Criterios algebraicos de separabilidad y demostraciones algorítmicas de la existencia de MUBs

Nicolás Ciancaglini[1], Santiago Cifuentes[1,2], Guido Bellomo[1], Santiago Figueira[1,2], and Ariel Bendersky[1,2]

[1] CONICET-Universidad de Buenos Aires. Instituto de Ciencias de la Computación (ICC). Buenos Aires, Argentina
[2] Departamento de Computación, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Argentina

Resumen. En este trabajo discutimos como ciertos problemas relevantes en información cuántica pueden analizarse desde una perspectiva lógica-matemática. Mostramos que propiedades como la separabilidad de estados multipartitos, y la existencia de conjuntos de bases mutuamente no sesgadas en dimensión arbitraria, pueden formularse como predicados existenciales en lógica de primer orden sobre los reales. Esta formulación permite encontrar criterios algebraicos para la separabilidad de estados en cualquier dimensión, y demostrar la existencia o no de conjuntos de bases mutuamente no sesgadas. Además, analizamos la aplicabilidad práctica de estos métodos y discutimos la necesidad de estrategias heurísticas para enfrentar su complejidad computacional en instancias de tamaño moderado.

Keywords: Eliminación de cuantificadores, Entrelazamiento, Bases mutuamente no sesgadas

1 Introducción

Preguntas como la separabilidad de estados bipartitos o la existencia de conjuntos máximos de bases mutuamente no sesgadas requieren evaluar propiedades bien definidas sobre objetos matemáticos finitamente representables. Una forma sistemática de abordar estos problemas consiste en traducir las propiedades relevantes del sistema cuántico a expresiones en Lógica de Primer Orden (LPO) sobre los números reales (Cifuentes et al., 2023; Wolf et al., 2011).

Dado que la separabilidad de un estado o la falta de sesgo entre bases pueden ser expresadas mediante igualdades, desigualdades polinomiales, sumas, productos y las operaciones lógicas booleanas con cuantificadores, ambos problemas se pueden formular como predicados de primer orden en la teoría de los números reales (Marker, 2006). Esta teoría admite procedimientos de decisión efectivos, como la eliminación de cuantificadores, que permiten establecer la veracidad o

falsedad de dichos predicados en tiempo finito (Grädel et al., 2007). Estos algoritmos son *exactos*: en ningún momento recurren a aproximaciones, sino que operan de forma simbólica.

En la Sección 2 introducimos algunas nociones de lógica de primer orden (LPO) sobre los reales, que usaremos en las siguientes secciones para el análisis de dos problemas centrales en información cuántica: el de determinar la separabilidad de estados multipartitos (Sección 3) y el de decidir la existencia de un conjunto de bases mutuamente no sesgadas (MUBs) de tamaño dado en dimensión arbitraria (Sección 4). En ambos casos, formularemos estas propiedades como predicados en LPO, lo que permite aplicar técnicas algorítmicas desarrolladas en teoría de modelos y geometría algebraica real. Este enfoque habilita, en principio, demostraciones algorítmicas de la existencia (o inexistencia) de MUBs, y la obtención de criterios algebraicos de separabilidad en dimensión finita.

Si bien los algoritmos de decisión general no son eficientes, sirven como herramienta conceptual para describir la forma que tendrían tales criterios y motivan la búsqueda de soluciones más específicas y computacionalmente viables. A modo de *prueba de concepto* en (Cifuentes et al., 2023) puede verse una utilización de un algoritmo semidecisional para el caso de inexistencia de 4 MUBs en dimensión 2.

2 Lógica de Primer Orden

La lógica de primer orden es un lenguaje formal que permite razonar sobre estructuras matemáticas mediante igualdades, conectores booleanos (como conjunción, disyunción, negación e implicación), cuantificadores (*para todo*, *existe*) y variables. Dado un lenguaje $\mathcal{L}$ con símbolos para funciones, relaciones y constantes, una $\mathcal{L}$-estructura $\mathcal{M}$ consiste en un conjunto X (dominio) junto con una interpretación de los símbolos de $\mathcal{L}$: cada constante se interpreta como un elemento de X, cada relación n-aria como un subconjunto de X^n, y cada función como una aplicación $X^n \to X$. Una fórmula ϕ sobre $\mathcal{L}$ es verdadera en $\mathcal{M}$ si la propiedad que expresa se verifica al interpretar las variables libres según una valuación $v\colon \mathrm{Var} \to X$ y los símbolos de $\mathcal{L}$ según $\mathcal{M}$. Las fórmulas sin variables libres se denominan *sentencias*. Dado un conjunto T de $\mathcal{L}$-sentencias, decimos que $\mathcal{M}$ es un *modelo* de T si satisface todas las $\mathcal{L}$-sentencias de T.

Una $\mathcal{L}$-teoría T es un conjunto de sentencias sobre el lenguaje $\mathcal{L}$. Las sentencias que se deducen de T se llaman *teoremas*. Decimos que T es *completa* si para toda sentencia ϕ, o bien ϕ o su negación pertenece a T.

La teoría de los *cuerpos reales cerrados* (RCF) se define en el lenguaje de los anillos ordenados $\mathcal{L}_{\mathrm{or}}$, que incluye las operaciones $+, -, \cdot$, las constantes $0, 1$ y la relación de orden $<$. Sus axiomas incluyen: 1) los axiomas de cuerpo, 2) que -1 no es suma de cuadrados, 3) que todo elemento es cuadrado o su opuesto lo es, y 4) que todo polinomio de grado impar tiene raíz. Tarski demostró que RCF es una teoría completa, y que $\mathbb{R}$ es un modelo de RCF (ver, por ej., Mishra, 2012).

2.1 Eliminación de cuantificadores

Debido a la completitud de RCF se puede decidir si una $\mathcal{L}_{or}$-sentencia ϕ es un teorema de RCF enumerando exhaustivamente todos las demostraciones de la lógica hasta encontrar una que demuestre ϕ o su negación.

Aunque este algoritmo demuestra la decidibilidad de la lógica, resulta impráctico para aplicaciones concretas. Un enfoque más eficiente se basa en la propiedad de RCF de admitir *eliminación de cuantificadores*: dada una fórmula φ, es posible computar otra fórmula ψ, sin cuantificadores, tal que φ y ψ son equivalentes en la teoría de los cuerpos reales cerrados. El algoritmo más conocido para llevar a cabo esta transformación es el método CAD (Cylindrical Algebraic Decomposition), desarrollado por Collins en 1975 (Collins, 1975), cuya complejidad de peor caso es doblemente exponencial en el número de variables. CAD ha sido implementado en diversos sistemas de álgebra computacional como `Maple`, `Mathematica` y `Singular`.

En el caso de fórmulas puramente existenciales (conocido como la *teoría existencial de los reales*), la eliminación de cuantificadores es un problema NP-hard, pero resoluble en espacio polinomial. Si bien estos algoritmos no operan directamente sobre fórmulas en $\mathbb{C}$, es posible expresar sentencias sobre matrices complejas en términos de sus componentes reales, volviendo aplicables los resultados mencionados.

3 Criterios de separabilidad

Sea $\rho \in \mathbb{C}^{d\times d}$, con $d = d_A d_B$, una matriz de densidad que describe un sistema bipartito. La definición general de separabilidad (Werner, 1989) establece que ρ es separable si y sólo si admite una descomposición convexa del tipo $\rho = \sum_{i=1}^{k} p_i\, \rho_A^{(i)} \otimes \rho_B^{(i)}$, donde $p_i \geq 0$, $\sum_i p_i = 1$, y $\rho_A^{(i)} \in \mathbb{C}^{d_A\times d_A}$, $\rho_B^{(i)} \in \mathbb{C}^{d_B\times d_B}$ son matrices de densidad. Para analizar esta propiedad desde una perspectiva lógico-algebraica, puede asumirse $k \leq d^2$, según el teorema de Carathéodory (Rockafellar, 1997) aplicado al conjunto convexo de matrices separables.

Además, por convexidad y linealidad, toda matriz separable puede escribirse como combinación convexa de productos de estados puros: $\rho = \sum_{i=1}^{k} p_i\ |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|$, con $p_i \geq 0$ y $\sum_i p_i = 1$. Esta es la forma que utilizaremos para formular la propiedad de separabilidad como predicado existencial en lógica de primer orden.

Para cada $|\psi_i\rangle$ ($|\phi_i\rangle$), se usan $2d_A$ ($2d_B$) variables reales para sus coordenadas reales e imaginarias. La separabilidad de ρ se expresa como la existencia de variables reales para los pesos p_i y las partes real e imaginaria de los vectores $|\psi_i\rangle$ y $|\phi_i\rangle$, satisfaciendo la normalización de los p_i, la norma unitaria de los vectores, y la coincidencia con ρ. Estas condiciones forman un sistema de igualdades y desigualdades polinomiales sobre un número finito de variables reales, y por tanto, una fórmula *existencial* en el lenguaje de los RCF: $\exists\{p_i, \psi_i, \phi_i\} \quad \Phi(p_i, \psi_i, \phi_i)$, con Φ una conjunción de fórmulas cuantificador-libre de $\mathcal{L}_{\text{or}}$. Esta fórmula puede transformarse, por eliminación de cuantificadores, en una sentencia equivalente

sin cuantificadores, dependiendo solo de los coeficientes de ρ. Así, el conjunto de matrices separables (en dimensión fija) se define por una fórmula de LPO sobre los reales, generando descripciones algebraicas exactas de separabilidad. Este marco lógico permite incluso diseñar heurísticas verificables que exploran subconjuntos de la fórmula original.

3.1 Separabilidad vía criterio de Peres-Horodecki

Para dimensiones 2×2 o 2×3, el criterio de Peres-Horodecki (PPT) (Horodecki et al., 1996; Peres, 1996) da una condición necesaria y suficiente para la separabilidad: ρ es separable si y sólo si su traspuesta parcial ρ^{T_B} es semidefinida positiva ($\rho^{T_B} \geq 0$). Esto equivale a desigualdades polinomiales, formulando la separabilidad como un predicado existencial en la teoría de cuerpos reales cerrados.

El criterio puede expresarse en RCF usando el polinomio característico $\chi_{\rho^{T_B}}(\lambda)$. El entrelazamiento corresponde a $\exists \lambda < 0\ (\chi_{\rho^{T_B}}(\lambda) = 0)$, donde la anulación del polinomio (posiblemente complejo) implica la conjunción de dos ecuaciones polinómicas reales. Mediante eliminación de cuantificadores con algoritmos como CAD, esta fórmula se transforma en un predicado equivalente sin cuantificadores, verificable aritméticamente sobre las componentes de ρ. Para estados de Werner de la forma $\rho = p\,|\psi\rangle\langle\psi| + \frac{1-p}{4} I$ (con $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$), $\exists \lambda < 0 (\chi_{\rho^{T_B}}(\lambda) = 0)$ se reduce utilizando el solver de `Wolfram` a $p < -1 \vee p > 1/3$. Esto genera un *algoritmo de decisión exacto* para separabilidad en estas dimensiones, aplicable a cualquier ρ y extensible a problemas como la existencia de MUBs.

Sin embargo, la complejidad computacional limita la aplicación práctica. CAD es doblemente exponencial en el número de variables. En el criterio PPT para matrices de 4×4, el número de variables es moderado ($\sim$16), y el algoritmo es implementable en instancias concretas. En el problema de las MUBs en dimensión d (ver Sección 4), el número de variables crece cuadráticamente con d y linealmente con k, haciendo inviable la resolución directa incluso para valores moderados como $d = 6$, $k = 4$. Esto motiva algoritmos heurísticos o semidecisionales. Una estrategia es aplicar eliminación de cuantificadores a subconjuntos de variables/ecuaciones para buscar contradicciones y probar inexistencia (Cifuentes et al., 2023), útil cuando se sospecha no existencia (ej: 4 MUBs en $d = 6$). La combinación de métodos exactos y heurísticos proporciona un marco flexible para estudiar problemas decidibles de alta complejidad en información cuántica.

4 Existencia de bases mutuamente no sesgadas

Dado un espacio de Hilbert $\mathbb{C}^d$, se dice que dos bases ortonormales $\mathcal{B} = \{|\psi_i\rangle\}$ y $\mathcal{B}' = \{|\phi_j\rangle\}$ son *mutuamente no sesgadas* si $|\langle\psi_i|\phi_j\rangle|^2 = \frac{1}{d},\ \forall i, j$. Un conjunto de bases $\{\mathcal{B}_1, \ldots, \mathcal{B}_k\}$ es mutuamente no sesgado si esta condición se verifica para todo par de bases distintas del conjunto. Se sabe que en dimensiones $d = p^n$, con p primo, existen conjuntos completos de $d + 1$ MUBs (Wootters & Fields, 1989). En cambio, para otras dimensiones el número máximo de MUBs posibles

es desconocido (ver por ej. Paterek et al., 2009). Incluso para dimensión 6, la menor dimensión que no es potencia de primo, no se sabe si existen 4 bases mutuamente no sesgadas.

La existencia de k bases $\mathcal{B}_1, \dots \mathcal{B}_k$ mutuamente no sesgadas en $\mathbb{C}^d$ se reduce a la existencia de vectores satisfaciendo ciertas relaciones entre sus productos internos. Más formalmente, si $\mathcal{B}_m = \{|\psi_i^m\rangle : 1 \leq i \leq d\}$, luego las bases son mutuamente no sesgadas si

$$\left|\langle\psi_i^m|\psi_j^n\rangle\right|^2 = \begin{cases} \frac{1}{d} & \text{if } m \neq n \\ \delta_{ij} & \text{otherwise.} \end{cases} \tag{1}$$

Estas $\binom{kd}{2} + kd$ ecuaciones pueden escribirse en el lenguaje de RCF tras descomponer cada elemento de cada vector en su parte real e imaginaria como explicamos en el caso anterior, empleando $2kd^2$ variables. En el caso paradigmático de $k = 4$ y $d = 6$ el sistema tiene 288 variables, muchas más de las que las implementaciones disponibles de eliminación de cuantificadores soportan[3]. No obstante, el solver de `Wolfram` es capaz de concluir la existencia de 3 MUBs en dimensión 3, y similarmente la no existencia de 4 MUBs en dimensión 2.

Para tener una idea de la complejidad de aplicar el algoritmo CAD a la fórmula completa, podemos estimar su tiempo de ejecución utilizando la cota establecida por Renegar, 1992. La cantidad estimada de operaciones necesarias supera el orden de 10^{520} (Cifuentes et al., 2023). Esta estimación pone en evidencia la dificultad práctica de aplicar procedimientos de decisión generales para instancias de tamaño moderado. Sin embargo, en instancias concretas con estructura altamente simétrica, como ocurre con las condiciones impuestas por la existencia de MUBs, tal vez sea posible acelerar el proceso de eliminación de cuantificadores utilizando algoritmos específicos que exploten dicha simetría. Explorar esta posibilidad representa una vía prometedora para el desarrollo de procedimientos más eficientes en problemas algebraicamente estructurados.

5 Conclusiones

Hemos demostrado que la separabilidad de estados multipartitos y la existencia de conjuntos de bases mutuamente no sesgadas (MUBs) se formulan como sentencias existenciales en la teoría de cuerpos reales cerrados, lo que conduce a criterios algebraicos exactos. Sin embargo, la complejidad computacional de algoritmos generales de eliminación de cuantificadores (por ej. CAD) es muy alto y resulta inviable en casos prácticos.

Para salvar esta brecha nos proponemos dos alternativas a explorar. Por un lado, el desarrollo de heurísticas que apliquen eliminación de cuantificadores parcialmente, sobre subconjuntos críticos, para detectar contradicciones con menor

[3] En particular, el algoritmo no solo es demasiado lento para tales parámetros, sino que aparte consume mucha más memoria que la disponible en una computadora típica.

demanda computacional. Por otro lado, la búsqueda de algoritmos especializados que exploten las simetrías y estructura algebraica de los problemas para reducir variables y acelerar CAD. La sinergia de ambos enfoques podría ofrecer herramientas prácticas para resolver problemas abiertos en información cuántica.

Aunque la metodología propuesta no ha logrado todavía resolver concretamente los problemas abiertos limitándose más bien a pruebas de concepto, la incorporación de heurísticas al análisis de tales problemas resulta un hallazgo novedoso. Un siguiente paso sería utilizar estos algoritmos semidecisionales en el contexto de criterios de separabilidad.

References

Cifuentes, S., Ciancaglini, N., Bellomo, G., Figueira, S., & Bendersky, A. (2023). Towards exact algorithmic proofs of maximal mutually unbiased bases sets in arbitrary integer dimension. *arXiv preprint arXiv:2309.12399*.

Collins, G. E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decompostion. *Automata Theory and Formal Languages: 2nd GI Conference Kaiserslautern, May 20–23, 1975*, 134–183.

Grädel, E., Kolaitis, P. G., Libkin, L., Marx, M., Spencer, J., Vardi, M. Y., Venema, Y., Weinstein, S., et al. (2007). *Finite model theory and its applications* (Vol. 28). Springer.

Horodecki, M., Horodecki, P., & Horodecki, R. (1996). On the necessary and sufficient conditions for separability of mixed quantum states. *Phys. Lett. A*, *223*(1).

Marker, D. (2006). *Model theory: An introduction* (Vol. 217). Springer Science & Business Media.

Mishra, B. (2012). *Algorithmic algebra*. Springer Science & Business Media.

Paterek, T., Dakić, B., & Brukner, Č. (2009). Mutually unbiased bases, orthogonal latin squares, and hidden-variable models. *Physical Review A*, *79*(1), 012109.

Peres, A. (1996). Separability criterion for density matrices. *Physical Review Letters*, *77*(8), 1413.

Renegar, J. (1992). On the computational complexity and geometry of the first-order theory of the reals. part i: Introduction. preliminaries. the geometry of semi-algebraic sets. the decision problem for the existential theory of the reals. *Journal of symbolic computation*, *13*(3), 255–299.

Rockafellar, R. T. (1997). *Convex analysis* (Vol. 28). Princeton university press.

Werner, R. F. (1989). Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Physical Review A*, *40*(8), 4277.

Wolf, M. M., Cubitt, T. S., & Perez-Garcia, D. (2011). Are problems in quantum information theory (un) decidable? *arXiv preprint arXiv:1111.5425*.

Wootters, W. K., & Fields, B. D. (1989). Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, *191*(2), 363–381.