

MUTUALLY UNBIASED BASES AND ORTHOGONAL LATIN SQUARES

TOMASZ PATEREK

On first sight, the number of mutually unbiased bases (MUBs) in d dimensions and the number of mutually orthogonal Latin squares (MOLS) of order d seem to be closely related. A careful look however reveals the connections cannot be really strong. In this talk a few similarities and differences between MUBs and MOLS are presented.

The first similarity involves their maximal numbers. There are at most $d + 1$ MUBs and also $d + 1$ squares in an augmented set of MOLS. This number is attained if d is a power of a prime and we give an algorithm which relates MUBs and MOLS in these dimensions [1].

Another similarity follows from considerations of composite d . One can think about a Hilbert space of a composite dimension as describing several subsystems of prime-power dimensions. Since we can always build MUBs in the global space as tensor products of MUBs for the subspaces, there are at least $M + 1$ of them for the whole system, where M is the smallest prime-power factor of d . A similar construction exists for MOLS: squares of composite orders can be built as direct products of squares of prime-power orders. The corresponding lower bound on the number of MOLS is called the MacNeish's bound.

In general, both the MacNeish's bound and the number of MUBs which follows from the tensor product construction are known not to be tight. However, the simplest example today involves dimension $d = 676$ for MUBs [2], whereas MacNeish's bound is not tight already for $d = 10$. We therefore checked whether the connection [1] also works for $d = 10$, and found it no longer links all MOLS to MUBs [3]. The general results of Ref. [4] reveal in this context that the connection fails whenever MacNeish's bound is not tight.

The last (apparent) similarity to be presented is related to incomplete sets of MOLS and MUBs. There is a Latin square of order 4 which does not have an orthogonal mate (so called bachelor Latin square) and connection [1] links it with a set of MUBs which also cannot be extended. It might be tempting to conjecture that every unextendible augmented set of MOLS has a corresponding unextendible set of MUBs. We already disproved such conjecture for the connection [1] and now we briefly describe that there is no other connection for which the conjecture would hold true.

One can see this in at least two ways [5]. The first involves bachelor Latin square of order 5. It was recently shown that bachelor Latin squares exist for all orders $d > 3$ [6]. If there is a strong relation between MOLS and MUBs, there should correspondingly exist a set of 3 MUBs in all dimensions $d > 3$. To the contrary, it is known that for $d = 5$ every set of 3 MUBs can be extended to a complete set of 6 MUBs [7].

The second way is more dramatic. It turns out that for $d = 6$ there exists a set of two MUBs which cannot be extended any further (and six is the smallest dimension in which this happens). Since an augmented set of MOLS contains at least 3 elements, the strong relation is excluded.

For more arguments against a close connection between MOLS and MUBs see Ref. [8].

REFERENCES

- [1] T. Paterek, B. Dakić and Č. Brukner, *Phys. Rev. A* **79**, 012109 (2009).
- [2] P. Wocjan and T. Beth, *Quant. Inf. Comp.* **5**, 93 (2005).
- [3] T. Paterek, M. Pawłowski, M. Grassl and Č. Brukner, in print in *Phys. Scr.*
- [4] M. Aschbacher, A. Childs, and P. Wocjan, *J. Algebr. Comb.* **25**, 111 (2007).
- [5] M. Grassl and T. Paterek, in preparation.
- [6] A. B. Evans, *Des Codes Crypt* **40**, 121 (2006); I. M. Wanless and B. S. Webb, *Des Codes Crypt* **40**, 131 (2006).
- [7] S. Brierley, S. Weigert and I. Bengtsson, *Quant. Inf. Comp.* **10**, 803 (2010).
- [8] S. Weigert and T. Durt, arXiv:1007.3969 (2010).

CENTRE FOR QUANTUM TECHNOLOGIES, NATIONAL UNIVERSITY OF SINGAPORE, EMAIL: CQTP@NUS.EDU.SG