On Pivot Orbits of Boolean Functions

Constanza Riera,* Matthew G. Parker†

March 13, 2006

Abstract

We derive a spectral interpretation of the pivot operation on a graph and generalise this operation to hypergraphs. We enumerate the number of inequivalent pivot orbits for small numbers of vertices. We also construct a family of Boolean functions of degree higher than two with a large number of flat spectra with respect to the $\{I,H\}^n$ set of transforms, and compute a lower bound on this number. We establish lower bounds on the number of flat spectra of a function w.r.t. $\{I,H\}^n$ and $\{I,H,N\}^n$ depending on internal structures.

1 Introduction

Define the n-vertex graph, G, by its $n \times n$ symmetric adjacency matrix, Γ. Identify G with a quadratic Boolean function $p(x_0, x_1, \ldots, x_{n-1})$, where $p(\mathbf{x}) = \sum_{i<j} \Gamma_{ij} x_i x_j$ [10]. Let $s = (-1)^p$ be a length 2^n n-dimensional vector such that $s_i = (-1)^{p(x=i)}$. In this paper we characterise the pivot operation on graphs using algebraic normal form (ANF). We also generalise pivot to hypergraphs (i.e. to boolean functions of degree ≥ 2), and state the (necessary and sufficient) condition that a function of degree higher than quadratic must fulfill in order to allow such an operation. Then we show how the pivot operation on a (hyper)graph can be written as a transform on the bipolar vector of the function associated to it. We construct a family of Boolean functions that have a large number of flat spectra w.r.t. $\{I,H\}^n$, and compute this number. We study

*C. Riera is with the Depto. de Álgebra, Facultad de Matemáticas, Universidad Complutense de Madrid, Avda. Complutense s/n, 28040 Madrid, Spain. E-mail: `criera@mat.ucm.es`

†M.G.Parker is with the Selmer Centre, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: `matthew@ii.uib.no`. Web: `http://www.ii.uib.no/~matthew/`

the pivot orbit trajectory of structures that include a clique and develop lower bounds on the number of flat spectra of a graph w.r.t. $\{I,H\}^n$ and $\{I,H,N\}^n$.

Let $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ be the Walsh-Hadamard kernel, $N = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, where $i^2 = -1$, be the Negahadamard kernel, and I the 2×2 identity matrix. The boolean function p is defined to have a *flat spectra* with respect to an arbtirary unitary matrix U iff $s = U(-1)^p$ satisfies $|s_i| = |s_j|$, $\forall i \neq j$. Define $\{I,H,N\}^n$ as the set of unitary transforms comprising all $2^n \times 2^n$ transform matrices, U, of the form $U = \bigotimes_{j \in \mathbf{R_I}} I_j \bigotimes_{j \in \mathbf{R_H}} H_j \bigotimes_{j \in \mathbf{R_N}} N_j$, where $\mathbf{R_I}, \mathbf{R_H}$ and $\mathbf{R_N}$ partition the set of vertices. In this paper we consider mainly the (sub)set $\{I,H\}^n$ of the transforms $U \in \{I,H,N\}^n$ where $\mathbf{R_N} = \emptyset$.

2 Pivot

Definition 1 *[2, 6, 7] The action of* local complementation (LC) *(or* vertex-neighbour-complement (VNC)*) on a graph G at vertex v is defined as the graph transformation obtained by replacing the subgraph $G[\mathcal{N}(v)]$ (i.e., the induced subgraph of the neighbourhood of the v^{th} vertex of G) by its complement.*

Definition 2 *[1] The action of* pivot *on a graph, G, at two connected vertices, u and v, (i.e. where G contains the edge uv), is given by $LC(v)LC(u)LC(v)$ - that is the action of LC at vertex v, then vertex u, then vertex v again.*

Lemma 1 *Let p be a quadratic Boolean function. If we write $p = x_ix_j + x_i\mathcal{N}_i + x_j\mathcal{N}_j + R$, where $\mathcal{N}_i$, $\mathcal{N}_j$, and R are not functions of x_i or x_j. Then, after pivoting its associated graph on the edge ij, p becomes (equivalent[1] to)*

$$p_{iji} = x_ix_j + x_i\mathcal{N}_j + x_j\mathcal{N}_i + \mathcal{N}_i\mathcal{N}_j + R = p + (x_i + x_j)(\mathcal{N}_i + \mathcal{N}_j) + \mathcal{N}_i\mathcal{N}_j \ .$$

Definition 3 *Let $p = x_ix_j + q(x_0, \ldots, x_{n-1})$ be a function of any degree (≥ 2) in the variables $\{x_0, \ldots, x_{n-1}\}$ such that x_ix_j is not a multiplying term in q (that is, such that $\frac{\partial^2}{\partial x_i x_j} q = 1$). Then define the* pivot *operation in the associated hypergraph on the edge ij by its ANF as $p_{iji} = x_ix_j + x_i\mathcal{N}_j + x_j\mathcal{N}_i + \mathcal{N}_i\mathcal{N}_j + R = p + (x_i + x_j)(\mathcal{N}_i + \mathcal{N}_j) + \mathcal{N}_i\mathcal{N}_j$, where $p = x_ix_j + x_i\mathcal{N}_i + x_j\mathcal{N}_j + R$ as before.*

Remarks: Note that now there is no restriction in the degree of $\mathcal{N}_i, \mathcal{N}_j$, and also that due to the condition on p (and equivalently to it) $\mathcal{N}_i$ and $\mathcal{N}_j$ are independent of both x_i and x_j and so the formula is well-defined, while if we don't have this condition the definition is ambiguous. When p is quadratic

[1]By 'equivalent' we understand here that the graph associated to p_{iji} is the same as the graph obtained from the associated graph of p by pivoting on the edge ij.

and the vertices i and j are connected, the condition is always fulfilled and the definition is consistent.

Lemma 2 *Let G be a bipartite (hyper)graph (i.e., associated to a function of the type $X \cdot g(Y)$, with $g(Y)$ a Boolean function of any degree). Then, after pivoting on any edge of G, the resultant (hyper)graph is bipartite.*

Theorem 1 *Let p be a function that fulfills the condition of definition 3. Then, the pivot of its associated (hyper)graph lies in the orbit of $\{I, H\}^n$. Concretely, if we call p_{iji} the function result of pivoting on the edge ij of the (hyper)graph associated with p, then $(-1)^{p_{iji}} = (\bigotimes_{k \neq i,j} I_k \otimes H_i \otimes H_j)(-1)^p$.*

Corollary 1 *Let p be a Boolean function of any degree such that it satisfies the conditions of definition 3. Then, p has a flat spectrum with respect to the transform $U = \bigotimes_{k \neq i,j} I_k \otimes H_i \otimes H_j$.*

3 Enumeration of pivot orbits

We enumerate the number of orbits of connected graphs of n vertices, which are inequivalent with respect to pivot, both for the unlabelled and labelled case, as shown in Table 1. It follows from Definition 2 that each LC orbit is partitioned into a set of pivot orbits so that, given a list of all LC orbits over n vertices, we can generate and enumerate all pivot orbits over n vertices. For the unlabelled case we make use of the classification of self-dual quantum codes, which is isomorphic to the classification of LC graph orbits, as described in [4, 5] and available at [3]. This classification used *nauty* [8] to deal efficiently with graph isomorphism. The subsequent enumeration of pivot orbits of unlabelled connected graphs is shown in Table 1 up to $n = 11$. We have also classified and enumerated all pivot orbits for labelled connected graphs as shown in Table 1. A list of pivot orbit representatives for both labelled and unlabelled connected graphs is available at http://www.ii.uib.no/~matthew/pivotorbits/files.html.

Each $(k, n-k)$-bipartite graph simultaneously represents systematic forms of the generator matrix for both a binary $[n, k, d]$ linear code, C, and its dual $[n, n-k, d]$ code, $C^\perp$. Moreover, indicator vectors for both C and $C^\perp$ can be obtained from $(-1)^p$ via transforms from the set of $\{I, H\}^n$ transforms [9]. The action of pivot on a bipartite graph generates, in general, new bipartite graphs (Lemma 2) which can be interpreted as alternative systematic generator matrices for C and $C^\perp$. It follows that C and $C^\perp$ are invariant under pivot of the associated bipartite graph. It is therefore of interest to enumerate the number of pivot orbits of bipartite graphs. Table 1 enumerates all pivot orbits of unlabelled and labelled connected bipartite graphs, and a list of bipartite pivot orbit representatives for unlabelled and labelled connected graphs is available at http://www.ii.uib.no/˜matthew/bipivotorbits/files.html [2].

n	1	2	3	4	5	6	7	8	9	10	11	12	13
i_n	1	1	2	4	10	35	134	777	6702	104825	3370317		
j_n	1	1	2	11	119	2303	80923						
k_n	1	1	1	2	3	8	15	43	110	370	1260	5366	25684
l_n	1	1	1	4	26	251	3412						

Table 1: Number of pivot-inequivalent labelled/unlabelled connected graphs, i_n: unlabelled, j_n: labelled, k_n: unlabelled-bipartite, l_n: labelled-bipartite

4 Construction and bounds

We now design a family of Boolean functions in n variables of degree less or equal to $\max\{t, 2\}$, where $0 \leq t \leq n-1$, and that have a large number of flat spectra w.r.t. $\{I, H\}^n$.

- $f^{n,t} = \sum_{i=0}^{t-1} \sum_{j=t}^{n-1} x_i x_j + \sum_{i=t}^{n-2} \sum_{j=i+1}^{n-1} x_i x_j + a(x_0, x_1, \ldots, x_{n-1})$, where $\deg(a) \leq 1$.
- Family $\mathcal{F}^{n,t}$: $\mathcal{F}^{n,t} = \{f^{n,t} + h(x_0, x_1, \ldots, x_{t-1})\}$, where h is an arbitrary boolean function in t variables.

Conjecture 1 *Let $f \in \mathcal{F}^{n,t}$. Then, the pivot orbit of f occurs within $\bigcup_{k=0}^{n-1} \mathcal{F}^{n,k}$.*

Theorem 2 *Let $f \in \mathcal{F}^{n,t}$. Then the number of flat spectra of f w.r.t. $\{I, H\}^n$ is at least $(t+1)2^{n-t-1}$, where the bound is tight if f has degree t.*

Remark: If f has degree t then all the $(t+1)2^{n-t-1}$ flat spectra correspond to restrictions of f down to residual quadratic functions.

Lemma 3 *Let $f \in \mathcal{F}^{n,t}$. Then the number of flat spectra of f w.r.t. $\{I, H, N\}^n$ is at least $(n+1)(t+1)2^{n-t-1}$.*

[2] Let d_n be the number of binary linear codes isomorphic to their dual. Let c_n be the number of inequivalent binary linear codes. Then it appears that $c_n = 2k_n - d_n$, although it remains to prove this rigorously.

5 Number of flat spectra w.r.t. $\{I, H\}^n$

The *clique* in n variables (or *complete graph*) is defined as $\sum_{0 \leq i < j \leq n-1} x_i x_j$.

Lemma 4 *[11] The clique has 2^{n-1} flat spectra w.r.t. $\{I, H\}^n$, and thus maximises the number of flat spectra w.r.t. $\{I, H\}^n$.*

We study here the behaviour of a graph that contains a clique. We consider 3 cases, depending on the positions of the vertices A and B, where we pivot on the edge AB. Let C_r be the clique in r variables contained in the graph. We denote by $\mathcal{N}_A$ and $\mathcal{N}_B$ the neighbourhoods of A and B respectively, and by $\mathcal{N}_{AB}$ the intersection of the neighbourhoods.

- $A, B \in C_r$: The clique remains invariant.
- $A \in C_r,\ B \notin C_r$: Let m be the number of variables of C_r that are in $\mathcal{N}_{AB}$. Then C_r splits and we get the cliques $C_{r-m},\ C_{m+2}$, connected just by B. Moreover $A \notin C_{r-m},\ B \in C_{r-m}$ and $A, B \in C_{m+2}$.
- $A, B \notin C_r$: In this case, C_r remains invariant, independently of whether A or B are connected to it or not.

We give lower bounds on the number of flat spectra w.r.t. $\{I, H\}^n$ and $\{I, H, N\}^n$ depending on internal structures:

Lemma 5 *Consider a graph G and two unconnected subgraphs G_1 and G_2. The number of flat spectra of G w.r.t. $\{I, H\}^n$, K_{IH}, has as lower bound: $K_{IH}(G) \geq K_{IH}(G_1) \cdot K_{IH}(G_2)$*

Corollary 1 *If we decompose the graph in unconnected subgraphs $G_1, \ldots, G_t$, then $K_{IH}(G) \geq \prod_{i=1}^{t} K_{IH}(G_i)$. For instance, if we decompose the graph in unconnected cliques $C_{r_1}, \ldots, C_{r_t}$, then $K_{IH}(G) \geq \prod_{i=1}^{t} 2^{n_i - 1}$.*

Lemma 6 *This is also true for the number of flat spectra w.r.t. $\{I, H, N\}^n$: If we decompose the graph in unconnected subgraphs $G_1, \ldots, G_t$, then we have that $K_{IHN}(G) \geq \prod_{i=1}^{t} K_{IHN}(G_i)$.*

References

[1] R. Arratia, B. Bollobas, and G. B. Sorkin, "The Interlace Polynomial: a new graph polynomial", *Proc. 11th Annual ACM-SIAM Symp. on Discrete Math.*, pp. 237–245, 2000.

[2] A. Bouchet, "Tutte-Martin Polynomials and Orienting Vectors of Isotropic Systems", *Graphs Combin.*, **7**, pp. 235–252, 1991.

[3] L. E. Danielsen, "Database of Self-Dual Quantum Codes", http://www.ii.uib.no/~larsed/vncorbits/, 2004.

[4] L. E. Danielsen and M. G. Parker, "Spectral Orbits and Peak-to-Average Power Ratio of Boolean Functions with respect to the $\{I, H, N\}^n$ Transform", *Proc. of SETA04, 2004, to be published in Lecture Notes in Computer Science (LNCS), Springer-Verlag*, http://www.ii.uib.no/~matthew/seta04-parihn.pdf, 2005.

[5] L. E. Danielsen, "On Self-Dual Quantum Codes, Graphs, and Boolean Functions", *Master's Thesis, the Selmer Center, Dept. of Informatics, University of Bergen, Norway*, http://arxiv.org/abs/quant-ph/0503236, March, 2005.

[6] D. G. Glynn, "On Self-Dual Quantum Codes and Graphs", *Submitted to the Electronic Journal of Combinatorics*, Preprint: http://homepage.mac.com/dglynn/quantum_files/Personal3.html, April 2002.

[7] M. Hein, J. Eisert and H. J. Briegel, "Multi-Party Entanglement in Graph States", *Phys. Rev. A*, **69**, 6, 2004. Preprint: http://xxx.soton.ac.uk/abs/quant-ph/0307130.

[8] B. D. McKay, "nauty User's Guide", http://cs.anu.edu.au/~bdm/nauty/nug.pdf, 2004.

[9] M. G. Parker and V. Rijmen, "The Quantum Entanglement of Bipolar Sequences", *Proc. of Sequences and Their Applications - SETA 2001.* http://xxx.soton.ac.uk/ps/quant-ph/010710600 2001.

[10] C. Riera and M. G. Parker, "Generalised Bent Criteria for Boolean Functions (I)", *submitted to IEEE Trans Inform. Theory*, Dec. 2004. http://xxx.soton.ac.uk/ps/cs.IT/0502049

[11] C. Riera, G. Petrides and M. G. Parker, "Generalised Bent Criteria for Boolean Functions (II)", *submitted to IEEE Trans Inform. Theory*, Dec. 2004. http://xxx.soton.ac.uk/ps/cs.IT/0502050

[12] O. S. Rothaus, "On Bent Functions", *J. Comb. Theory*, **20A**, pp. 300–305, 1976.