Lift-Off Fellowship report: Constructions of mutually unbiased bases

Joanne L. Hall*

My research uses combinatorial and algebraic techniques to investigate structures of importance in cryptography and information theory.

I used the Lift-off funding for three things. Time to write a publication from my thesis [1], a research visitor and attendance at the AustMS conference and Early Career Workshop.

I arranged for Associate Professor Diane Donovan from the University of Queensland to visit RMIT for one week. Associate Professor Asha Rao (RMIT), Associate Professor Diane Donovan and I spent some intensive time around a whiteboard working on the problem outlined below.

I presented some results from my PhD thesis at the 55th Annual AustMS Meeting in Wollongong, and attended the Early Career Workshop held in the days before. The highlight of these events for me was the discussion on balancing family responsibilities with a research career.

In the final stages of writing my thesis I had an idea surrounding the construction of mutually unbiased bases. This idea was the focus of my research during the Lift-Off Fellowship.

Mutually unbiased bases (MUBs) are an important tool in quantum information theory. Two orthonormal bases B_1 and B_2 of $\mathbb{C}^d$ are *unbiased* if $|\langle \vec{x}|\vec{y}\rangle| = 1/\sqrt{d}$ for all $\vec{x} \in B_1$ and $\vec{y} \in B_2$. A set of bases for $\mathbb{C}^d$ which are pairwise unbiased is a set of *mutually unbiased bases* (MUBs).

It is known that there can be maximum of $d+1$ MUBs in $\mathbb{C}^d$ [5]. A set of $d+1$ MUBs in $\mathbb{C}^d$ is called *complete*. It is known that complete sets of MUBs exists when d is a power of a prime [5], however it is unknown if complete sets of MUBs exist in non-prime power dimensions. There are two known families of constructions of complete sets of MUBs, the Planar function construction, and the Alltop construction.

* Mathematical Sciences School, Queensland University of Technology, GPO Box 2434, Brisbane, QLD 4001, Australia. Email: j42.hall@qut.edu.au

Theorem 1 (Planar function construction)**.** [4, Theorem 4.1.] *Let $\mathbb{F}_q$ be a field of odd characteristic p. Let $\Pi(x)$ be a planar function on $\mathbb{F}_q$. Let $V_a := \{v_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors*

$$\vec{v}_{ab} = \frac{1}{\sqrt{q}}(\omega_p^{\operatorname{tr}(a\Pi(x)+bx)})_{x\in\mathbb{F}_q} = \frac{1}{\sqrt{q}}(\chi(a\Pi(x)+bx))_{x\in\mathbb{F}_q} \quad \textit{with } a,b \in \mathbb{F}_q. \tag{1}$$

The standard basis E along with the sets V_a, $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Theorem 2 (Alltop Construction)**.** [3, Theorem 1.] *Let $\mathbb{F}_q$ be a finite field of odd characteristic $p \geq 5$ and $\omega := e^{2i\pi/p}$. Let $V_a := \{\vec{v}_{ab} : b \in \mathbb{F}_q\}$ be the set of vectors*

$$\begin{aligned}\vec{v}_{ab} &:= \frac{1}{\sqrt{q}}(\omega^{\operatorname{tr}((x+b)^3+a(x+b))})_{x\in\mathbb{F}_q}\\ &= \frac{1}{\sqrt{q}}(\chi((x+b)^3+a(x+b)))_{x\in\mathbb{F}_q} \quad \textit{with } a,b \in \mathbb{F}_q.\end{aligned} \tag{2}$$

The standard basis E along with the sets V_a, $a \in \mathbb{F}_q$, form a complete set of $q+1$ MUBs in $\mathbb{C}^q$.

Let $f_{ab}(x) = (x+b)^3 + a(x+b)$. Then f_{ab} is not of the form $\alpha\Pi(x) + \beta x$ for any planar function Π or any $\alpha, \beta, a, b \in \mathbb{F}_q$. However

$$f_{ab} - f_{cd} = 3(a-c)x^2 + (3a^2 - 3c^2 + b - d)x + (a^3 - c^3 + ba - dc) \tag{3}$$

is a quadratic function. Since all quadratic functions are planar, $f_{ab} - f_{cd}$ can therefore be written in the form $\alpha\Pi(x) + \beta x$ for some $\alpha, \beta \in \mathbb{F}_q$. Hence the differences between the vectors of Alltop type MUBs are Planar function type MUBs.

Conjecture 1. *The set of functions $\{f_{ab}(x) = (a+b)^3 + a(x+b) : a, b \in \mathbb{F}_{p^r}, p > 3\}$, as used in the Alltop construction, is the only set of functions which cannot be written in the form $\alpha\Pi(x) + \beta a$ but the difference of any pair of functions can.*

Initial results have ruled out several families of planar functions [2]. New planar functions are currently being discovered, thus solving for individual families of planar function will not prove (or disprove) this conjecture. A deeper result may be required. On the other hand if we do find a counter example, then we will have a new construction of mutually unbiased bases; a perhaps more interesting result.

References

[1] Hall, J.L. and Rao, A. An algorithm for constructing Hjelmslev planes. *Submitted.*

[2] Hall, J.L., Rao, A. and Donovan, D.(2012). Planar difference functions. In *Proceedings 2012 IEEE International Symposium on Information Theory*, pp. 1082–1086.

[3] Klappenecker, A. and Rötteler, M. (2004). Constructions of mutually unbiased bases. In *Proceedings 7th International Conference on Finite Fields and Applications* (Lecture Notes Comput. Sci. **2948**), Springer, Berlin, pp. 137–144.

[4] Roy, A. and Scott A.J. (2007). Weighted complex projective 2-designs from bases: optimal state determination by orthogonal measurements. *J. Math. Phys.* **48(072110),** 24 pp.

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

Dr Hall studied algebra and coding theory for Bachelor and Master degrees at ANU. In 2011 she was awarded a PhD by RMIT University for her thesis *Mutually unbiased bases and related structures* under the supervision of Associate Professor Asha Rao. She spent a postdoctoral year at Charles University in Prague before commencing her current position as Lecturer at QUT.