Second Order Conditions for Hadamard Matrices Stemming from the Fourier Matrix

Remus Nicoara and Joseph White
University of Tennessee, Knoxville

Abstract

Let G be a finite group and denote by $\mathfrak{C}_G$ the commuting square associated to G. In [Ni3] the first author introduced second order conditions necessary for a commuting square to admit sequential deformations in the moduli space of non-isomorphic commuting squares. In this paper we investigate these conditions for group commuting squares $\mathfrak{C}_G$. We are especially interested in the case $G = \mathbb{Z}_n$, since deforming the commuting square $\mathfrak{C}_{\mathbb{Z}_n}$ is equivalent to deforming the Fourier matrix F_n by complex Hadamard matrices. We show that for $G = \mathbb{Z}_n$ the second order conditions follow automatically from the first order conditions, but the same is not true for every finite abelian group G. Our result gives a complete description of the second order deformations of the Fourier matrix F_n in the moduli space of non-equivalent complex Hadamard matrices.

1 Introduction

Commuting squares were introduced in [Po2], as invariants and construction data in Jones' theory of subfactors ([Jo], [JS]). They encode the generalized symmetries of the subfactor, and in certain situations they are complete invariants of the subfactor ([Po1],[Po2]). The 'easiest' class of commuting squares arises from groups. Any finite group G can be encoded in a group commuting square:

$$\mathfrak{C}_G = \begin{pmatrix} D & \subset & \mathrm{M_n}(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C}I_n & \subset & \mathbb{C}[G] \end{pmatrix}$$

where $D \simeq l^\infty(G)$ is the algebra of $n \times n$ diagonal matrices, and $\mathbb{C}[G]$ denotes the group algebra of G. It can be shown that two group commuting squares are isomorphic if and only if the corresponding groups are isomorphic. The subfactor associated to $\mathfrak{C}_G$ by iterating Jones' basic construction is a cross product subfactor, hence of depth 2. Moreover, if G is abelian then $\mathfrak{C}_G$ is a spin model commuting square, and the associated subfactor is a Hadamard subfactor in the sense of [Ni2].

In this paper we attempt to better understand the structure of the moduli space of non-isomorphic commuting squares around some of its 'easier' points. Even in the case of commuting squares arising from Fourier matrices (cyclic groups), this is an unsolved problem with far-reaching consequences. For example, the structure of the moduli space of non-equivalent 6×6 Hadamard matrices in a neighborhood of F_6 has applications in quantum information theory (see [We], [TaZy2]).

In [Ni1] the first author initiated a study of the sequential deformations of a commuting square, in the class of commuting squares. It was shown that if a commuting square satisfies a certain *span condition*, then it is isolated among all non-isomorphic commuting squares. In the case of $\mathfrak{C}_G$, the span condition is $V = \mathrm{M_n}(\mathbb{C})$, where V is the subspace of $\mathrm{M_n}(\mathbb{C})$ given by:

$$V = \mathrm{span}\{du - ud : d \in D, u \in \mathbb{C}[G]\} + \mathbb{C}[G] + \mathbb{C}[G]' + D$$

When the span condition fails, the dimension $d'(G)$ of $V^{\perp} = \mathrm{M_n}(\mathbb{C}) \ominus \mathrm{V}$ can be interpreted as an upper bound for the number of independent directions in which $\mathfrak{C}_G$ can be deformed by non-isomorphic commuting squares. In [NiWh] we computed this dimension, which we called *the dephased defect of the group G*. We also studied the related quantity $d(G) = \dim_{\mathbb{C}}([D, \mathbb{C}[G]]^{\perp})$, called *the undephased defect of G* (or just the defect of G), which can be interpreted as an upper bound for the number of independent directions in which $\mathfrak{C}_G$ can be deformed by (not necessarily non-isomorphic) commuting squares. The terminologies 'dephased defect' and 'undephased defect' are based on previous work of [Ka], [TaZy1] and [Ba1].

Let $\mathcal{C}(\mathrm{n}) = \mathrm{M_n}(\mathbb{T}) \cap \sqrt{\mathrm{n}}\mathrm{U}(\mathrm{n})$ denote the real algebraic manifold of $n \times n$ complex Hadamard matrices, where $\mathrm{U}(\mathrm{n}) \subset \mathrm{M_n}(\mathbb{T})$ denotes the set of unitary matrices. The defect $d(\mathbb{Z}_n)$ can be interpreted as the dimension of the enveloping tangent space of $\mathcal{C}(\mathrm{n})$ at the matrix F_n:

$$\tilde{\mathrm{T}}_{\mathrm{F_n}}\mathcal{C}(\mathrm{n}) = \mathrm{T}_{\mathrm{F_n}}\mathrm{M_n}(\mathbb{T}) \cap \mathrm{T}_{\mathrm{F_n}}\sqrt{\mathrm{n}}\mathrm{U}(\mathrm{n})$$

(see [TaZy1], [Ba1], [Ba2]). Thus the defect can be regarded as an upper bound for the dimension of the tangent space to $\mathcal{C}(n)$, at the point F_n.

Note that, for general n, the manifold $\mathcal{C}(n)$ is not smooth or connected. In this paper we study further conditions on matrices a in the tangent space to $\mathcal{C}(n)$ (and more generally the tangent space to a group commuting square) to admit an analytic family of commuting squares tangent to a. We show that for $G = \mathbb{Z}_n$ the second order conditions introduced in [Ni3] follow automatically from the first order conditions, but the same is not true for every finite group G. In other words, the bound on the number $d(F)$ of possible directions of convergence around F, obtained as tangent vectors using a first order derivative argument, is not decreased by the second order condition which corresponds to taking second order derivatives. This is rather surprising and we note that the same result does not hold in general, for other abelian groups.

2 Preliminaries

For most of our paper we will assume that $G = \mathbb{Z}_n$ is a cyclic group with n elements. In this case we can identify the group algebra $\mathbb{C}[G]$ with the matrix algebra FDF^* where F is the $n \times n$ Fourier matrix, and D denotes the algebra of $n \times n$ diagonal matrices with complex entries. When n is non-prime, the dephased defect of G is nonzero and there are several constructions of analytic families of non-isomorphic Hadamard matrices containing F (see for instance [Di]).

However, it is not known what are all the analytic families of complex Hadamard matrices, containing the Fourier matrix. This problem is quite interesting for n as low as 6, as it has potential applications in quantum information theory (see [We]). We present below a more general, discrete version of this question, which pertains to the local structure around F of the moduli space of (non-equivalent) complex Hadamard matrices U.

It is more convenient to phrase our question in terms of the matrices $V = UF^*$ which are close to the identity matrix I, rather than in terms of the Hadamard matrices U which are close to F. Observe that that $V\mathbb{C}[G]V^* = VFDF^*V^* = UDU^*$, and the fact that U is Hadamard means that the following is a commuting square:

$$\begin{pmatrix} D & \subset & \mathrm{M_n}(\mathbb{C}) \\ \cup & & \cup \\ \mathbb{C}I & \subset & V\mathbb{C}[G]V^* \end{pmatrix}.$$

Question 2.1. *Let F be the Fourier matrix of order n, and $U_k \neq F$ $(k \geq 1)$ be any sequence of Hadamard matrices satisfying $U_k \to F$ as $k \to \infty$. Let $V_k = U_k F^* \to I$. What are the possible directions of convergence for V_k?*

A direction of convergence for a sequence $(V_k)_{k\geq 1}$, as defined in [Ni1], is the limit $a \in \mathrm{M_n}(\mathbb{C})$ of a subsequence of $\frac{V_k - I}{i\|V_k - I\|}$. By a compactness argument, $(V_k)_{k\geq 1}$ must have at least one direction of convergence. From results in [Ni1] it follows that any such a is orthogonal to $\mathrm{span}[D, \mathbb{C}[G]]$. Thus, the undephased defect $d(G) = \dim_{\mathbb{C}}(\mathrm{span}[D, \mathbb{C}[G]]^{\perp})$ is an upper bound for the number of independent directions of convergence. Also, the dephased defect $d'(G)$ is an upper bound for the number of independent directions of convergence if we only allow for non-equivalent Hadamard matrices.

There are however further restrictions that a must satisfy. We recall the following theorem from [Ni3], which we now state just for the case of Hadamard matrices.

Theorem 2.2. *Let $n > 1$ be non-prime, let $U_k \neq F$ be $n \times n$ Hadamard matrices converging to the Fourier matrix F, and let $a \in \mathrm{M_n}(\mathbb{C})$, $\|a\| = 1$, be a direction of convergence for U_k. Then a must satisfy the conditions:*

(i). $a = a^*$ and for all $d \in D$, $u \in FDF^*$ we have:

$$a \perp [d, u]$$

(ii). There exists $b \in \mathrm{M_n}(\mathbb{C})$ such that $b+b^* = a^2$ and for all $d \in D$, $u \in FDF^*$ we have:

$$\tau(b[d,u]) = \tau(dua^2) - \tau(daua)$$

Note that the second condition (ii) is linear in d and u, but not in a. Thus it is a priori possible that a linear combination of directions of convergence is not a direction of convergence.

Remark 2.3. *Assume that an analytic family $U_t \to F$ exists ($t \in \mathbb{R}$), and expand*

$$V_t = U_t F^* = I + ita - \frac{t^2}{2} b + ...$$

Then a, b satisfy (i) and (ii). This follows easily by just writing the unitary and commuting square relations, then identifying the coefficients of t to obtain (i) and of t^2 to obtain (ii). This suggests that also in the general situation of just a discrete sequence of Hadamard matrices we can think of (i) as a first order condition, and (ii) as a second order condition on a.

The following lemma gives us an equivalent form of the second order condition (ii), which is more suitable for computations as it no longer involves b.

Lemma 2.4. *Condition (ii) is equivalent to the following:*

(ii)' Let $d_g = e_{g,g}$ be the canonical basis for D, and let $u_h \in \mathbb{C}[G]$ be the unitaries representing $G = \mathbb{Z}_n$ ($g, h \in G$). Then for any $c_{g,h} \in \mathbb{C}$ ($g, h \in G$) we have:

$$\text{If } \sum_{g,h \in G} c_{g,h}[d_g, u_h] = 0, \text{ then } \sum_{g,h \in G} c_{g,h}(\tau(d_g u_h a^2) - \tau(d_g a u_h a)) = 0$$

Proof. The fact that (ii) implies $(ii)'$ follows easily by summing up the relations

$$c_{g,h}\tau(b[d_g, u_h]) = c_{g,h}(\tau(d_g u_h a^2) - \tau(d_g a u_h a))$$

for all $g, h \in G$. Indeed, the left side of the sum is 0:

$$\sum_{g,h \in G} c_{g,h}\tau(b[d_g, u_h]) = \tau(b(\sum_{g,h \in G} c_{g,h}[d_g, u_h])) = 0$$

which gives $\sum_{g,h \in G} c_{g,h}(\tau(d_g u_h a^2) - \tau(d_g a u_h a)) = 0$.

We now show that $(ii)'$ implies (ii). Let $f : D \times \mathbb{C}[G] \to \mathbb{C}$ be the map $f(d,u) = \tau(dua^2) - \tau(daua)$ and let $g : D \times \mathbb{C}[G] \to W$ be the map $g(d,u) = [d,u]$, where $W = \mathrm{span}[D, \mathbb{C}[G]]$. f and g are bi-linear maps. Notice that $(ii)'$ is equivalent to the existence of a linear map $\theta : W \to \mathbb{C}$ satisfying $\theta \circ g = f$. Any such linear map is of the form $\theta(x) = \tau(xb_0)$ for some $b_0 \in \mathrm{M_n}(\mathbb{C})$. Thus we obtain:

$$\tau(b_0[d,u]) = \tau(dua^2) - \tau(daua), \text{ for all } d \in D, u \in \mathbb{C}[G]$$

Taking the adjoint of this relation, using $a = a^*$, and using that D and $\mathbb{C}[G]$ are $*$-closed yields:

$$-\tau(b_0[d,u]) = \tau(a^2ud) - \tau(auad), \text{ for all } d \in D, u \in \mathbb{C}[G]$$

Subtracting the last two relations gives:

$$\tau((b_0 + b_0^*)[d,u]) = \tau([d,u]a^2), \text{ or equivalently } \tau((b_0 + b_0^* - a^2)[d,u]) = 0$$

Thus, if we denote $b = b_0 - \frac{1}{2}(b_0 + b_0^* - a^2)$, we have that $\tau(b[d,u]) = \tau(b_0[d,u])$. This means that b still satisfies $\tau(b[d,u]) = \tau(dua^2) - \tau(daua)$. Also, it is easy to check $b + b^* = a^2$. Thus b satisfies both the conditions that form (ii).

■

We end this section by recalling two results from [NiWh], which give us 'easy' bases that we will need for our computations. Note that these results are for general finite groups G and thus are in multiplicative notation, but we will switch to additive notation when working with $G = \mathbb{Z}_n$.

Remark 2.5. *Let G be a finite group. If for fixed $g, h \in G$ we define $c(h,g) \in M_n(\mathbb{C})$ by*

$$(c(h,g))_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h \text{ for some } k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

then the distinct $c(h,g)$ form a basis for $\{(c_{g,h})_{g,h\in G} \in \mathrm{M_n(\mathbb{C})} : \sum_{\mathrm{g,h}} \mathrm{c_{g,h}[d_g, u_h]} = 0\}$.

Theorem 2.6. *For every $g, h \in G$ let $a(h,g) \in M_n(\mathbb{C})$ be the matrix*

$$(a(h,g))_{p,q} = \begin{cases} 1 & \text{if } p = h^k g \text{ and } q = h^{k+1} g \text{ for some } k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}$$

For each $h \in G$, let $g_1^h, ... g_{n(h)}^h$ be a choice of representatives of the right cosets of $G/ < h >$, where $n(h) = |G|/ord(h)$ is the number of elements of $G/ < h >$. Then the matrices $\{a(h, g_k^h) : h \in G, 1 \leq k \leq n(h)\}$ form a basis for $W^\perp$.

3 The main result

We first recall a well known group theory lemma, which we will use in the proof of the main result.

Lemma 3.1. *Let G be a group, let $\{H_i\}_{i\in I}$ be a family of subgroups of G and let $(g_i)_{i\in I} \in G$. Then the set $\cap_{i\in I} g_i H_i$ is either empty, or it is a left coset of $\cap_{i\in I} H_i$.*

We are now ready to prove the main result of this paper, stating that any hermitian a in the tangent space $W^\perp$ (i.e. satisfying the first order condition) automatically satisfies the second order condition. In other words, the bound on the number of possible directions of convergence around F, given by the defect of F, is not decreased by the second order condition. This is rather surprising, and the same result does not necessarily hold for other examples of Hadamard matrices or abelian groups (see the remark at the end of this section).

Theorem 3.2. *Let $G = \mathbb{Z}_n$ and $a \in \mathrm{M_n}(\mathbb{C})$ such that a satisfies the first order condition: $a = a^*$ and $a \perp [\mathrm{D}, \mathbb{C}[\mathrm{G}]]$. Then there exists $b \in \mathrm{M_n}(\mathbb{C})$ satisfying the second order condition*

$$b + b^* = a^2 \text{ and } \tau(b[d,u]) = \tau(dua^2) - \tau(daua) \text{ for all } d \in \mathrm{D}, \mathrm{u} \in \mathbb{C}[\mathrm{G}]$$

Proof. By Lemma 2.4, it suffices to show that whenever $\sum_{g,h\in G} c_{g,h}[d_g, u_h] = 0$ then we must have

$$\sum_{g,h\in G} c_{g,h}(\tau(d_g u_h a^2) - \tau(d_g a u_h a)) = 0.$$

Since these relations are linear in $c_{g,h}$, it is sufficient to check them for a basis for all matrices $(c_{g,h})$ satisfying $\sum_{g,h\in G} c_{g,h}[d_g, u_h] = 0$. We will use the basis introduced in Remark 2.5 (which is Theorem 2.8 of [NiWh]). Fix $g, h \in \mathbb{Z}_n$ and let $c = c(g,h)$ be the matrix with entries 0 except for $c_{g+kh,g} = 1$ for $k = 1, ..., |h|$, where $|h|$ denotes the order of h.

In the computations below, all sums and products involved in the indices are taken modulo n. We have to show that

$$\sum_{k=1}^{|h|} (\tau(d_{kh+g} u_h a^2) - \tau(d_{kh+g} a u_h a)) = 0$$

Let $(a_i)_{1\le i\le N}$ be a basis for $[D, \mathbb{C}[G]]^\perp$ as in Theorem 2.6 (which is Theorem 2.13 of [NiWh]). Then every $a \in [D, \mathbb{C}[G]]^\perp$ is of the form $\sum_{i=1}^N \alpha_i a_i$ ($\alpha_i \in \mathbb{C}$) and we have:

$$\tau(dua^2) - \tau(daua) = \sum_{i,j=1}^{N} \alpha_i \alpha_j (\tau(du a_i a_j) - \tau(d a_i u a_j))$$

for all $d \in D$ and $u \in \mathbb{C}[\mathbb{G}]$. Combining the last two equalities, it follows that it is sufficient to show that for any (fixed) g, h we have:

$$\sum_{k=1}^{|h|} (\tau(d_{kh+g} u_h a_i a_j) - \tau(d_{kh+g} a_i u_h a_j)) = 0 \tag{1}$$

for any a_i, a_j (not necessarily distinct) elements of our basis.

For simplicity, we will slightly change notations and call $a = a_i$ and $\tilde{a} = a_j$ for the rest of the proof. Then (1) can be rewritten as:

$$\sum_{k=1}^{|h|} \sum_{h'=1}^{n} a_{h(k-1)+g,h'} \tilde{a}_{h',hk+g} = \sum_{k=1}^{|h|} \sum_{h'=1}^{n} a_{hk+g,h'} \tilde{a}_{-h+h',hk+g}.$$

With the notations from Theorem 2.6, we have $a = a(h_0, g_0)$ for some $h_0, g_0 \in \mathbb{Z}_n$. For the ease of notation in our computations, we will denote a by a^{h_0,g_0}. Similarly we have $\tilde{a} = a(h_1, g_1) = a^{h_1,g_1}$ for some $h_1, g_1 \in \mathbb{Z}_n$. Let $S_h = \langle h \rangle + g$, $S_{h_0} = \langle h_0 \rangle + g_0$, and $S_{h_1} = \langle h_1 \rangle + g_1$. Let δ_i^j denote the Kronecker function. We have:

$$\begin{aligned}\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{h(k-1)+g,h'}\tilde{a}_{h',hk+g} &= \sum_{k=1}^{|h|}\sum_{h'\in S_{h_0}\cap S_{h_1}} \delta_{h(k-1)+g}^{h'-h_0}\delta_{hk+g}^{h'+h_1} \\ &= \sum_{k=1}^{|h|}\sum_{h'\in S_{h_0}\cap S_{h_1}} \delta_{hk+g}^{h'+h_1}\delta_{h_1}^{h-h_0} \\ &= \delta_h^{h_0+h_1}\left|S_{h_0}\cap S_{h_1}\cap (S_h - h_1)\right|.\end{aligned}$$

Similarly, we have:

$$\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{hk+g,h'}\tilde{a}_{-h+h',hk+g} = \delta_h^{h_0+h_1}\left|S_{h_0}\cap (S_{h_1}+h)\cap (S_h + h_0)\right|.$$

By Lemma 3.1, if $S_{h_0} \cap S_{h_1} \cap (S_h - h_1)$ and $S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)$ are either both empty or non empty, then $|S_{h_0} \cap S_{h_1} \cap (S_h - h_1)| = |S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)|$ and hence, $\sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{h(k-1)+g,h'}\tilde{a}_{h',hk+g} = \sum_{k=1}^{|h|}\sum_{h'=1}^{n} a_{hk+g,h'}\tilde{a}_{-h+h',hk+g}$. Thus, it suffices to show that if $h = h_0 + h_1$, then

$$S_{h_0}\cap S_{h_1}\cap (S_h - h_1) \neq \emptyset \Leftrightarrow S_{h_0}\cap (S_{h_1}+h)\cap (S_h+h_0)\neq\emptyset$$

Assume $h = h_0 + h_1$ and $x \in S_{h_0} \cap S_{h_1} \cap (S_h - h_1)$. We exhibit a $y \in S_{h_0} \cap (S_{h_1} + h) \cap (S_h + h_0)$. If we write $y = x + z$, then z will have to satisfy $z \in < h_0 > \cap (< h_1 > +h) \cap (< h > +h_0 + h_1)$, which can be simplified to:

$$< h_0 > \cap (< h_1 > +h_0) \cap < h >$$

We used here that $h = h_0 + h_1$.

For simplicity of notations, let $r = -h_0$ and $s = h$. Then $h_1 = r + s$. We need to show that:

$$< r > \cap (< r+s > -r) \cap < s > \neq \emptyset, \text{ for any } r, s \in \mathbb{Z}_n$$

If we rewrite this statement in terms of elements of the group $\mathbb{Z}$, we have to show that for all integers $n > 1$ and r, s, we have:

$$(r\mathbb{Z}+n\mathbb{Z})\cap(s\mathbb{Z}+n\mathbb{Z})\cap(-r+(r+s)\mathbb{Z}+n\mathbb{Z})\neq\emptyset \tag{2}$$

In what follows, we will use the notations (x, y) and $[x, y]$ for the greatest common divisor, respectively the least common multiple of the integers x, y. We have:

$$r\mathbb{Z} + n\mathbb{Z} = (r,n)\mathbb{Z} \text{ and } s\mathbb{Z} + n\mathbb{Z} = (s,n)\mathbb{Z}$$

It follows that

$$(r\mathbb{Z} + n\mathbb{Z}) \cap (s\mathbb{Z} + n\mathbb{Z}) = [(r,n),(s,n)]\mathbb{Z}$$

Thus, (2) can be rewritten as:

$$[(r,n),(s,n)]\mathbb{Z} \cap (-r + (r+s,n)\mathbb{Z}) \neq \emptyset$$

or equivalently

$$r \in k\mathbb{Z}, \text{ where } k = ([(r,n),(s,n)],(r+s,n))$$

which means that all we have to check is that k divides r. It is a well known identity that $[(r,n),(s,n)] = ([r,s],n)$. Thus $k = (([r,s],n),(r+s,n)) = ([r,s],r+s,n)$. In particular k divides $([r,s],r+s)$, so if we show that $([r,s],r+s)$ divides r we are done.

Let $d = (r,s)$, $r = dr'$, $s = ds'$ with $(r',s') = 1$. Then $([r,s],r+s) = (dr's',dr'+ds') = d(r's',r'+s') = d$, which divides $r = dr'$. We used here that $(r's',r'+s') = 1$, which follows immediately from $(r',s') = 1$. This ends the proof.

■

We conclude with an example that shows that the result from the previous theorem can not be extended from $\mathbb{Z}_n$ to any abelian finite group. The computations for this example were performed using Mathematica.

Remark 3.3. *Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2$. If*

$$a = \begin{pmatrix} 0 & -1 & 0 & 1 \\ -1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

then there is no 4×4 matrix b satisfying $\tau(b[d,u]) = \tau(daua) - \tau(dua^2)$ for all $d \in \mathrm{D}$ and $u \in \mathbb{C}[G]$.

References

[Ba1] T. Banica, *The defect of generalized Fourier matrices*, Linear Algebra and its Applications, **438**, 3667-3688 (2013).

[Ba2] T. Banica, *First order deformations of the Fourier matrix*, J. Math. Phys. **55**, 1-22 (2014).

[Di] P. Dita, *Some results on the parametrization of complex Hadamard matrices*, J. Phys. A, **37** (2004) no. 20, 5355-5374

[Ha] U. Haagerup, *Orthogonal maximal abelian *-subalgebras of the $n \times n$ matrices and cyclic n-roots*, Operator Algebras and Quantum Field Theory (ed. S.Doplicher et al.), International Press (1997), 296-322

[Jo] V. F. R. Jones, *Index for subfactors*, Invent. Math **72** (1983), 1–25

[JS] V. F. R. Jones and V. S. Sunder, *Introduction to subfactors*, London Math. Soc. Lecture Notes Series **234**, Cambridge University Press, 1997

[Ka] A. Karabegov, *The reconstruction of a unitary matrix from the moduli of its elements and symbols on a finite phase space*, YERPHI preprint (1989).

[Ni1] R. Nicoara, A finiteness result for commuting squares of matrix algebras, *J. of Operator Theory* **55** (2006), no. 2, 295-310

[Ni2] R. Nicoara, Subfactors and Hadamard matrices, *J. of Operator Theory* **64** (2010)

[Ni3] R. Nicoara, *Limit Points of Commuting Squares*, Indiana University Math Journal, **60**, No 3, 847-858 (2011)

[NiWh] R. Nicoara, J. White, *The defect of a group-type commuting square*, Revue Roumaine Math., Issue 2 (2014)

[Pe] M. Petrescu, *Existence of continuous families of complex Hadamard matrices of certain prime dimensions and related results*, PhD thesis, Univ. of California Los Angeles, 1997

[Po1] S.Popa, *Classification of subfactors : the reduction to commuting squares*, Invent. Math., **101**(1990),19-43

[Po2] S.Popa, *Othogonal pairs of *-subalgebras in finite von Neumann algebras*, J. Operator Theory **9**, 253-268 (1983)

[TaZy1] W. Tadej and K. Zyczkowski, *Defect of a unitary matrix*, Linear Algebra Appl. **429** (2008), 447-481.

[TaZy2] W. Tadej and K. Zyczkowski, *A concise guide to complex Hadamard matrices* Open Systems & Infor. Dyn.,**13**(2006), 133-177

[We] R.F. Werner, *All teleportation and dense coding schemes*, J. Phys. A: Math. Gen. **34** 7081-94 (2001).