SYMMETRY IN SEMIDEFINITE PROGRAMS

FRANK VALLENTIN

ABSTRACT. This paper is a tutorial in a general and explicit procedure to simplify semidefinite programming problems which are invariant under the action of a group. The procedure is based on basic notions of representation theory of finite groups. As an example we derive the block diagonalization of the Terwilliger algebra in this framework. Here its connection to the orthogonal Hahn and Krawtchouk polynomials becomes visible.

1. INTRODUCTION

A *(complex) semidefinite programming problem* is an optimization problem of the form

(1) $$\min\{\langle C, Y\rangle : \langle A_i, Y\rangle \leq b_i,\ i = 1, \ldots, n, \text{ and } Y \succeq 0\},$$

where $A_i \in \mathbb{C}^{X\times X}$, and $C \in \mathbb{C}^{X\times X}$ are Hermitian matrices whose rows and columns are indexed by a finite set X, $(b_1, \ldots, b_n)^t \in \mathbb{R}^n$ is a given vector and $Y \in \mathbb{C}^{X\times X}$ is a variable Hermitian matrix and where "$Y \succeq 0$" means that Y is positive semidefinite. Here $\langle C, Y\rangle = \operatorname{trace}(CY)$ denotes the trace product between matrices.

Semidefinite programming is an extension of linear programming and has a wide range of applications: combinatorial optimization and control theory are the most famous ones. Although semidefinite programming has an enormous expressive power in formulating convex optimization problems it has a few practical drawbacks: Robust and efficient solvers, unlike their counterparts for solving linear programs, are currently under heavy development. So it is crucial to exploit the problems' structure to be able to perform computations.

In the last years many results were obtained if the problem under consideration has symmetry. This was done for a variety of problems and applications: interior point algorithms (Kanno, Ohsaki, Murota, Katoh [16] and de Klerk, Pasechnik [5]), polynomial optimization (Parillo and Gatermann [10] and Jansson, Lasserre, Riener, Theobald [14]), truss topology optimization (Bai, de Klerk, Pasechnik, Sotirov [3]), quadratic assignment (de Klerk, Sotirov [7]), fast mixing Markov chains on graphs (Boyd, Diaconis, Xiao [4]), graph coloring (Gvozdenovic, Laurent [13]), crossing numbers for complete binary graphs (de Klerk, Pasechnik,

---

Date: June 28, 2007.

1991 *Mathematics Subject Classification.* 90C22, 33C90.

The author was supported by the Netherlands Organization for Scientific Research under grant NWO 639.032.203 and by the Deutsche Forschungsgemeinschaft (DFG) under grant SCHU 1503/4-2.

Schrijver [6]) and coding theory (Schrijver [20], Gijswijt, Schrijver, Tanaka [11] and Laurent [18]).

In all these applications the underlying principles are similar: one simplifies the original semidefinite program which is invariant under a group action by applying an algebra isomorphism mapping a "large" matrix algebra to a "small" matrix algebra. Then it is sufficient to solve the semidefinite program using the smaller matrices. The existence of an appropriate algebra isomorphism is a classical fact from Artin-Wedderburn theory. However, in the above mentioned papers the explicit determination of an appropriate isomorphism is rather mysterious. The aim of this paper is to give an algorithmic way to do this which also is well-suited for symbolic calculations by hand.

The paper is structured as follows: Section 2 recalls basic definitions and shows how the Artin-Wedderburn theorem stated in (4) can be applied to simplify a semidefinite program invariant under a group action. Section 3 contains a proof of the Artin-Wedderburn theorem giving an explicit isomorphism. In Section 4 we apply this to the Terwilliger algebra.

This paper is of expository nature and probably few of the results are new. On the other hand a tutorial of how to use symmetry in semidefinite programming is not readily available. Furthermore our treatment of the Terwilliger algebra for binary codes is new. Schrijver [20] treated the Terwilliger algebra with elementary combinatorial and linear algebraic arguments. Our derivation has the advantage that it gives an interpretation for the matrix entries in terms of Hahn polynomials. In a similar way one can derive the block diagonalization of the Terwilliger algebra for nonbinary codes which was computed by Gijswijt, Schrijver, Tanaka [11]. Here products of Hahn and Krawtchouk polynomials occur.

2. Background and notation

In this section we present the basic framework for simplifying a semidefinite program invariant under a group action.

Let G be a finite group which acts on a finite set X by $(a, x) \mapsto x^a$ with $a \in G$ and $x \in X$. This group action extends to an action on pairs $(x, y) \in X \times X$ by $(a, (x, y)) \mapsto (x^a, y^a)$. In this way it extends to square matrices whose rows and columns are indexed by X: for an $X \times X$-matrix M we have $M^a(x, y) = M(x^a, y^a)$. A matrix M is called *invariant under* G if $M = M^a$ for all $a \in G$.

A Hermitian matrix $Y \in \mathbb{C}^{X \times X}$ is called a *feasible solution* of (1) if it fulfills the conditions $\langle A_i, Y\rangle \leq b_i$ and $Y \succeq 0$. It is called an *optimal solution* if it is feasible and if for all other feasible solutions Y' we have $\langle C, Y\rangle \leq \langle C, Y'\rangle$.

We say that the semidefinite program (1) is *invariant under* G if for every feasible solution Y and for every $a \in G$ the matrix Y^a is again a feasible solution and if it is satisfies $\langle C, Y^a\rangle = \langle C, Y\rangle$ for all $a \in G$. Because of the convexity of (1) one can find an optimal solution of (1) in the subspace $\mathcal{B}$ of matrices which are invariant under G. In fact, if Y is an optimal solution of (1), so is $\frac{1}{|G|}\sum_{a \in G} Y^a$. Hence, (1) is equivalent to

$$\min\{\langle C, Y\rangle : \langle A_i, Y\rangle \leq b_i,\ i = 1, \ldots, n,\ Y \succeq 0 \text{ and } Y \in \mathcal{B}\}. \tag{2}$$

The set $X \times X$ can be decomposed into the orbits $R_1, \ldots, R_N$ by the action of G. For every $r \in \{1, \ldots, N\}$ we define the matrix $B_r \in \{0,1\}^{X \times X}$ by $B_r(x,y) = 1$ if $(x,y) \in R_r$ and $B_r(x,y) = 0$ otherwise. Then $B_1, \ldots, B_N$ forms a basis of $\mathcal{B}$. We call $B_1, \ldots, B_N$ the *canonical basis* of $\mathcal{B}$. If $(x,y) \in R_r$ we also write $B_{[x,y]}$ instead of B_r. Note that we have $B_{[y,x]} = (B_{[x,y]})^t$.

So the first step to simplify a semidefinite program which is invariant under a group is as follows:

If the semidefinite program (1) *is invariant under* G*, then* (1) *is equivalent to*

$$\min \Big\{ c_1 y_1 + \cdots + c_N y_N \quad : \quad \begin{array}{l} a_{i1} y_1 + \cdots + a_{iN} y_N \leq b_i, \ i = 1, \ldots, n, \\ y_j = \overline{y_k} \text{ if } B_j = (B_k)^t, \\ y_1 B_1 + \cdots + y_N B_N \succeq 0 \Big\}, \end{array} \tag{3}$$

where $c_r = \langle C, B_r \rangle$*, and* $a_{ir} = \langle A_i, B_r \rangle$*.*

The following obvious property is crucial for the next step of simplifying (3): The subspace $\mathcal{B}$ is closed under matrix multiplication. So $\mathcal{B}$ is a (semisimple) algebra over the complex numbers. The Artin-Wedderburn theory (cf. [17, Chapter 1]) gives:

There are numbers d*, and* $m_1, \ldots, m_d$ *so that there is an algebra isomorphism*

$$\varphi : \mathcal{B} \to \bigoplus_{k=1}^{d} \mathbb{C}^{m_k \times m_k}. \tag{4}$$

This applied to (3) gives the final step of simplifying (1):

If the semidefinite program (1) *is invariant under* G*, then* (1) *is equivalent to*

$$\min \Big\{ c_1 y_1 + \cdots + c_N y_N \quad : \quad \begin{array}{l} a_{i1} y_1 + \cdots + a_{iN} y_N \leq b_i, \ i = 1, \ldots, n, \\ y_j = \overline{y_k} \text{ if } B_j = (B_k)^t, \\ y_1 \varphi(B_1) + \cdots + y_N \varphi(B_N) \succeq 0 \Big\}. \end{array} \tag{5}$$

Notice that since φ is an algebra isomorphism between matrix algebras with unity, φ preserves eigenvalues and hence positive semidefiniteness. In accordance to the literature, applying φ to a semidefinite program is called *block diagonalization*.

The advantage of (5) is that instead of dealing with matrices of size $|X| \times |X|$ one has to deal with block diagonal matrices with d block matrices of size $m_1, \ldots, m_d$, respectively. In many applications the sum $m_1 + \cdots + m_d$ is much smaller than $|X|$ and in particular many practical solvers take advantage of the block structure.

3. Determining a block diagonalization

In this section we give an explicit construction of an algebra isomorphism φ. It has two main features: One can turn the construction into an algorithm as we show at the end of this section, and one can use it for symbolic calculations by hand as we demonstrate in Section 4.

3.1. **Construction.** We begin with some basic notions from representation theory of finite groups. Consider the complex vector space $\mathbb{C}^X$ with inner product $(f, g) = \frac{1}{|X|}\sum_{x \in X} f(x)\overline{g(x)}$. The group G acts on $\mathbb{C}^X$ by $f^a(x) = f(x^{a^{-1}})$. Note that the inner product on $\mathbb{C}^X$ is invariant under the group action: For all $f, g \in \mathbb{C}^X$ and all $a \in G$ we have $(f^a, g^a) = (f, g)$. A subspace $H \subseteq \mathbb{C}^X$ is called a *G-space* if $H^G \subseteq H$ where $H^G = \{f^a : f \in H, a \in G\}$. It is called *irreducible* if the only proper subspace $H' \subseteq H$ with $H'^G \subseteq H'$ is $\{0\}$. Two G-spaces H and H' are called *equivalent* if there is an *G-isometry* $\phi : H \to H'$, i.e. a linear isomorphism with $\phi(f^a) = \phi(f)^a$ for all $f \in H$ and $a \in G$ and $(\phi(f), \phi(g)) = (f, g)$ for all $f, g \in H$.

By Maschke's theorem (cf. [12, Theorem 2.4.1]) one can decompose $\mathbb{C}^X$ orthogonally into irreducible G-spaces:

$$\mathbb{C}^X = (H_{1,1} \perp \ldots \perp H_{1,m_1}) \perp \ldots \perp (H_{d,1} \perp \ldots \perp H_{d,m_d}), \tag{6}$$

where $H_{k,l}$ with $k = 1, \ldots, d$ and $l = 1, \ldots, m_d$ is an irreducible G-space of dimension h_k and where $H_{k,l}$ and $H_{k',l'}$ are equivalent if and only if $k = k'$.

Let $\mathcal{A}$ be the subalgebra of $\mathbb{C}^{X \times X}$ which is generated by the permutation matrices $P_a \in \mathbb{C}^{X \times X}$ with $a \in G$ where

$$P_a(x, y) = \begin{cases} 1 & \text{if } x^{a^{-1}} = y, \\ 0 & \text{otherwise.} \end{cases} \tag{7}$$

Because of (6) the algebra $\mathcal{A}$ decomposes as a complex vector space in the following way

$$\mathcal{A} \cong \bigoplus_{k=1}^{d} \mathbb{C}^{h_k \times h_k} \otimes I_{m_k}. \tag{8}$$

By $\mathcal{B}$ we denote the *commutant* of $\mathcal{A}$:

$$\mathcal{B} = \mathrm{Comm}(\mathcal{A}) = \{B \in \mathbb{C}^{X \times X} : BA = AB \text{ for all } A \in \mathcal{A}\}. \tag{9}$$

Note that a matrix $M \in \mathbb{C}^{X \times X}$ is invariant under G if and only if it lies in the commutant $\mathcal{B}$. The double commutant theorem [12, Theorem 3.3.7] gives the following decomposition of $\mathcal{B}$ as a complex vector space:

$$\mathcal{B} \cong \bigoplus_{k=1}^{d} I_{h_k} \otimes \mathbb{C}^{m_k \times m_k}. \tag{10}$$

Let $e_{k,1,r}$ with $r = 1, \ldots, h_k$ be an orthonormal basis of the space $H_{k,1}$. Choose G-isometries $\phi_{k,l} : H_{k,1} \to H_{k,l}$. Then, $e_{k,l,r} = \phi_{k,l}(e_{k,1,r})$ is an orthonormal basis of $H_{k,l}$. Define the matrix $E_{k,i,j} \in \mathbb{C}^{X \times X}$ with $i, j = 1, \ldots, m_k$ by

$$E_{k,i,j}(x, y) = \frac{1}{|X|} \sum_{l=1}^{h_k} e_{k,i,l}(x)\overline{e_{k,j,l}(y)}. \tag{11}$$

The definition of these matrices depend on the choice of the orthonormal basis, on the chosen G-isometries and on the chosen decomposition (6). The following proposition shows the effect of different choices.

Proposition 3.1. *By $E_k(x,y)$ we denote the $m_k \times m_k$ matrix $(E_{k,i,j}(x,y))_{i,j}$.*

(a) The matrix entries $E_{k,i,j}(x,y)$ do not depend on the choice of the orthonormal basis of $H_{k,1}$.

(b) The change of $\phi_{k,i}$ to $\alpha\phi_{k,i}$ with $\alpha \in \mathbb{C}$, $|\alpha| = 1$, simultaneously changes the i-th row and i-th column in the matrix $E_k(x,y)$ by a multiplication with α and $\overline{\alpha}$, respectively.

(c) The choice of another decomposition of $H_{k,1} \perp \ldots \perp H_{k,m_k}$ as a sum of m_k orthogonal, irreducible G-spaces changes $E_k(x,y)$ to $UE_k(x,y)\overline{U}^t$ for some unitary matrix $U \in U(\mathbb{C}^{m_k})$.

Proof. This was proved in [2, Theorem 3.1] with the only difference that there only the real case was considered. The complex case follows mutatis mutandis. □

The following theorem shows that the map

$$\psi : \mathcal{B} \to \bigoplus_{k=1}^{d} \mathbb{C}^{m_k \times m_k} \tag{12}$$

mapping $E_{k,i,j}$ to the elementary matrix with the only non-zero entry 1 at position (i,j) in the k-th summand $\mathbb{C}^{m_k \times m_k}$ of the direct sum is an algebra isomorphism.

Theorem 3.2. *The matrices $E_{k,i,j}$ form a basis of $\mathcal{B}$ satisfying the equation*

$$E_{k,i,j}E_{k',i',j'} = \delta_{k,k'}\delta_{j,i'}E_{k,i,j'}. \tag{13}$$

Proof. The multiplication formula (13) is a direct consequence of the orthonormality of the vectors $e_{k,i,l}$. That $E_{k,i,j}$ is an element of $\mathcal{B}$ follows from [2, Theorem 3.1 (c)]. From (13) it follows that the matrices $E_{k,i,j}$ are linearly independent, they span a vector space of dimension $\sum_{k=1}^{d} m_k^2$. Hence, by (10), they form a basis of $\mathcal{B}$. □

Now the expansion of the basis B_r in the basis $E_{k,i,j}$ with coefficients $p_r(k,i,j)$

$$B_r = \sum_{k=1}^{d} \sum_{i,j=1}^{m_k} p_r(k,i,j)E_{k,i,j}. \tag{14}$$

gives the desired algebra isomorphism from $\mathcal{B}$ to the direct sum $\bigoplus_{k=1}^{d} \mathbb{C}^{m_k \times m_k}$:

$$\varphi(B_r) = \sum_{k=1}^{d} \sum_{i,j=1}^{m_k} p_r(k,i,j)\psi(E_{k,i,j}), \tag{15}$$

where ψ was defined in (12).

3.2. **Orthogonality relation.** For the computation of the coefficients $p_r(k,i,j)$ the following orthogonality relation is often helpful.

If we expand the basis $|X|E_{k,i,j}$ in the basis B_r we get a relation which after normalization is inverse to (14)

$$|X|E_{k,i,j} = \sum_{r=1}^{N} q_{k,i,j}(r) B_r. \tag{16}$$

So we have a orthogonality relation between the $q_{k,i,j}$:

Lemma 3.3. *Let* $v_r = |\{(x,y) \in X \times X : (x,y) \in R_r\}|$. *Then,*

$$\sum_{r=1}^{N} v_r q_{k,i,j}(r) \overline{q_{k',i',j'}(r)} = |X|^2 \delta_{k,k'} \delta_{j,j'} \operatorname{trace} E_{k,i,i'}. \tag{17}$$

Proof. Consider the sum $\sum_{x \in X} E_{k,i,j} E_{k',j',i'}(x,x)$. On the one hand it is equal to

$$\sum_{x \in X} \delta_{k,k'} \delta_{j,j'} E_{k,i,i'}(x,x) = \delta_{k,k'} \delta_{j,j'} \operatorname{trace} E_{k,i,i'}. \tag{18}$$

On the other hand it is

$$\sum_{x \in X} \sum_{y \in X} E_{k,i,j}(x,y) E_{k',j',i'}(y,x) = \frac{1}{|X|^2} \sum_{r=1}^{n} v_r q_{k,i,j}(r) \overline{q_{k',i',j'}(r)}, \tag{19}$$

which proves the lemma. □

In the case that $\operatorname{trace} E_{k,i,i'} = 0$ whenever $i \neq i'$, the orthogonality relation gives a direct way to compute $p_r(k,i,j)$ once $q_{k,i,j}(r)$ is known.

Since $E_{k,i,i}^2 = E_{k,i,i}$ the trace of $E_{k,i,i}$ equals its rank. Because one can write $E_{k,i,i}$ as

$$E_{k,i,i} = \sum_{j=1}^{h_k} e_{k,i,j} (\overline{e_{k,i,j}})^t, \tag{20}$$

and $e_{k,i,j}$, $j = 1, \ldots, h_k$, are linearly independent, the rank of $E_{k,i,i}$ is h_k.

We have

$$p_r(k,i,j) = \frac{v_r \overline{q_{k,i,j}(r)}}{|X| h_k}, \tag{21}$$

since by Lemma 3.3 and the previous remark

$$\sum_{r=1}^{N} v_r q_{k,i,j}(r) \overline{q_{k',i',j'}(r)} = |X|^2 \delta_{k,k'} \delta_{i,i'} \delta_{j,j'} h_k, \tag{22}$$

and by (14) and (16)

$$\sum_{r=1}^{N} p_r(k,i,j) q_{k',i',j'}(r) = |X| \delta_{k,k'} \delta_{i,i'} \delta_{j,j'}. \tag{23}$$

3.3. **Algorithmic issues.** We conclude this section by reviewing algorithmic issues for computing φ. To calculate the isomorphism one has to perform the following steps:

(1) Compute the orthogonal decomposition (6) $\mathbb{C}^X$ into irreducible G-spaces $H_{k,l}$.
(2) For every irreducible G-space $H_{k,1}$ determine an orthonormal basis.
(3) Find G-isometries $\phi_{k,l} : H_{k,1} \to H_{k,l}$.
(4) Express the basis B_r in the basis $E_{k,i,j}$.

Only the first step requires an algorithm which is not classical. Here one can use an algorithm of Babai and Rónya [1]. It is a randomized algorithm running in expected polynomial time for computing the orthogonal decomposition (6). It requires the permutation matrices P_a given in (7) as input, where a runs through a (favorably small) generating set of G. The other steps can be carried out using Gram-Schmidt orthonormalization and solving systems of linear equations.

4. Block diagonalization of the Terwilliger algebra

The symmetric group S_n acts on the set $X = \{0,1\}^n$ of binary vectors with length n by $(x_1,\ldots,x_n)^\sigma = (x_{\sigma(1)},\ldots,x_{\sigma(n)})$. In [20] Schrijver determined the block diagonalization of the algebra $\mathcal{B}$ of $X \times X$-matrices invariant under this group action. The algebra $\mathcal{B}$ is called the *Terwilliger algebra of the binary Hamming scheme*. Now we shall derive a block diagonalization in the framework of the previous section. In this it is possible to work over the real numbers only because all irreducible representations of the symmetric group are real.

Under the group action the set X splits into $n+1$ orbits $X_0,\ldots,X_n$ where X_m contains the elements of $\{0,1\}^n$ having Hamming weight m. So we have the orthogonal decomposition of the S_n-space $\mathbb{R}^X$ into

$$\mathbb{R}^X = \mathbb{R}^{X_0} \perp \ldots \perp \mathbb{R}^{X_n}. \tag{24}$$

It is a classical fact (cf. [8, Theorem 2.10]) that the S_n-space $\mathbb{R}^{X_m}$ decomposes further into

$$\mathbb{R}^{X_m} = \begin{cases} H_{0,m} \perp \ldots \perp H_{m,m}, & \text{when } 0 \le m \le \lfloor n/2 \rfloor, \\ H_{0,m} \perp \ldots \perp H_{n-m,m}, & \text{otherwise.} \end{cases} \tag{25}$$

where $H_{k,m}$ are irreducible S_n-spaces which correspond to the irreducible representation of S_n given by the partition $(n-k,k)$ (cf. [19, Chapter 2]). Its dimension is $h_k = \binom{n}{k} - \binom{n}{k-1}$.

Thus, the matrices $E_{k,s,t}$, with $k = 0,\ldots,\lfloor n/2 \rfloor$, which correspond to the isotypic component $H_{k,k} \perp \ldots \perp H_{k,n-k}$ of $\mathbb{R}^X$ of type $(n-k,k)$ are conveniently indexed by $s,t = k,\ldots,n-k$.

To determine $E_{k,s,t}(x,y)$ we rely on the papers [8] and [9] of Dunkl. We recall the facts and notation which we will need from them. Let $T_k : S_n \to O(\mathbb{R}^{h_k})$ be an orthogonal, irreducible representation of S_n given by the partition $(n-k,k)$. Let $k \le s \le t \le n-k$. By H, K we denote the subgroups $H = S_s \times S_{n-s}$ and $K = S_t \times S_{n-t}$ of S_n. Let $V_k \subseteq \mathbb{R}^{S_n}$ be the vector space spanned by the function T_{ij}, with $1 \le i,j \le h_k$, which are the matrix entries of T: $T_{ij}(\pi) = [T(\pi)]_{ij}$. A function $f \in V_k$ is called *H-K-invariant* if $f(h\pi k) = f(\pi)$ for all $h \in H$, $\pi \in S_n$, $k \in K$. In [8, §4] and [9, §4] Dunkl computed the H-K-invariant functions of V_k. These are all real multiples of

$$\psi_{k,s,t}(\pi) = \frac{(-s)_k(t-n)_k}{(-t)_k(s-n)_k} Q_k(v(\pi); -(n-t)-1, -t-1, s), \tag{26}$$

where $(a)_0 = 1$, $(a)_k = a(a+1)\dots(a+k-1)$, and where,

$$Q_k(x; -a-1, -b-1, m) = \frac{1}{\binom{m}{k}} \sum_{j=0}^{k} (-1)^j \frac{\binom{b-k+j}{j}}{\binom{a}{j}} \binom{m-x}{k-j} \binom{x}{j}, \tag{27}$$

are Hahn polynomials (for integers m, a, b with $a \geq m, b \geq m \geq 0$), and where

$$v(\pi) = s - |\{1, \dots, s\}^\pi \cap \{1, \dots, t\}|. \tag{28}$$

The polynomials $Q_k(x) = Q_k(x; -a-1, -b-1, m)$ are the orthogonal polynomials for the weight function $\binom{a}{x}\binom{b}{m-x}$, $x = 0, 1, \dots, m$, normalized by $Q_k(0) = 1$. For more information about Hahn polynomials we refer to [15].

We will need the square of the norm of $\psi_{k,s,t}$ which is given in [9, before Proposition 2.7]:

$$(\psi_{k,s,t}, \psi_{k,s,t}) = \frac{\psi_{k,s,t}(\mathrm{id})}{h_k} = \frac{(-s)_k(t-n)_k}{(-t)_k(s-n)_k h_k}. \tag{29}$$

Let $e_{k,s,1}, \dots, e_{k,s,h_k}$ be an orthonormal basis of $H_{k,s}$. We get an orthogonal, irreducible representation $T_{k,s} : S_n \to O(\mathbb{R}^{h_k})$ by

$$(e_{k,s,i})^\pi = \sum_{j=1}^{h_k} [T_{k,s}(\pi)]_{j,i} e_{k,s,j}. \tag{30}$$

Consider the function

$$z_{k,s,t}(\pi) = E_{k,s,t}((1^s 0^{n-s})^\pi, 1^t 0^{n-t}). \tag{31}$$

This is an H-K-invariant function because $E_{k,s,t} \in \mathcal{B}$. It lies in V_k because vector spaces spanned by matrix entries of two equivalent irreducible representations coincide. Thus, $z_{k,s,t}$ is a real multiple of $\psi_{k,s,t}$. By computing the squared norm of $z_{k,s,t}$ we determine this multiple up to sign:

$$\begin{aligned}
(z_{k,s,t}, z_{k,s,t}) &= \frac{1}{n!} \sum_{\pi \in S_n} z_{k,s,t}(\pi) z_{k,s,t}(\pi) \\
&= \frac{1}{\binom{n}{s} 2^n} \sum_{i=1}^{h_k} (e_{k,t,i}(1^t 0^{n-t}))^2 \\
&= \frac{1}{\binom{n}{s}} E_{k,t,t}(1^t 0^{n-t}, 1^t 0^{n-t}).
\end{aligned}$$

Here we used that $e_{k,s,i}$ is an orthonormal basis of $H_{k,s}$ where the inner product is $(f, g) = \frac{1}{2^n} \sum_{x \in X_s} f(x) g(x)$.

All diagonal entries belonging to $X_t \times X_t$ of $E_{k,t,t}$ coincide and all others are zero, so $\binom{n}{t} E_{k,t,t}(1^t 0^{n-t}, 1^t 0^{n-t})$ is the trace of $E_{k,t,t}$ which equals its rank h_k. Hence, $(z_{k,s,t}, z_{k,s,t}) = h_k(\binom{n}{s}\binom{n}{t})^{-1}$. So we have determined $E_{k,s,t}$ up to sign. To adjust the signs it is enough to ensure that the multiplication formula (13) is satisfied.

So putting it together, we have proved the following theorem.

Theorem 4.1. *For $x, y \in X$ define $v(x, y) = |\{i \in \{1, \ldots, n\} : x_i = 1, y_i = 0\}|$. For $k = 0, \ldots, \lfloor n/2 \rfloor$ and $s, t = k, \ldots, n-k$ with $s \leq t$ we have*

$$E_{k,s,t}(x, y) = \frac{h_k}{(\binom{n}{s}\binom{n}{t})^{1/2}} \left(\frac{(-s)_k (t-n)_k}{(-t)_k (s-n)_k} \right)^{-\frac{1}{2}} \cdot Q_k(v(x, y); -(n-t)-1, -t-1, s), \tag{32}$$

when $x \in X_s$, $y \in X_t$. In the case $x \notin X_s$ or $y \notin X_t$ we have $E_{k,s,t}(x, y) = 0$. Furthermore, $E_{k,t,s} = (E_{k,s,t})^t$.

Finally, to find the desired algebra isomorphism (4) we determine the values of $p_r(k, i, j)$ by formula (21). This is possible because $\operatorname{trace} E_{k,s,t} = 0$ whenever $s \neq t$. We represent the orbits $R_1, \ldots, R_N$ by triples (i, j, d): Two pairs $(x, y), (x', y') \in X \times X$ are equivalent whenever $x, x' \in X_i$, $y, y' \in X_j$, and $v(x, y) = v(x', y') = d$. Then,

$$p_{i,j,d}(k, s, t) = \frac{v_{i,j,d} E_{k,s,t}(x, y)}{h_k}, \tag{33}$$

where

$$v_{i,j,d} = \binom{n}{d}\binom{n-d}{i-d}\binom{n-i}{j-d+i}. \tag{34}$$

Remark 4.2. *In a similar way one can give an interpretation of the block diagonalization of the Terwilliger algebra for nonbinary codes which was computed in* [11]. *Using* [8, Theorem 4.2] *one can show the matrix entries are, up to scaling factors, products of Hahn polynomials and Krawtchouk polynomials.*

References

[1] L. Babai, L. Rónyai, *Computing irreducible representations of finite groups*, Math. Comp. **55** (1990), 705–722.

[2] C. Bachoc, F. Vallentin, *New upper bounds for kissing numbers from semidefinite programming*, preprint, arXiv:math.MG/0608426, October 2006.

[3] Y. Bai, E. de Klerk, D.V. Pasechnik, R. Sotirov, *Exploiting group symmetry in truss topology optimization*, preprint, Optimization Online, April 2007.

[4] S. Boyd, P. Diaconis, L. Xiao, *Fastest mixing Markov chain on a graph*, SIAM Rev. **46** (2004), 667–689.

[5] E. de Klerk, D.V. Pasechnik, *Solving SDP's in non-commutative algebras part I: the dual-scaling algorithm*, Discussion paper from Tilburg University, Center for economic research, 2005.

[6] E. de Klerk, D.V. Pasechnik, A. Schrijver, *Reduction of symmetric semidefinite programs using the regular $*$-representation*, Math. Prog. **109** (2007) 613–624.

[7] E. de Klerk, R. Sotirov, *Exploiting group symmetry in semidefinite programming relaxations of the quadratic assignment problem*, preprint, Optimization Online, June 2007.
[8] C.F. Dunkl, *A Krawtchouk polynomial addition theorem and wreath product of symmetric groups*, Indiana Univ. Math. J. **25** (1976), 335–358.
[9] C.F. Dunkl, *Spherical functions on compact groups and applications to special functions*, Sympos. Math. **22** (1979) 145–161.
[10] K. Gatermann, P.A. Parrilo, *Symmetry groups, semidefinite programs, and sums of squares*, J. Pure Appl. Alg. **192** (2004), 95–128.
[11] D.C. Gijswijt, A. Schrijver, H. Tanaka, *New upper bounds for nonbinary codes*, J. Combin. Theory Ser. A **13** (2006) 1719–1731.
[12] R. Goodman, N.R. Wallach, *Representations and invariants of the classical groups*, Cambridge University Press, 1998.
[13] N. Gvozdenovic, M. Laurent, *Computing the ψ and Ψ semidefinite programming bounds for the chromatic number*, preprint, Optimization Online, February, 2007.
[14] L. Jansson, J.B. Lasserre, C. Riener, T. Theobald, *Exploiting symmetries in SDP-relaxations for polynomial optimization*, preprint, Optimization Online, September 2006.
[15] S. Karlin, J. McGregor, *The Hahn polynomials, formulas and applications*, Scripta Math. **26** (1961), 33–46.
[16] Y. Kanno, M. Ohsaki, K. Murota, N. Katoh, *Group symmetry in interior-point methods for semidefinite program*, Optimization and Engineering **2** (2001) 293–320.
[17] T.Y. Lam, *A first course in noncommutative rings*, Springer, 1991.
[18] M. Laurent, *Strengthened semidefinite programming bounds for codes*, Math. Prog. **109** (2007), 239–261.
[19] B.E. Sagan, *The symmetric group, representations, combinatorial algorithms, and symmetric functions*, Springer, 2001.
[20] A. Schrijver, *New code upper bounds from the Terwilliger algebra and semidefinite programming*, IEEE Trans. Inform. Theory **51** (2005), 2859–2866.

F. VALLENTIN, CENTRUM VOOR WISKUNDE EN INFORMATICA (CWI), KRUISLAAN 413, 1098 SJ AMSTERDAM, THE NETHERLANDS

E-mail address: f.vallentin@cwi.nl