Galois algebras of squeezed quantum phase states

Michel Planat[1], Metod Saniga[2]

[1]Département LPMO, Institut FEMTO-ST, 32 avenue de l'Observatoire, F-25044 Besançon cedex, France

[2]Astronomical Institute, Slovak Academy of Sciences, 05960 Tatranská Lomnica, Slovak Republic

Corresponding author: Michel Planat (planat@lpmo.edu)

Coding, transmission and recovery of states with high security and efficiency, and with low fluctuations, is the main goal of quantum information protocols and their physical implementation. Quantum phase states originating from Galois algebra, and their quantum optics based realization, seems to fill the promise.

We first review the construction of complete (i.e., of cardinality $q+1$) sets of mutually unbiased bases (MUBs) of such quantum phase states in a Hilbert space of finite dimension $q = p^m$, employing the algebra of Galois fields F_q of odd characteristic p (for qudits), and that of Galois rings R_q of characteristic 4 (for qubits) [1]. Our construction is based on the additive (and the multiplicative) characters of such finite fields and rings, in the spirit of [2] and [3].

We investigate the complementarity properties of the corresponding Hermitian phase operator with respect to the number operator. We also study the phase probability distribution and variance for physical states and find them related to the Gauss sums,

$$G(\psi, \kappa) = \sum_{n \in F_q^*} \psi(n)\kappa(n), \tag{1}$$

where $\psi(n)$ represent multiplicative characters and where the additive characters are $\kappa(n) = \omega_p^{tr(n)}$, with $\omega_p = \exp(2i\pi/p)$ and $tr(n)$ being the field theoretical trace from F_q to F_p. A similar formula holds for the rings R_q with ω_p replaced by i and the corresponding trace mapping from R_q to $R_4 = Z_4$. This allows the use of well-studied number theoretical concepts as an efficient tool in our quest for the minimum uncertainty in quantum phase measurements. In particular, from the MUBs the phase variance for a class of pure physical phase states is found to be either zero for a trivial multiplicative character $\psi = 1$ (perfect squeezing) or scales as q^{-1}.

Complete sets of MUBs are also used to derive sets of maximally entangled states. The generalized Bell states in characteristic 4 are of the form

$$|\mathcal{B}_{h,b}^a\rangle = \frac{1}{\sqrt{d}} \sum_{n \in R_q} i^{tr[(a \oplus 2 \odot b) \odot n]} |n, n \oplus h\rangle, \tag{2}$$

where the addition $\oplus$ and multiplication $\odot$ are performed in the Galois ring (as already introduced in the context of quaternary codes [4]), and b, a, h are indices for the vectors, MUBs and the maximally entangled states, respectively. Conventional Bell states correspond to $q = 4$.

The Galois algebras are the crossroad of a number of important concepts, like mutual unbiasedness, quantum coherence and entanglement. Therefore, the applications such as transmitting secrete quantum keys, state recovery, error correction and computing should greatly benefit of this formalism. Recently, this approach has also been found to be intimately linked with the concept of finite projective planes and their particular geometrical objects called ovals [5].

References

[1] M. Planat et al, *Finite algebraic geometry underlying mutually unbiased quantum measurements* (submitted to Phys. Rev. A).

[2] W. K. Wootters and B.D. Fields, *Optimal state-determination by mutually unbiased measurements*, Ann. of Phys. 191, 363-381 (1989)

[3] A. Klappenecker and M. Rötteler, *Constructions of mutually unbiased bases*, quant-ph/0309120.

[4] Z.X. Wan, *Quaternary codes*, World Scientific, Singapore, 1997.

[5] M. Saniga and M. Planat, *Sets of mutually unbiased bases as arcs in finite projective planes?*, quant-ph/0409184.