The equivalence of certain auto-correlated quaternary and binary arrays

G. Hughes

Department of Mathematics, R.M.I.T.,
GPO Box 2476V, Melbourne, VIC 3001, AUSTRALIA
email: garry.hughes@rmit.edu.au

Abstract

An array of complex fourth roots of unity with a perfect auto-correlation property (a PQA) is shown to correspond to an equivalently correlated binary array (a GPBA) by a simple explicit formula. Both objects also correspond to Hadamard matrices of certain forms.

1 Introduction

A Perfect Quaternary Array (PQA) is a perfectly auto-correlated array of the complex fourth roots of unity. Arasu and de Launey [1] have constructed many new two dimensional examples. Some of these exist for dimensions where a perfectly auto-correlated binary array (a Perfect Binary Array or PBA) is either unknown or cannot exist. The concept of PBA was extended by Jedwab [4] and we show PQAs correspond precisely to certain of these so called Generalized Perfect Binary Arrays (GPBAs). This equivalence can be deduced by considering the relative difference sets that both objects define, but is easily stated explicitly. Just as GPBAs correspond to Hadamard matrices of a certain form, so then do PQAs by this correspondence.

2 PQAs and GPBAs

Let $\mathbf{s} = (s_1, \ldots, s_m)$ be a vector of positive integers and let $S = \mathbb{Z}_{s_1} \times \cdots \times \mathbb{Z}_{s_m}$, where $\mathbb{Z}_k$ denotes the cyclic group of integers $\{0, 1, \ldots, k-1\}$ under addition mod k. Define further groups, $W = \mathbb{Z}_2 \times S$ and $G = \mathbb{Z}_4 \times S$.

Let $p : S \to \{\pm 1, \pm i\} \subset \mathbb{C}$ and $\lambda : W \to \{\pm 1\}$ be set maps taking $\mathbf{0}$ to 1. The map p is a PQA if $\mathbf{0} \neq \mathbf{u} \in S$ implies

$$\sum_{\mathbf{m} \in S} p(\mathbf{m}) \overline{p(\mathbf{m} + \mathbf{u})} = 0.$$

A PBA is a PQA taking only the values ±1. We will not give the general definition of GPBA from [4], but rather restrict ourselves to the special case that is important here. We define an expansion $\Lambda : G \to \{\pm 1\}$ of λ as follows. Write $\mathbf{g} \in G$ as $\mathbf{g} = (r, \mathbf{m})$ for $r \in \mathbb{Z}_4$ and $\mathbf{m} \in S$ and let

$$\Lambda(r, \mathbf{m}) = \begin{cases} \lambda(r, \mathbf{m}) & \text{if } r = 0, 1, \\ -\lambda(r-2, \mathbf{m}) & \text{if } r = 2, 3. \end{cases}$$

Further define the auto-correlation function of Λ to be, for $\mathbf{g} \in G$,

$$\chi(\mathbf{g}) = \sum_{\mathbf{h} \in G} \Lambda(\mathbf{h}) \Lambda(\mathbf{h} + \mathbf{g}).$$

Finally, we say $\lambda : W \to \{\pm 1\}$ is a GPBA if $\mathbf{g} \neq \mathbf{0}, (2, 0, \ldots, 0)$ implies $\chi(\mathbf{g}) = 0$. In the general definition (see [4]) λ would be called a GPBA$(2, \mathbf{s})$ of type $(1, 0, \ldots, 0)$.

We now show how to convert a PQA into a GPBA and *vice versa.*

Theorem 2.1 *Suppose for all* $\mathbf{m} \in S$ *that* p *and* λ *are related by*

$$p(\mathbf{m}) = \frac{1-i}{2}(\lambda(0, \mathbf{m}) + i\lambda(1, \mathbf{m})). \tag{1}$$

Then p *is a PQA if and only if* λ *is a GPBA.*

Proof Let $\mathbf{u} \in S$. We quickly deduce the following identities,

$$\begin{aligned} \chi(0, \mathbf{u}) = -\chi(2, \mathbf{u}) &= 2 \sum_{\mathbf{m} \in S} \lambda(0, \mathbf{m})\lambda(0, \mathbf{u} + \mathbf{m}) + \lambda(1, \mathbf{m})\lambda(1, \mathbf{u} + \mathbf{m}), \\ \chi(1, \mathbf{u}) = -\chi(3, \mathbf{u}) &= 2 \sum_{\mathbf{m} \in S} \lambda(0, \mathbf{m})\lambda(1, \mathbf{u} + \mathbf{m}) - \lambda(1, \mathbf{m})\lambda(0, \mathbf{u} + \mathbf{m}). \end{aligned} \tag{2}$$

Using (1) and collecting real and imaginary terms we obtain,

$$\sum_{\mathbf{m} \in S} p(\mathbf{m}) \overline{p(\mathbf{m} + \mathbf{u})} = \frac{1}{4}(\chi(0, \mathbf{u}) - i\chi(1, \mathbf{u})). \tag{3}$$

If λ is a GPBA we have, for $\mathbf{u} \neq \mathbf{0}$, $\chi(0, \mathbf{u}) = \chi(1, \mathbf{u}) = 0$ and p is a PQA by (3). Conversely, suppose p is a PQA. On equating real and imaginary parts in (3) and using (2) we obtain $\chi(r, \mathbf{u}) = 0$ for all $(r, \mathbf{u}) \in G$ with $\mathbf{u} \neq \mathbf{0}$. Similarly, for $\mathbf{u} = \mathbf{0}$ we have $\chi(1, \mathbf{u}) = \chi(3, \mathbf{u}) = 0$ (and $\chi(0, \mathbf{u}) = -\chi(2, \mathbf{u}) = 4|S|$). Hence $\chi(\mathbf{g}) = 0$ for every $\mathbf{g} \neq \mathbf{0}, (2, 0, \ldots, 0)$. □

The equivalence of the existence of a PQA and a GPBA also follows since both objects are equivalent to a relative difference set in G relative to the subgroup $\langle (2, 0, \ldots, 0) \rangle$ (see [1, 4]). Indeed, therefore, new results on relative difference sets give corresponding results on PQAs. We give as an example a result in [1] which includes, as a special case, the well known result that there is a Perfect Quaternary Sequence of period 2^b if and only if $1 \leq b \leq 4$.

Corollary 2.2 [Arasu and De Launey] *Let* $k, b_1 \leq b_2 \neq 0$ *be non-negative integers. There is a two-dimensional PQA for* $\mathbf{s} = (2^{b_1}3^k, 2^{b_2}3^k)$ *if and only if* $b_2 - b_1 \leq 4$.

Proof When $b_2 - b_1 \leq 4$, [2, Corollary 8.1] gives, after an obvious isomorphism, a $(v, 2, v, v/2)$ relative difference set, D say, in $\mathbb{Z}_4 \times \mathbb{Z}_{2^{b_1}3^k} \times \mathbb{Z}_{2^{b_2}3^k}$ relative to the subgroup $\langle(2, 0, \dots, 0)\rangle$, where $v = 2^{1+b_1+b_2}3^{2k}$. In fact, by the remarks after [2, Corollary 8.1], this exponent bound, $b_2 - b_1 \leq 4$, is also necessary for the existence of such a D. Finally, by [4, Theorem 3.2], D is equivalent to a GPBA. □

3 PQAs and Hadamard Matrices

It is easily shown that a PQA, p, corresponds to a complex Hadamard matrix $[p(\mathbf{m} - \mathbf{u})]_{\mathbf{m},\mathbf{u}\in S}$ (see [1]). A PQA also corresponds to a (standard) Hadamard matrix as we now indicate. We define two functions from $W \times W$ to $\{\pm 1\}$ as follows: $\gamma(\mathbf{u}, \mathbf{v}) = -1$ if and only if $u_1 = v_1 = 1$; and $\partial\lambda(\mathbf{u}, \mathbf{v}) = \lambda(\mathbf{u})\lambda(\mathbf{v})\lambda(\mathbf{u} + \mathbf{v})$. The result below may be easily proved using Theorem 2.1 and general results connecting GPBAs and orthogonal cocycles (see [3, Theorem 5.3]). However, we prefer to give a direct proof because it indicates the relationship between Theorem 2.1 and the result of Miyamoto [5, Lemma 4] connecting block Hadamard matrices and complex Hadamard matrices.

Theorem 3.1 *If p and λ are related by (1), p is a PQA if and only if $\gamma\partial\lambda$ is a Hadamard matrix indexed by the elements of W.*

Proof $\gamma\partial\lambda$ is Hadamard equivalent to the block matrix $M = \begin{bmatrix} A & B \\ -B & A \end{bmatrix}$ where $A = [\lambda(0, \mathbf{m} + \mathbf{u})]_{\mathbf{m},\mathbf{u}\in S}$ and $B = [\lambda(1, \mathbf{m} + \mathbf{u})]_{\mathbf{m},\mathbf{u}\in S}$ are matrices group developed over S. By [5, Lemma 4], any block matrix such as M is a Hadamard matrix if and only if $N = \frac{1-i}{2}(A + iB)$ is a complex Hadamard matrix. Here $N = [p(\mathbf{m} + \mathbf{u})]_{\mathbf{m},\mathbf{u}\in S}$, which is group developed over S and so is Hadamard equivalent to $[p(\mathbf{m} - \mathbf{u})]_{\mathbf{m},\mathbf{u}\in S}$. □

In view of the above we see that the equivalence between PQAs and GPBAs in Theorem 2.1 arises from imposing a condition of group development on a complex Hadamard matrix.

Among PQAs those that are *flat* are of particular interest because they correspond to certain generalised Hadamard matrices indexed by S with elements in $\{\pm 1, \pm i\}$. They also correspond to PBAs of a certain form as we will see. We call a PQA *flat* if for each $\mathbf{0} \neq \mathbf{u} \in S$, the list $p(\mathbf{m})\overline{p(\mathbf{m} + \mathbf{u})}, \mathbf{m} \in S$ contains each of the four elements $\{\pm 1, \pm i\}$ an equal number of times.

Theorem 3.2 *Given a PQA, p, or equivalently a GPBA, λ, related by (1), then p is flat if and only if $p^2(\mathbf{m}) = \lambda(0, \mathbf{m})\lambda(1, \mathbf{m})$ is a PBA.*

Proof Let $\mathbf{0} \neq \mathbf{u} \in S$. Because p is a PQA, we can say that S is a union of four disjoint subsets B_k such that $|B_0| = |B_2|, |B_1| = |B_3|, |B_0| + |B_1| = |S|/2$ and $p(\mathbf{m} + \mathbf{u}) = i^k p(\mathbf{m})$ if $\mathbf{m} \in B_k$ $(k = 0, \dots, 3)$. Squaring we have,

$$p^2(\mathbf{m} + \mathbf{u}) = \begin{cases} p^2(\mathbf{m}) & \text{if } \mathbf{m} \in B_0 \cup B_2. \\ -p^2(\mathbf{m}) & \text{if } \mathbf{m} \in B_1 \cup B_3. \end{cases}$$

Assuming that p is flat we have $|B_k| = |S|/4$ $(k = 0, \dots, 3)$ and consequently $|B_0 \cup B_2| = |B_1 \cup B_3| = |S|/2$. So, the list $p^2(\mathbf{m})p^2(\mathbf{m}+\mathbf{u}), \mathbf{m} \in S$ contains ±1 an equal number of times.

Conversely, assuming p^2 is a PBA, there are two disjoint subsets A_0, A_1 of S such that $|A_0| = |A_1| = |S|/2$ and $p^2(\mathbf{m}+\mathbf{u}) = (-1)^j p^2(\mathbf{m})$ if $\mathbf{m} \in A_j$ $(j = 0, 1)$. Hence $A_0 = B_0 \cup B_2$ and $A_1 = B_1 \cup B_3$, and therefore $|B_k| = |A_0|/2 = |S|/4$ $(k = 0, \dots, 3)$. This makes p flat. □

Acknowledgments

I would like to thank Prof. Kathy Horadam for many helpful discussions.

References

[1] K. T. Arasu and W. de Launey, Two Dimensional Perfect Quaternary Arrays, *Draft* Jan. 1998.

[2] J. A. Davis and J. Jedwab, A Unifying Construction for Difference Sets, *J. Comb. Theory Ser. A*, **80** (1997), pp. 13-78.

[3] G. Hughes, Non-Splitting Abelian $(4t, 2, 4t, 2t)$ Relative Difference Sets and Hadamard Cocycles, *European J. Combin.* **21(3)** (2000), pp. 323-331.

[4] J. Jedwab, Generalized Perfect Arrays and Menon Difference Sets, *Des. Codes Cryptogr.*, **2** (1992), pp. 19-68.

[5] M. Miyamoto, A Construction of Hadamard Matrices, *J. Comb. Theory Ser. A*, **57** (1991), pp. 86-108.

(Received 31/5/99)