Classes of Boolean circuits

František Hakl

ICS AS CR
hakl@cs.cas.cz

May 2013

Definition (operators $\natural$, $\flat$ and $\sharp$)

Let $\vec{\boldsymbol{x}} = (\vec{\boldsymbol{x}}_1, \vec{\boldsymbol{x}}_2, \cdots, \vec{\boldsymbol{x}}_n) \in \{-1, +1\}^n$. Then define the number $\vec{\boldsymbol{x}}^{int} \in \{0, \ldots, 2^n - 1\}$ as $\vec{\boldsymbol{x}}^{int} \stackrel{\text{def}}{=} \sum_{k=1}^{n} \left(\frac{\vec{\boldsymbol{x}}_k + 1}{2}\right) 2^{n-k}$.
Further let $i \in \{1, \ldots, 2^n - 1\}$ and $\vec{\alpha} \in \{0, 1\}^n$ such that $i = \sum_{j=1}^{n} \vec{\alpha}_j 2^{n-j}$. Then $i^{bin} \stackrel{\text{def}}{=} \vec{\alpha}$ and $i^{pm1} \stackrel{\text{def}}{=} 2 \cdot \vec{\alpha} - \vec{\mathbf{1}}$.

Example

1. $\left((1, -1, 1, 1, -1, -1)^T\right)^{int} = 2^5 + 2^3 + 2^2 = 44$,
2. $44^{bin} = (1, 0, 1, 1, 0, 0)^T$,
3. $44^{pm1} = (1, -1, 1, 1, -1, -1)^T$,
4. $i = \left(i^{pm1}\right)^{int}$ and $\vec{\boldsymbol{x}} = \left(\vec{\boldsymbol{x}}^{int}\right)^{pm1}$.

Definition (James Joseph Sylvester, 1867)

Let $\boldsymbol{B}^{(1)} \stackrel{\text{def}}{=} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\boldsymbol{B}^{(n)} \stackrel{\text{def}}{=} \begin{pmatrix} \boldsymbol{B}^{(n-1)} & \boldsymbol{B}^{(n-1)} \\ \boldsymbol{B}^{(n-1)} & -\boldsymbol{B}^{(n-1)} \end{pmatrix}$. Than the matrix $\boldsymbol{B}^{(n)}$ is a parity matrix of degree n.

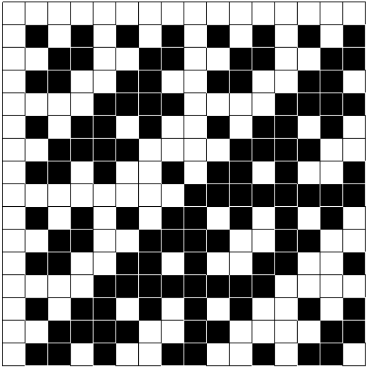
Lemma

1. $\boldsymbol{B}^{(n)}$ *is symmetric Hadamard matrix* ($\boldsymbol{B}^{(n)} \cdot {\boldsymbol{B}^{(n)}}^{T} = 2^n \boldsymbol{I}$),
2. *for all* $\vec{\boldsymbol{i}}, \vec{\boldsymbol{j}} \in \{0,1\}^n$ *is*

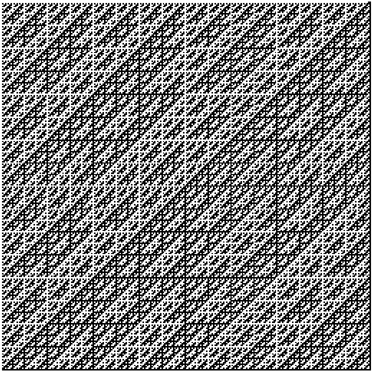
$$\boldsymbol{B}^{(n)}{}_{\vec{\boldsymbol{i}}^{int}, \vec{\boldsymbol{j}}^{int}} = \left(-1\right)^{\sum_{\alpha=1}^{n} \vec{\boldsymbol{i}}_\alpha \cdot \vec{\boldsymbol{j}}_\alpha},$$

(rows and cols of $\boldsymbol{B}^{(n)}$ *are numbered from 0 to* $2^n - 1$*).*

$\boldsymbol{B}^{(4)}$



$\boldsymbol{B}^{(8)}$



Definition

Square matrix $\boldsymbol{A}$ is INCREASING if the entries in each row and column forms a nondecreasing sequence. Square matrix $\boldsymbol{A}$ is POTENTIALLY INCREASING iff there exist permutation matrices $\boldsymbol{P}$ and $\boldsymbol{Q}$ such that the matrix $\boldsymbol{P} \cdot \boldsymbol{A} \cdot \boldsymbol{Q}$ is increasing.

Lemma

A square matrix $\boldsymbol{A}$ with entries ± 1 is potentially increasing iff does not contain submatrix of the forms $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ or $\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$.

Theorem

Let $\boldsymbol{C}$ *be square matrix of the order* 2^n, $n \geq 1$, *fulfilled condition that* $\boldsymbol{C}_{i,j} \stackrel{def}{=} 1$ *for* $i + j \leq 2^n + 1$ *and* $\boldsymbol{C}_{i,j} \stackrel{def}{=} -1$ *for* $i + j > 2^n + 1$ *(* $\boldsymbol{C}$ *has on collateral diagonal and upon* 1 *only, bellow* -1 *only). Further let us assume that the matrix* $\boldsymbol{D}$ *is arbitrary potentially increasing matrix of the order* 2^n. *Than:*

$$2^n(n+1) = \left\langle \boldsymbol{B}^{(n)} \,|\boldsymbol{C} \right\rangle \geq \left\langle \boldsymbol{B}^{(n)} \,|\boldsymbol{D} \right\rangle.$$

$=$: Let $\tau(n) \stackrel{\text{def}}{=} \left\langle \boldsymbol{B}^{(n)} \,|\boldsymbol{C} \right\rangle$ and ϕ_n^+ and ϕ_n^- denotes numbers of 1 and -1 in the matrix $\boldsymbol{B}^{(n)}$, respectively. Then $\phi_n^+ - \phi_n^- = 2^n$ implies $\tau(n) = 2^n + 2 \cdot \tau(n-1)$.
$\geq$: induction

Definition

Let the function $\widetilde{sgn} : \Re^n \rightarrow \{-1, +1\}$ is defined as $\widetilde{sgn}(z) \stackrel{\text{def}}{=} 1$ if $x > 0$ and $\widetilde{sgn}(z) \stackrel{\text{def}}{=} -1$ if $x \leq 0$.

Definition

Let $\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S$ be vectors from the space $\{-1, +1\}^n$. Than say that vector $\vec{\boldsymbol{y}}$ is THRESHOLD VECTOR of $\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S$, if there exists numbers $w_1, \ldots, w_S$ such that vector $\sum_{i=1}^{S} w_i \cdot \vec{\boldsymbol{x}}_i$ has only nonzero components and it holds that:

$$\vec{\boldsymbol{y}} \stackrel{\text{def}}{=} \widetilde{sgn}\left(\sum_{i=1}^{S} w_i \cdot \vec{\boldsymbol{x}}_i\right).$$

(Here, function $\widetilde{sgn}$ is applied to vector componentwise).

Definition

Assume that vectors $\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S$ are linearly independent and let

$$\vec{\boldsymbol{y}} \stackrel{\text{def}}{=} \sum_{i=1}^{S} \beta_i \vec{\boldsymbol{x}}_i + \vec{\boldsymbol{y}}^{\perp},$$

where $\vec{\boldsymbol{y}}^{\perp}$ is in orthogonal complement of $[\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S]_\lambda$. Further denote

$$\beta_{max} \stackrel{\text{def}}{=} \max\left\{|\beta_i| \,|\, i \in \{1, \ldots, S\}\right\}.$$

Numbers β_i can be evaluated using pseudoinverse matrices: Let $\boldsymbol{X} \stackrel{\text{def}}{=} \left(\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S\right)^T$. Than holds

$$\vec{\beta} = \left(\boldsymbol{X}^T \boldsymbol{X}\right)^{-1} \boldsymbol{X}^T \vec{\boldsymbol{y}}.$$

Lemma

Let $\vec{\boldsymbol{y}}$ *be threshold vector of the system* $(\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S)$. *Than*

$$\sum_{i=1}^{S} \left|\vec{\beta}_i\right| \geq 1 \quad .$$

Let $\sum_{i=1}^{S} \left|\vec{\beta}_i\right| < 1$. It follows $\left((\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S) \cdot \vec{\beta}\right)_i < 1$.
At the same time $\vec{\boldsymbol{y}} = (\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S)\,\vec{\beta} + \vec{\boldsymbol{y}}^{\perp}$, therefore

$$\widetilde{sgn}\left(\vec{\boldsymbol{y}}^{\perp}\right) = \widetilde{sgn}\left(\vec{\boldsymbol{y}} - (\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S)\,\vec{\beta}\right) = \widetilde{sgn}\left(\vec{\boldsymbol{y}}\right) = \vec{\boldsymbol{y}}. \tag{1}$$

Further, $\vec{\boldsymbol{y}}$ is threshold vector, so there exists $\vec{\boldsymbol{w}}$ such that $\widetilde{sgn}\left((\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S)\,\vec{\boldsymbol{w}}\right) = \vec{\boldsymbol{y}}$. This equation and equation (1) imply inequality $\left(\vec{\boldsymbol{y}}^{\perp}\right)^T \cdot (\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S)\,\vec{\boldsymbol{w}} > 0$ which contradicts with orthogonality of the vector $\vec{\boldsymbol{y}}^{\perp}$ to vectors $\vec{\boldsymbol{x}}_1, \ldots, \vec{\boldsymbol{x}}_S$.

Theorem

Let $\vec{\boldsymbol{y}}$ *be threshold vector of orthogonal system of vectors* $\vec{\boldsymbol{x}}_1, \dots, \vec{\boldsymbol{x}}_S \in \{-1, +1\}^n$. *Than*

$$S \geq \frac{n}{\max_i \left| \langle \vec{\boldsymbol{y}} \,|\, \vec{\boldsymbol{x}}_i \rangle \right|} \quad . \tag{2}$$

$\frac{\vec{\boldsymbol{x}}_i}{\|\vec{\boldsymbol{x}}_i\|}$ is orthonormal system.

Hence $\beta_i \|\vec{\boldsymbol{x}}_i\| = \left\langle \vec{\boldsymbol{y}} \,\middle|\, \frac{\vec{\boldsymbol{x}}_i}{\|\vec{\boldsymbol{x}}_i\|} \right\rangle$, and $\|\vec{\boldsymbol{x}}_i\| = \sqrt{n}$.

Thus

$$S \cdot \frac{\max_i \left| \langle \vec{\boldsymbol{y}} \,|\, \vec{\boldsymbol{x}}_i \rangle \right|}{n} = S \cdot \beta_{max} \geq \sum_{i=1}^{S} \left| \vec{\beta}_i \right| \geq 1 .$$

Basic parity vectors $\vec{\boldsymbol{p}}_i$ (dim = 2^{2k}) and corresponding conjugated matrices $\boldsymbol{M}_{\vec{\boldsymbol{p}}_i}$

$$\begin{pmatrix} 1\\1\\1\\1\\1\\1\\1\\1\\-1\\-1\\-1\\-1\\-1\\-1\\-1\\-1 \end{pmatrix}
\begin{pmatrix} 1\\1\\1\\1\\-1\\-1\\-1\\-1\\1\\1\\1\\1\\-1\\-1\\-1\\-1 \end{pmatrix}
\begin{pmatrix} 1\\1\\-1\\-1\\1\\1\\-1\\-1\\1\\1\\-1\\-1\\1\\1\\-1\\-1 \end{pmatrix}
\begin{pmatrix} 1\\-1\\1\\-1\\1\\-1\\1\\-1\\1\\-1\\1\\-1\\1\\-1\\1\\-1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & -1 & -1\\ 1 & 1 & -1 & -1\\ 1 & 1 & -1 & -1\\ 1 & 1 & -1 & -1 \end{pmatrix} \quad
\begin{pmatrix} 1 & -1 & 1 & -1\\ 1 & -1 & 1 & -1\\ 1 & -1 & 1 & -1\\ 1 & -1 & 1 & -1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\\ -1 & -1 & -1 & -1\\ -1 & -1 & -1 & -1 \end{pmatrix} \quad
\begin{pmatrix} 1 & 1 & 1 & 1\\ -1 & -1 & -1 & -1\\ 1 & 1 & 1 & 1\\ -1 & -1 & -1 & -1 \end{pmatrix}$$

Theorem

Let $n \stackrel{def}{=} 2k$, $\vec{\boldsymbol{y}} \in \{-1,+1\}^{2^n}$ *be threshold vector of the system of basic parity vectors and constant vector. Than the matrix* $\boldsymbol{M}_{\vec{\boldsymbol{y}}}$ *is potentially increasing.*

Obviously

$$\vec{\boldsymbol{y}} = \sum_{j=1}^{k} \alpha_j \cdot \vec{\boldsymbol{p}}_j + \sum_{j=1}^{k} \beta_j \cdot \vec{\boldsymbol{p}}_{k+j}$$

So

$$\boldsymbol{M}_{\vec{\boldsymbol{y}}} = \sum_{j=1}^{k} \alpha_j \cdot \boldsymbol{M}_{\vec{\boldsymbol{p}}_j} + \sum_{j=1}^{k} \beta_j \cdot \boldsymbol{M}_{\vec{\boldsymbol{p}}_{k+j}} \stackrel{\text{def}}{=} \boldsymbol{A} + \boldsymbol{B}$$

$$\boldsymbol{R}\boldsymbol{M}_{\vec{\boldsymbol{y}}}\boldsymbol{S} = \boldsymbol{R}\left(\boldsymbol{A} + \boldsymbol{B}\right)\boldsymbol{S} = \boldsymbol{R}\boldsymbol{A}\boldsymbol{S} + \boldsymbol{R}\boldsymbol{B}\boldsymbol{S} = \boldsymbol{A}\boldsymbol{S} + \boldsymbol{R}\boldsymbol{B}$$

Definition

Let $\vec{\boldsymbol{y}} \in \{-1,+1\}^{2^n}$. Then a vector $\vec{\boldsymbol{y}}$ is SYMMETRIC iff

$$(\forall i,j\in\{0,\ldots,2^n-1\})\left[\left(\sum_{k=1}^{n}\left(i^{bin}\right)_k = \sum_{k=1}^{n}\left(j^{bin}\right)_k \Rightarrow \vec{\boldsymbol{y}}_i = \vec{\boldsymbol{y}}_j\right]\right. .$$

- columns of $\boldsymbol{B}^{(n)}$
- majority function
- $$\vec{\boldsymbol{g}}_i^{(n)} \stackrel{\text{def}}{=} \begin{cases} -1 & \text{pro} \quad \sum_{l=1}^{n}(i^{bin})_l \equiv 4 \quad mod \quad 0,1 \\ 1 & \quad\quad\;\; \sum_{l=1}^{n}(i^{bin})_l \equiv 4 \quad mod \quad 2,3. \end{cases}$$

Theorem

Let $n \in N$ and a vector $\vec{\boldsymbol{y}} \in \{-1,+1\}^{2^n}$ is symmetric. Let $d_1, \ldots, d_m$ be lengths of successive constant blocks of the sequence

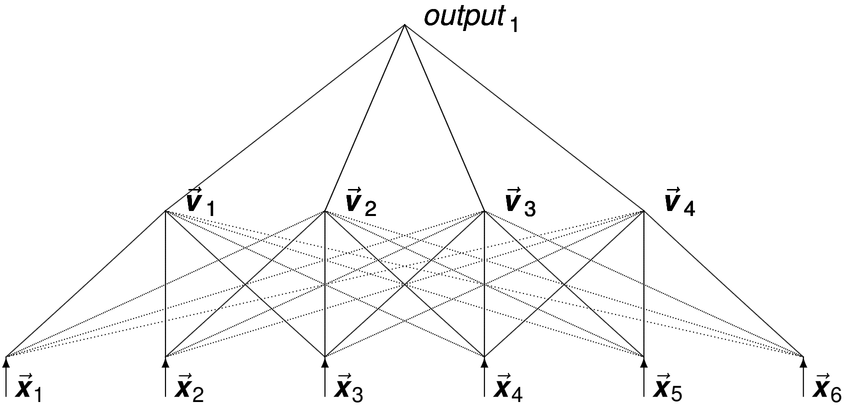
$$\vec{\boldsymbol{y}}_0, \vec{\boldsymbol{y}}_{2^1-1}, \vec{\boldsymbol{y}}_{2^2-1}, \ldots, \vec{\boldsymbol{y}}_{2^n-1}.$$

Further for each $k \in \{1,\ldots,m\}$ and $\vec{\boldsymbol{x}} \in \{-1,+1\}^n$ is

$$\widetilde{v_k}\left(\vec{\boldsymbol{x}}\right) \stackrel{def}{=} \widetilde{sgn}\left(\sum_{j=1}^{n} \vec{\boldsymbol{x}}_j + n - 2\sum_{j=1}^{k} d_j + \frac{1}{2}\right).$$

Then

$$-\vec{\boldsymbol{y}}_0\left(1 - \sum_{j=1}^{m} (-1)^j \left(\widetilde{v_j}\left(\vec{\boldsymbol{x}}\right) - 1\right)\right) = \vec{\boldsymbol{y}}_{\vec{\boldsymbol{x}}^{int}}.$$



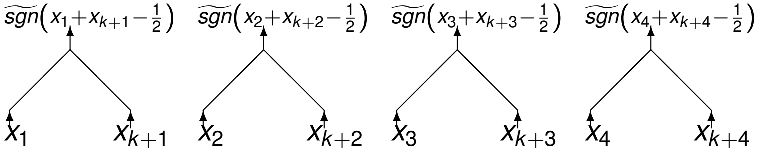
Theorem

$\mathbf{PT}_1 \subset \mathbf{LT}_3$ *and* $\mathbf{SYM}_2 \not\subset \mathbf{PT}_1$.

Theorem

Let $n = 2k$ and for $\vec{\boldsymbol{y}} \in \{-1, +1\}^n$ be $\boldsymbol{M}_{\vec{\boldsymbol{y}}} = \boldsymbol{B}^{(n)}$. Than $\vec{\boldsymbol{y}} \in \mathbf{LT}_3$ and $\vec{\boldsymbol{y}} \notin \mathbf{LT}_2$.

add $\vec{\boldsymbol{y}} \in \mathbf{LT}_3$:



$$\widetilde{sgn}\left(\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} + \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} - \frac{1}{2} \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} 1 \\ -1 \\ -1 \\ -1 \end{pmatrix}$$

now, let $\vec{\boldsymbol{y}} \in \mathbf{LT}_2$:
$\vec{\boldsymbol{y}}$ is threshold vector of
$\{\vec{\boldsymbol{p}}_1, \ldots, \vec{\boldsymbol{p}}_S\} \cup \{$threshold vectors of vectors $\vec{\boldsymbol{p}}_1, \ldots, \vec{\boldsymbol{p}}_S\}$. All whose conjugated matrices (say $\boldsymbol{M}$) are potentially increasing so for arbitrary $j \in \{1, \ldots, S\}$ the following inequality holds

$$\left\langle \boldsymbol{B}^{(k)} \middle| \boldsymbol{M} \right\rangle = \left\langle \boldsymbol{M}_{\vec{\boldsymbol{y}}} \middle| \boldsymbol{M} \right\rangle \leq (k+1) \cdot 2^k.$$

Therefore (remember $S \geq \frac{n}{\max_i \left| \left\langle \vec{\boldsymbol{y}} \middle| \vec{\boldsymbol{x}}_i \right\rangle \right|}$) it holds that

$$S \geq \frac{2^n}{(k+1)2^k} = \frac{2 \cdot 2^{\frac{n}{2}}}{n+2}.$$

Perceptron $\times$ XOR:

- inequalities
- geometry

- $\vec{\boldsymbol{y}} \perp \vec{\boldsymbol{x}}_1$ and $\vec{\boldsymbol{y}} \perp \vec{\boldsymbol{x}}_2$
- $\boldsymbol{M}_{\vec{\boldsymbol{y}}}$ contains $\begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\begin{pmatrix} -1 \\ 1 \\ 1 \\ -1 \end{pmatrix} = \widetilde{sgn}\left(\beta \begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix} + \gamma \begin{pmatrix} 1 \\ -1 \\ 1 \\ -1 \end{pmatrix}\right)$$

$$\left.\begin{array}{l} \beta + \gamma < 0 \\ \beta - \gamma > 0 \\ \beta + \gamma > 0 \\ \beta - \gamma < 0 \end{array}\right\} \rightarrow \left.\begin{array}{l} \beta + \gamma = 0 \\ \beta - \gamma = 0 \end{array}\right\} \rightarrow \begin{array}{l} \beta = 0 \\ \gamma = 0 \end{array}$$