimal measurement can be readily performed after the computation of the spectral decomposition of state (14), and this is done for an arbitrary N in Sec. IV. For a more detailed account of the $N=1$, 2, and 3 cases, see Sec. V, where also the gain of information up to $N=80$ has been computed explicitly.

Note also that there are other ways measuring strategies that can be evaluated and, consequently, there is not a unique notion of optimality. For instance, in Refs. [1–6] a guess for the unknown state is made depending on the outcome of the measurement, and then both guessed and unknown states are compared using the fidelity. It can be proved, following Ref. [16], that the optimal measurements presented here, the most informative ones, are also optimal if we decide, alternatively, on a fidelitylike figure of merit satisfying some very general conditions [19].

IV. COMPUTATION OF $\rho^{(N)}$

It has been shown that the spectrum of $\rho^{(N)}(b)$ determines the maximal gain of information about b, whereas its eigenprojectors lead to the corresponding measuring strategy. Our

next step will be the computation of the spectral decomposition of this effective mixed state.

Let us rewrite the generic two-qubit pure state [Eq. (1)] as

$$|\psi\rangle = U_A \otimes U_B (c_+ |+\rangle_A \otimes |+\rangle_B + c_- |-\rangle_A \otimes |-\rangle_B) \equiv U_A \otimes U_B |\psi(b)\rangle, \tag{19}$$

where $c_+ \equiv \sqrt{(1+b)/2}$, $c_- \equiv \sqrt{(1-b)/2}$, the single-qubit pure states $|+\rangle_A$ and $|-\rangle_A$ ($|+\rangle_B$ and $|-\rangle_B$) constitute an orthonormal basis in Alice's (Bob's) part (corresponding to some fixed direction in the Bloch sphere), U_A and U_B are unitary transformations in each single-qubit space, and $|\psi(b)\rangle$ is a reference state.

The state $\rho^{(N)}(b)$ corresponds then to a Haar integral over the group SU(2)×SU(2), since it can be expressed as

$$\rho^{(N)}(b) = \int_{g \in G} dg [D(g) M(b) D(g)^\dagger]^{\otimes N}, \tag{20}$$

where the index g denotes the elements of the group $G = \mathrm{SU}(2) \times \mathrm{SU}(2)$, $D(g) = \mathrm{U}_A \otimes \mathrm{U}_B$ is a $\frac{1}{2} \times \frac{1}{2}$ irreducible representation (irrep) of this group and $M(b) = |\psi(b)\rangle\langle\psi(b)|$.

A well-known result in group representation theory following from Schur's lemma, the so-called orthogonality lemma, will be useful in the calculation of this integral. Consider a matrix $A^{\alpha\beta}(B)$ given by

$$A^{\alpha\beta}(B) = \int_{g \in G} dg D^\alpha(g) B D^{\beta\dagger}(g), \tag{21}$$

where D^α and D^β are two unitary irreps of the group G. Then we have the following,

Lemma 1 (orthogonality lemma):

$$A^{\alpha\beta}(B) = a(B)\, \delta^{\alpha\beta} I, \tag{22}$$

so $A^{\alpha\beta}(B)$ is zero if the two representations are inequivalent, and proportional to the identity if the two representations are equivalent.

In order to benefit from this lemma we identify B with $M(b)^{\otimes N} = |\psi(b)\rangle\langle\psi(b)|^{\otimes N}$ and then consider the relevant irreps of SU(2)×SU(2) borne by the N-fold tensor product of the $\frac{1}{2} \times \frac{1}{2}$ irrep of the group. These representations are the support of the state $|\psi(b)\rangle^{\otimes N}$, and our next task is to recognize them.

The state $|\psi(b)\rangle^{\otimes N}$ can be expanded as

$$\begin{aligned} |\psi(b)\rangle^{\otimes N} = {} & c_+^N |+ + \cdots + +\rangle_A \otimes |\cdot\rangle_B, \\ & + c_+^{N-1} c_- (|+ + \cdots + -\rangle_A \otimes |\cdot\rangle_B + \cdots \\ & + |- + \cdots + +\rangle_A \otimes |\cdot\rangle_B), \\ & + c_+^{N-2} c_-^2 (|+ \cdots + - -\rangle_A \otimes |\cdot\rangle_B + \cdots \\ & + |- - + \cdots +\rangle_A \otimes |\cdot\rangle_B), \\ & + c_+^{N-3} c_-^3 (\quad) + \cdots + c_+ c_-^{N-1} (\quad), \\ & + c_-^N |- - \cdots - -\rangle_A \otimes |\cdot\rangle_B, \end{aligned} \tag{23}$$

where $|\cdot\rangle_B$ means that we have exactly the same vector in the second subsystem. Notice that in the expression above all the elements of the product basis $\{|u_i\rangle\}$ of the local spaces $\mathcal{H}_2^{\otimes N}$ of Alice's and Bob's N qubits—i.e., $|u_1\rangle = |+ + \cdots + +\rangle$, $|u_2\rangle = |+ + \cdots + -\rangle$, $\ldots$, $|u_{2^N}\rangle = |- - \cdots - -\rangle$ — appear in the form $|u_i\rangle_A \otimes |u_i\rangle_B$. Notice, in addition, that if we denote by m_T the sum of the third spin component of all spinors in each ket—i.e., for instance $m_T(|+ + +\rangle) = 3/2$, $m_T(|+ + -\rangle) = 1/2$, $m_T(|- + -\rangle) = -1/2$, $\cdots$—, the terms multiplied by the same combination of the factors c_+ and c_- have the same m_T in A and B. State (23) can thus also be expressed as

$$\begin{aligned} |\psi(b)\rangle^{\otimes N} = {} & c_+^N \sum_{i; m_T = N/2} |u_i\rangle_A \otimes |u_i\rangle_B \\ & + c_+^{N-1} c_- \sum_{i; m_T = (N/2)-1} |u_i\rangle_A \otimes |u_i\rangle_B + \cdots \\ & + c_-^N \sum_{i; m_T = -N/2} |u_i\rangle_A \otimes |u_i\rangle_B. \end{aligned} \tag{24}$$

We now move from the local spin basis $\{|u_i\rangle_A\}$ to the coupled one $\{|v_i\rangle_A\}$ in Alice's N qubits, and we also do the same in Bob's. The following lemma, that can be easily checked, will be useful here.

Lemma 2: Let $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ be two orthonormal basis in $\mathcal{C}^l$, related by an orthogonal transformation O, so that $|e_i\rangle = \Sigma_j O_{ij} |f_j\rangle$, with $O^* = O$, and $O^{-1} = O^\dagger$. Then,

$$\sum_{i=1}^{l} |e_i\rangle \otimes |e_i\rangle = \sum_{i=1}^{l} |f_i\rangle \otimes |f_i\rangle. \tag{25}$$

Now, note that the unitary transformation relating the local basis and the coupled one is real (since all the Clebsch-Gordan coefficients are real), and that there is a conservation rule for the total third spin component (i.e., the Clebsch-Gordan coefficients that couple two states with third component m_1 and m_2 to a coupled state with third component m are proportional to $\delta_{m, m_1 + m_2}$). Then Eq. (24) can be reexpressed, using the previous two facts and lemma 2, in the coupled basis as

$$\begin{aligned} |\psi(b)\rangle^{\otimes N} = {} & c_+^N \sum_{i; m_T = N/2} |v_i\rangle_A \otimes |v_i\rangle_B \\ & + c_+^{N-1} c_- \sum_{i; m_T = (N/2)-1} |v_i\rangle_A \otimes |v_i\rangle_B + \cdots \\ & + c_-^N \sum_{i; m_T = -N/2} |v_i\rangle_A \otimes |v_i\rangle_B \end{aligned} \tag{26}$$

(see the examples in Sec. V for more details). We note that the symmetry between the terms in A and in B allows us to derive Eq. (26) from Eq. (24).

Let us now have a closer look into Eq. (26). The term with coefficient c_+^N corresponds simply to the state with a total spin j maximal in both Alice's and Bob's subsystem

(i.e., $j_A=j_B=N/2$) and also maximal third spin component m, namely, $m_A=m_B=N/2$. We can thus write, with the notation $|^{j_A}m_A\rangle_A\otimes|^{j_B}m_B\rangle_B$, $|v_1\rangle\equiv|v_1\rangle_A\otimes|v_1\rangle_B=|^{N/2}N/2\rangle_A\otimes|^{N/2}N/2\rangle_B$. This state belongs to a $N/2\otimes N/2$ irrep of the group $SU(2)\times SU(2)$. The coefficient $c_+^{N-1}c_-$ corresponds to all states with $m_A=m_B=(N/2)-1$. Apart from $|v_2\rangle\equiv|^{N/2}(N/2)-1\rangle_A\otimes|^{N/2}(N/2)-1\rangle_B$, which again belongs to the previous $N/2\otimes N/2$ irrep, the remaining $N-1$ kets, $|v_3\rangle\cdots|v_{N+1}\rangle$ have $j_A=j_B=(N/2)-1$, and thus belong to $N-1$ different (but equivalent)

$$\left(\frac{N}{2}-1\right)\otimes\left(\frac{N}{2}-1\right)$$

irreps of the group. But since only the linear combination $|v_3\rangle+\cdots+|v_{N+1}\rangle$ appears, the relevant irrep is just the symmetric combination of the latter $N-1$ ones, which we will denote by

$$\left\{\left(\frac{N}{2}-1\right)\otimes\left(\frac{N}{2}-1\right)\right\}_{sym},$$

and which no longer decomposes as the product of two irreps of $SU(2)$. The same applies for

$$\left(\frac{N}{2}-2\right)\otimes\left(\frac{N}{2}-2\right)$$

irreps, and so on.

Thus, the space which supports the initial state can be decomposed in terms of irreps of $SU(2)\times SU(2)$ as

$$\frac{N}{2}\otimes\frac{N}{2}\oplus\left\{\left(\frac{N}{2}-1\right)\otimes\left(\frac{N}{2}-1\right)\right\}_{sym}\oplus\cdots\oplus\left\{\frac{N \bmod 2}{2}\otimes\frac{N \bmod 2}{2}\right\}_{sym},\tag{27}$$

where $N \bmod 2$ is equal to 1 for odd N and equal to zero for even N. It can be checked that this result agrees dimensionally with formula (15).

The decomposition shown above in terms of the relevant irreps of the group $SU(2)\times SU(2)$, together with the orthogonality lemma, can be used to solve the integral in Eq. (20). As we have argued, when plugging Eq. (26) into Eq. (20) the cross terms corresponding to inequivalent representations—such as $|v_1\rangle(\langle v_3|+\cdots+\langle v_{N+1}|)$—vanish as we integrate, while the terms within the same representation—such as $|v_1\rangle\langle v_1|$—lead to a contribution proportional to the identity in the subspace associated with the representation. So the state $\rho^{(N)}(b)$ is equal to

$$\rho^{(N)}(b)=\lambda_1(b)I_{N/2\otimes N/2}+\lambda_2(b)I_{\{[(N/2)-1]\otimes[(N/2)-1]\}_{sym}}+\cdots+\lambda_m(b)I_{\{[(N \bmod 2)/2]\otimes[(N \bmod 2)/2]\}_{sym}}.\tag{28}$$

This is the spectral decomposition we are looking for, where $\{\lambda_j\}$ are the entanglement dependent eigenvalues of $\rho^{(N)}(b)$, the trace of the identities giving the corresponding multiplicities $\{n_j\}$. It is important to notice that, as it was mentioned before, the eigenspaces are independent of b.

The calculation of $n_j\lambda_j$ can now be readily performed from Eq. (26) by computing the trace of the projection of $|\psi(b)\rangle^N$ into each relevant irrep. The determination of the spectrum of $\rho^{(N)}(b)$ completes, as we have shown, the construction of the optimal measurement for the estimation of the entanglement. In Sec. V some examples are studied in order to clarify the implementation of the procedure.

V. SOME EXAMPLES: THE $N=1,2,3$ CASES AND BEYOND

In this section we will apply the procedure described above to obtain the optimal estimation of b when one, two, and three identical copies of the initial state are at our disposal.

A. $N=1$

The simplest case, $N=1$, is now straightforward. The state written as in Eq. (19) belongs to the $\frac{1}{2}\otimes\frac{1}{2}$ irrep of $SU(2)\times SU(2)$. From Eq. (20) we have, using the orthogonality lemma as in Eq. (28),

$$\rho^{(1)}(b)=\int dg D(g)M(b)D(g)^\dagger=\lambda_1(b)I.\tag{29}$$

The eigenvalue $\lambda_1(b)=\frac{1}{4}$ is obtained by taking the trace in the expression above. The probability $p(k|b)$ [see Eq. (13)] is independent of b, so that $p(k)=p(k|b)$ and the average Kullback information [Eq. (9)] vanishes. Consequently, no information whatsoever can be obtained about the entanglement of a completely unknown pure state if only one copy is at our disposal.

B. $N=2$

For the $N=2$ case the initial state has the form, from Eqs. (23) or (24),

$$|\psi(b)\rangle^{\otimes 2}=c_+^2|++\rangle_A\otimes|\cdot\rangle_B+c_+c_-(|+-\rangle_A\otimes|\cdot\rangle_B+|-+\rangle_A\otimes|\cdot\rangle_B)+c_-^2|--\rangle_A\otimes|\cdot\rangle_B,\tag{30}$$

Now, using lemma 2 and the conservation law mentioned above for the Clebsch-Gordan coefficients [cf. Eq. (26)], we can rewrite the state as

$$|\psi(b)\rangle^{\otimes 2}=c_+^2|^1 1\rangle_A\otimes|\cdot\rangle_B+c_+c_-(|^1 0\rangle_A\otimes|\cdot\rangle_B+|^0 0\rangle_A\otimes|\cdot\rangle_B)+c_-^2|^1-1\rangle_A\otimes|\cdot\rangle_B,\tag{31}$$

where for each party the coupled basis is related to the local one by means of an orthogonal transformation, as usual,

$$|^1 1\rangle=|++\rangle,\quad |^1-1\rangle=|--\rangle,\qquad |^1 0\rangle=\frac{1}{\sqrt{2}}(|+-\rangle+|-+\rangle),\tag{32}$$

$$|^0 0\rangle = \frac{1}{\sqrt{2}}(|+-\rangle - |-+\rangle).$$

The state $|\psi(b)\rangle^{\otimes 2}$ in Eq. (31) is supported then in the $1\otimes 1$ and the $0\otimes 0$ irreps of SU(2)×SU(2), and now the application of lemma 1 gives for $\rho^{(2)}(b)$:

$$\rho^{(2)}(b) = \lambda_1(b) I_{1\otimes 1} + \lambda_2(b) I_{0\otimes 0}. \tag{33}$$

We just need to pick up the contributions of Eq. (31) to each irrep, that is the trace of the corresponding projections, to find that

$$n_1\lambda_1(b) = (c_+^4 + c_+^2 c_-^2 + c_-^4) = \frac{3+b^2}{4},$$
$$n_2\lambda_2(b) = c_+^2 c_-^2 = \frac{1-b^2}{4}. \tag{34}$$

The optimal measurement [see Eq. (18)] then consists of two projectors onto the $1\otimes 1$ and $0\otimes 0$ irreps of $SU(2)\otimes SU(2)$, with probabilities $p(1|b) = n_1\lambda_1(b) = (3+b^2)/4$ and $p(2|b) = n_2\lambda_2(b) = (1-b^2)/4$, and from them $p(1) = \frac{9}{10}$ and $p(2) = \frac{1}{10}$. Finally the gain of information can be computed, using Eq. (9), and it gives $\bar{K} = 0.0375$ bits.

C. $N=3$

The last case we want to discuss is $N=3$. Starting now from Eq. (26), we have

$$\begin{aligned}|\psi(b)\rangle^{\otimes 3} = {} & c_+^3 |^{3/2}\tfrac{3}{2}\rangle_A \otimes |\cdot\rangle_B + c_+^2 c_- (|^{3/2}\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B + |^{1/2}\tfrac{1}{2}\rangle_A \\ & \otimes |\cdot\rangle_B + |^{1/2'}\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B) + c_+ c_-^2 (|^{3/2}-\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B \\ & + |^{1/2}-\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B + |^{1/2'}-\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B) \\ & + c_-^3 |^{3/2}-\tfrac{3}{2}\rangle_A \otimes |\cdot\rangle_B,\end{aligned} \tag{35}$$

we observe that only contributions to the $\frac{3}{2}\otimes\frac{3}{2}$ and to two different $\frac{1}{2}\otimes\frac{1}{2}$ irreps of SU(2)×SU(2) appear. Notice, in addition, that since in this expansion the contributions to $\frac{1}{2}\otimes\frac{1}{2}$ and to $\frac{1}{2}'\otimes\frac{1}{2}'$ only appear in a symmetric linear combination (i.e., $|^{1/2}\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B + |^{1/2'}\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B$ and $|^{1/2}-\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B + |^{1/2'}-\tfrac{1}{2}\rangle_A \otimes |\cdot\rangle_B$), the relevant irreps is precisely a symmetric combination of the two latter ones, $\{\frac{1}{2}\otimes\frac{1}{2}\}_{sym}$. The orthogonality lemma gives now

$$\rho^{(3)}(b) = \lambda_1(b) I_{3/2\otimes 3/2} + \lambda_2(b) I_{\{1/2\otimes 1/2\}_{sym}}. \tag{36}$$

Finally, by collecting the traces of each projection of Eq. (35) onto each irrep, we obtain

$$n_1\lambda_1(b) = (c_+^6 + c_+^4 c_-^2 + c_+^2 c_-^4 + c_-^6) = \frac{1+b^2}{2},$$
$$n_2\lambda_2(b) = 2(c_+^4 c_-^2 + c_+^2 c_-^4) = \frac{1-b^2}{2}, \tag{37}$$

and thus the optimal measurement is composed by 16-dimensional and four-dimensional projectors into the two irreps shown above, the corresponding probabilities being $p(1|b) = (1+b^2)/2$ and $p(2|b) = (1-b^2)/2$. From these, $p(1) = \frac{4}{5}$ and $p(2) = \frac{1}{5}$, and the gain of information is of 0.084 bits.

TABLE I. Average gain of information $\bar{K}$ about b given N copies of the state $|\psi\rangle$.

N	$\bar{K}$
1	0
2	0.03751
3	0.08397
4	0.13259
5	0.18059
10	0.39245
20	0.69639
40	1.07422
60	1.32005
80	1.50261

D. $N>3$

We have applied the same, general procedure to obtain the gain of information up to $N=80$, as reported in Table I and Fig. 1. We observe a logarithmic asymptotic dependence of the gain of information on the number N of available copies of $|\psi\rangle$, which reads

$$\bar{K} \approx 0.44 \log_2 N \tag{38}$$

bits of information on b.

VI. OPTIMAL ESTIMATION OF MIXING

So far we have considered the most general measurement involving the whole space $(\mathcal{H}_2\otimes\mathcal{H}_2)^{\otimes N}$ of N copies of a two-qubit pure state. Now we are going to study optimal *local* measurements for the estimation of its entanglement. Alice will perform a collective measurement over the N cop-

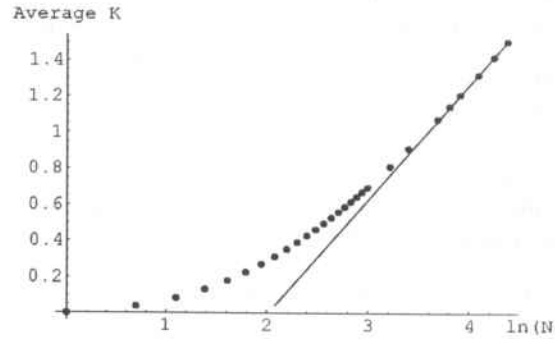


FIG. 1. Average gain of information $\bar{K}$ about b given N copies of the state $|\psi\rangle$. The points represent the results obtained by the described optimal measurement, while the line shows the asymptotic behavior.

ies of the state ρ_A in Eq. (2) at her disposal in order to estimate the parameter b. Consequently, we are also studying optimal strategies for estimating the degree of mixing of a single-qubit mixed state, when N copies are available.

In order to study the latter with more generality we will consider a generic prior distribution $f(b)$ for the degree of mixing while keeping an isotropic distribution in the Bloch vector direction $\hat{a}$ of the unknown mixed state, with

$$\int_{S^2}\frac{d\hat{a}}{4\pi}\int_0^1 db\, f(b)=1. \tag{39}$$

A general measurement on the local composite system supporting the state $\rho_A^{\otimes N}$ consists of a resolution of the identity in the corresponding Hilbert space $\mathcal{H}_2^{\otimes N}$ by means of positive operators $M^{(k)}$. The gain of information is as in Eq. (9), where now

$$p(k|b)=\mathrm{tr}[M^{(k)}\rho_A^{(N)}(b)], \tag{40}$$

so that we need to compute the effective mixed state

$$\rho_A^{(N)}(b)\equiv\int_{g\in G} dg[D(g)\rho_A(b)D(g)^\dagger]^{\otimes N}, \tag{41}$$

where the integral is performed over the group $G=\mathrm{SU}(2)$ and a single copy of the mixed state

$$\rho_A=U_A\rho_A(b)U_A^\dagger \tag{42}$$

has been expressed, as before, in terms of a reference state $\rho_A(b)\equiv(c_+^2|+\rangle\langle+|+c_-^2|-\rangle\langle-|)$ and a unitary transformation U_A. The procedure to be followed is analogous to the previous one, the spectral decomposition of the state (41), allowing us to build the optimal measurement.

The density matrix $\rho_A(b)^{\otimes N}$ can be written—by using a straightforward modification of lemma 2 and the mentioned properties of the Clebsh-Gordan coefficients—in terms of the coupled basis $\{|v_i\rangle_A\}$ as

$$\begin{aligned}\rho_A(b)^{\otimes N}=&c_+^{2N}\sum_{i;m_T=N/2}|v_i\rangle\langle v_i|_A\\&+c_+^{2(N-1)}c_-^2\sum_{i;m_T=(N/2)-1}|v_i\rangle\langle v_i|_A+\cdots\\&+c_-^{2N}\sum_{i;m_T=-(N/2)}|v_i\rangle\langle v_i|_A.\end{aligned} \tag{43}$$

Notice that the important role played before by the symmetry between the kets in A and B [cf. Eq. (26)] is now played by the symmetry between the terms in the bra and in the ket. However we see that now there are no cross-terms between inequivalent irreps of SU(2), and that equivalent irreps, such as the $N-1$ copies of the $[(N/2)-1]$ irrep, obtain equal but independent contributions. The space $\mathcal{H}_2^{\otimes N}$, decomposed in terms of irreps of SU(2) is (see also Refs. [6] and [17])

$$\begin{aligned}\mathcal{H}_2^{\otimes N}=&\frac{N}{2}\oplus\left(\frac{N}{2}-1\right)\oplus\cdots\oplus\left(\frac{N}{2}-1\right)\\&\oplus\cdots\oplus\frac{N\bmod 2}{2}\oplus\cdots\oplus\frac{N\bmod 2}{2}.\end{aligned} \tag{44}$$

The spectral decomposition of $\rho_A^{(N)}(b)$ is determined by application of the orthogonality lemma. Since equivalent irreps receive always the same contributions in the decomposition (43), the corresponding eigenvalues are equal, so that Eq. (41) reads

$$\begin{aligned}\rho_A^{(N)}(b)=&\lambda_1^L(b)I_{N/2}+\lambda_2^L(b)(I_{(N/2)-1}+\cdots+I_{(N/2)-1})+\cdots\\&+\lambda_m^L(b)(I_{(N\bmod 2)/2}+\cdots+I_{(N\bmod 2)/2}).\end{aligned} \tag{45}$$

This is, of course, simply what remains from Eq. (28) when Bob's subsystem is traced out, and we have included the whole derivation only for completeness.

Equations (16)–(18) still hold, and therefore the optimal measurement for the degree of mixing b corresponds, for any isotropic distribution, to projections onto each of the subspaces associated with the eigenvalues $\{\lambda_k^L\}$. The gain of information is then given by the right-hand side of Eq. (18). Notice that both the number of outcomes and the corresponding probabilities $p(k|b)=n_k^L\lambda_k^L(b)$ are equal to the ones obtained before for entanglement estimation. In particular, it follows that there is no way to learn about the degree of mixture of an unknown mixed state if only one copy is available.

VII. DISCUSSION AND CONCLUSIONS

In this work we have presented an optimal strategy for the estimation of the entanglement of two-qubit pure states, when N copies are available. Such optimal measurement is also minimal, in the sense that it consists of the minimum number of outcomes, namely, $N/2+1$-$(N+1)/2$ outcomes for the even-odd-N-copy case. Most of the corresponding projectors are of dimension greater than 1, and of course any further decomposition of them can be used in principle to obtain, simultaneously, some additional information about other properties of the unknown state, although our optimal POVM is not compatible with projecting onto states of the form $|\psi_i\rangle^{\otimes N}$ as optimal POVM for state determination are [2–5], and they are thus less powerful for that purpose.

An interesting particular case is when the initial state is a product state, i.e., $b=1$. It can be seen that in this situation we have only an outcome corresponding to the space of maximum spin, since $n_1\lambda_1(1)=1$. Therefore, if the outcome k, with $k>1$, is obtained, we can be assured that the state is entangled.

In Sec. VI we were also concerned with the optimal estimation of the degree of mixing. Our optimal measurement, again minimal, can be used, for instance, to quantify the degree of purity of states created by a preparation device whose polarization direction we ignore. Our strategy is actually complementary to the one aiming at optimally revealing the direction of polarization of the state [1]. As a matter of

fact, the optimal POVM we obtained is just a coarse graining of the one obtained in Ref. [6] for optimal estimation of mixed states, which turned out also to reach the optimal standards of direction estimation obtained in Ref. [1]. Consequently, the direction and modulus of the Bloch vector of an unknown mixed state can be optimally estimated simultaneously. Note that this is not a frequent situation. If, instead, we would like to estimate the x, y, and z components of the Bloch vector independently, we would have obtained incompatible optimal strategies (consider, e.g., the $N=1$ case, where an optimal measurement for the component of the Bloch vector along direction $\hat{n}$ consists of a two outcome measurement projecting on that direction).

Finally, we can argue that *bilocal* measurements, either *uncorrelated* or *classically correlated*, do not imply any improvement of the simpler, *local* ones for entanglement estimation. Once we obtain an outcome from Alice's local measurement, we can compute Bob's effective state, and it is clear from Eq. (28) that his outcome will be the same as Alice's, so that no extra information on b will be obtained. We have also seen that the optimal global measurement on $|\psi\rangle^{\otimes N}$ is perfectly mimicked by a local one on $\rho_A^{\otimes N}$ (or $\rho_B^{\otimes N}$), so that actually all four classes of measurements considered in Sec. III A are equivalent. In fact, with hindsight, one can understand this result: local measurements are performed on the reduced density matrix, which is obtained by a partial trace over the other subsystem. This operation erases the information contained in the parameters α and $\hat{b}$ of Eq. (1). On the other hand, the global measurement can be interpreted as being performed on the effective density matrix of Eq. (14), where the same parameters have been integrated over. This operation erases the information contained in them as well.

It would be challenging to address the same question for bipartite mixed states, and for systems shared by more than two parties. Note that in none of these cases is optimal estimation of the nonlocal parameters possible by means of local (or even uncorrelated bilocal) measuring strategies. This is the case for mixed states because any given reduced density matrix ρ_A may correspond to infinitely many mixed states ρ, with different degrees of entanglement, so that not even in the limit $N\to\infty$ can the entanglement of ρ be properly inferred from $\rho_A^{\otimes N}$. The mere existence of hidden nonlocal parameters [18]—that is, of entanglement parameters that are erased during the partial trace operation—also prevents uncorrelated local strategies from being optimal for estimation of pure-state tripartite entanglement. To conclude, two-qubit pure-state entanglement, a quantum nonlocal property, can be optimally estimated by means of local, but collective, measurements.

ACKNOWLEDGMENTS

We thank Susana Huelga for reactivating our interest in this problem and for interesting discussions, and J. I. Latorre for helping us with the computation of the values of Fig. 1. G.V. acknowledges CIRIT Grant No. 1997FI-00068 PG. A. A. acknowledges a grant from MEC. Financial support from CICYT Contract No. AEN98-0431 and CIRIT Contract No. 1998SGR-00026 are also aknowledged. This work was partially elaborated during the "Complexity, Computation and the Physics of Information" workshop of the Isaac Newton Institute. The authors thank the Institute and the European Science Foundation for support during this period.

[1] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
[2] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[3] R. Derka, V. Buzek, and A. K. Ekert, Phys. Rev. Lett. **80**, 1571 (1998); e-print quant-ph/9707028.
[4] J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. Lett. **81**, 1351 (1998); e-print quant-ph/9803066.
[5] A. Acín, J. I. Latorre, and P. Pascual, e-print quant-ph/9904056 [Phys. Rev. A (to be published)].
[6] G. Vidal, J. I. Latorre, P. Pascual, and R. Tarrach, Phys. Rev. A **60**, 126 (1999); e-print quant-ph/9812068.
[7] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[8] H.-K. Lo and S. Popescu, e-print quant-ph/9707038.
[9] M. A. Nielsen, Phys. Rev. Lett. **83**, 436 (1999).
[10] G. Vidal, Phys. Rev. Lett. **83**, 1046 (1999).
[11] D. Jonathan and M. B. Plenio, Phys. Rev. Lett. **83**, 1455 (1999).
[12] The problem of optimally estimating the entanglement of two-qubit pure states was recently analyzed by J. M. G. Sancho and S. F. Huelga, preprint, quant-ph/9910041. In their work they considered strategies for the N-copy case that measured only on one copy of the unknown state at a time. Their work and ours can be thus regarded as complementary.
[13] M. J. W. Hall, Phys. Lett. A **242**, 123 (1998); e-print quant-ph/9802052.
[14] S. Kullback, *Information Theory and Statistics* (Wiley, New York, 1959).
[15] A. Hobson, J. Stat. Phys. **1**, 383 (1969).
[16] R. Tarrach and G. Vidal, e-print quant-ph/9907098 [Phys. Rev. A (to be published)].
[17] J. I. Cirac, A. K. Ekert, and C. Macchiavello, Phys. Rev. Lett. **82**, 4344 (1999); e-print quant-ph/9812075.
[18] J. Kempe, Phys. Rev. A **A60**, 910 (1999).
[19] More specifically, the most informative measurements presented in this work are also optimal with respect to a fidelity-guided scheme if the quality of the guesses is evaluated through any *concave* fidelity function $F(b-b_k)$—where b is the unknown parameter and b_k is the guess made after outcome k—that reasonably takes its maximum for $b_k=b$, i.e., $F((x+x')/2)\geq[F(x)+F(x')]/2$ and $F(0)\geq F(x\in[-1,1])$.