CS 4124
More on the Lupanov Representation

September 16, 2005

1 Development of Lupanov Representation

Here we explain the development of the Lupanov representation for a Boolean function $f : \mathcal{B}^n \to \mathcal{B}$ using the example of Figure 2.22, where $n = 6$ and $k = 3$. The example is a Boolean function $f : \mathcal{B}^6 \to \mathcal{B}$. Since $k = 3$ and $n - k = 3$, we think of f as a function

$$f : \mathcal{B}^3 \times \mathcal{B}^3 \to \mathcal{B}.$$

We use the notation $\mathbf{a}$ for an element of $\mathcal{B}^k$ and $\mathbf{b}$ for an element of $\mathcal{B}^{n-k}$, so we can write $f(\mathbf{a}, \mathbf{b})$ for an evaluation of f. We take the elements of $\mathcal{B}^k$ to index the rows of a truth table and the elements of $\mathcal{B}^{n-k}$ to index its columns. Figure 1 contains the same truth table as in Figure 2.22.

				$\mathbf{b}_1$	$\mathbf{b}_2$	$\mathbf{b}_3$	$\mathbf{b}_4$	$\mathbf{b}_5$	$\mathbf{b}_6$	$\mathbf{b}_7$	$\mathbf{b}_8$	
				0	1	0	1	0	1	0	1	x_4
				0	0	1	1	0	0	1	1	x_5
$\mathbf{a}_{ij}$	x_1	x_2	x_3	0	0	0	0	1	1	1	1	x_6
$\mathbf{a}_{1,1}$	0	0	0	0	1	0	0	0	1	0	0	
$\mathbf{a}_{1,2}$	0	0	1	0	1	1	0	0	1	1	1	A_1
$\mathbf{a}_{1,3}$	0	1	0	1	0	0	1	0	0	0	1	
$\mathbf{a}_{2,1}$	0	1	1	1	0	1	1	0	0	1	0	
$\mathbf{a}_{2,2}$	1	0	0	0	0	0	0	1	0	0	1	A_2
$\mathbf{a}_{2,3}$	1	0	1	1	1	0	1	1	0	0	0	
$\mathbf{a}_{3,1}$	1	1	0	1	0	1	1	0	1	1	0	
$\mathbf{a}_{3,2}$	1	1	1	0	1	0	0	0	0	1	0	A_3
$\mathbf{a}_{3,3}$	1	1	1	0	1	0	0	0	0	1	0	

Figure 1: Truth table for $(3, 3)$-Lupanov representation.

As in the textbook, the row vectors (from $\mathcal{B}^k$) are partitioned into $p = 3$ sets A_1, A_2, and A_3. Each set has $s = 3$ row vectors, except for A_3, which contains only $s' = 2$ row vectors. For ease of exposition, an extra, duplicate, row has been added to A_3, so that it too has s rows.

We index the s row vectors in A_i to be $\mathbf{a}_{ij}$, where $1 \leq j \leq s$. In our example, we have these vectors in A_i: $\mathbf{a}_{i,1}$, $\mathbf{a}_{i,2}$, and $\mathbf{a}_{i,3}$. Similarly, we label the 2^{n-k} column vectors $\mathbf{b}_t$, where $1 \leq t \leq 2^{n-k}$. In our example, we label the columns $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_8$.

Fix i and hence A_i. Define

$$g_i : \mathcal{B}^{n-k} \to \mathcal{B}^s$$

to be

$$g_i(\mathbf{b}) \quad = \quad (f(\mathbf{a}_{i,1}, \mathbf{b}), f(\mathbf{a}_{i,2}, \mathbf{b}), \ldots, f(\mathbf{a}_{i,s}, \mathbf{b})),$$

$\mathbf{b}_t$	x_4	x_5	x_6	$g_1(\mathbf{b}_t)$			$g_2(\mathbf{b}_t)$			$g_3(\mathbf{b}_t)$		
$\mathbf{b}_1$	0	0	0	0	0	1	1	0	1	1	0	0
$\mathbf{b}_2$	1	0	0	1	1	0	0	0	1	0	1	1
$\mathbf{b}_3$	0	1	0	0	1	0	1	0	0	1	0	0
$\mathbf{b}_4$	1	1	0	0	0	1	1	0	1	1	0	0
$\mathbf{b}_5$	0	0	1	0	0	0	0	1	1	0	0	0
$\mathbf{b}_6$	1	1	0	1	1	0	0	0	0	1	0	0
$\mathbf{b}_7$	0	1	1	0	1	0	1	0	0	1	1	1
$\mathbf{b}_8$	1	1	1	0	1	1	0	1	0	0	0	0

Figure 2: Table of g_i values.

which is the s-vector of values in the column for $\mathbf{b}$ and the rows for A_i. Figure 2 gives all the g_i values for our example.

Now, for $1 \leq i \leq p$, define the *column function*

$$c_i : \mathcal{B}^s \times \mathcal{B}^{n-k} \to \mathcal{B}$$

to be

$$c_i(\mathbf{v}, \mathbf{b}) \quad = \quad \begin{cases} 1 & \text{if } g_i(\mathbf{b}) = \mathbf{v}; \\ 0 & \text{otherwise.} \end{cases}$$

Finally, for $1 \leq i \leq p$, define the *row function*

$$r_i : \mathcal{B}^s \times \mathcal{B}^k \to \mathcal{B}$$

to be

$$r_i(\mathbf{v}, \mathbf{a}) \quad = \quad \begin{cases} 1 & \text{if } \mathbf{a} = \mathbf{a}_{ij} \text{ and } \pi_j(\mathbf{v}) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

Now observe that, if $\mathbf{a} \in A_i$, $\mathbf{b} \in \mathcal{B}^{n-k}$ and $f(\mathbf{a}, \mathbf{b}) = 1$, then there exists $\mathbf{v} \in \mathcal{B}^s$ such that

$$\begin{aligned} r_i(\mathbf{v}, \mathbf{a}) \wedge c_i(\mathbf{v}, \mathbf{b}) &= 1 \\ &= f(\mathbf{a}, \mathbf{b}). \end{aligned}$$

Hence, we get the (k, s)-Lupanov representation of f:

$$f(\mathbf{a}, \mathbf{b}) \quad = \quad \vee_{i=1}^{p} \vee_{\mathbf{v} \in \mathcal{B}^s} (r_i(\mathbf{v}, \mathbf{a}) \wedge c_i(\mathbf{v}, \mathbf{b})).$$

For our example,

$$\begin{aligned}
f(\mathbf{a},\mathbf{b}) &= \vee_{i=1}^{3} \vee_{\mathbf{v}\in\{(0,0,0),(0,0,1),(0,1,0),(0,1,1),(1,0,0),(1,0,1),(1,1,0),(1,1,1)\}} (r_i(\mathbf{v},\mathbf{a}) \wedge c_i(\mathbf{v},\mathbf{b})) \\
&= (r_1((0,0,0),\mathbf{a}) \wedge c_1((0,0,0),\mathbf{b}) \vee r_1((0,0,1),\mathbf{a}) \wedge c_1((0,0,1),\mathbf{b}) \vee \\
&\quad r_1((0,1,0),\mathbf{a}) \wedge c_1((0,1,0),\mathbf{b}) \vee r_1((0,1,1),\mathbf{a}) \wedge c_1((0,1,1),\mathbf{b}) \vee \\
&\quad r_1((1,0,0),\mathbf{a}) \wedge c_1((1,0,0),\mathbf{b}) \vee r_1((1,0,1),\mathbf{a}) \wedge c_1((1,0,1),\mathbf{b}) \vee \\
&\quad r_1((1,1,0),\mathbf{a}) \wedge c_1((1,1,0),\mathbf{b}) \vee r_1((1,1,1),\mathbf{a}) \wedge c_1((1,1,1),\mathbf{b})) \vee \\
&\quad (r_2((0,0,0),\mathbf{a}) \wedge c_2((0,0,0),\mathbf{b}) \vee r_2((0,0,1),\mathbf{a}) \wedge c_2((0,0,1),\mathbf{b}) \vee \\
&\quad r_2((0,1,0),\mathbf{a}) \wedge c_2((0,1,0),\mathbf{b}) \vee r_2((0,1,1),\mathbf{a}) \wedge c_2((0,1,1),\mathbf{b}) \vee \\
&\quad r_2((1,0,0),\mathbf{a}) \wedge c_2((1,0,0),\mathbf{b}) \vee r_2((1,0,1),\mathbf{a}) \wedge c_2((1,0,1),\mathbf{b}) \vee \\
&\quad r_2((1,1,0),\mathbf{a}) \wedge c_2((1,1,0),\mathbf{b}) \vee r_2((1,1,1),\mathbf{a}) \wedge c_2((1,1,1),\mathbf{b})) \vee \\
&\quad (r_3((0,0,0),\mathbf{a}) \wedge c_3((0,0,0),\mathbf{b}) \vee r_3((0,0,1),\mathbf{a}) \wedge c_3((0,0,1),\mathbf{b}) \vee \\
&\quad r_3((0,1,0),\mathbf{a}) \wedge c_3((0,1,0),\mathbf{b}) \vee r_3((0,1,1),\mathbf{a}) \wedge c_3((0,1,1),\mathbf{b}) \vee \\
&\quad r_3((1,0,0),\mathbf{a}) \wedge c_3((1,0,0),\mathbf{b}) \vee r_3((1,0,1),\mathbf{a}) \wedge c_3((1,0,1),\mathbf{b}) \vee \\
&\quad r_3((1,1,0),\mathbf{a}) \wedge c_3((1,1,0),\mathbf{b}) \vee r_3((1,1,1),\mathbf{a}) \wedge c_3((1,1,1),\mathbf{b}))
\end{aligned}$$

2 A Circuit for the Lupanov Representation

A circuit for the Lupanov representation of f is built by decoding $\mathbf{a}$ and $\mathbf{b}$; computing $r_i(\mathbf{v},\mathbf{a})$ and $c_i(\mathbf{v},\mathbf{b})$ for fixed i and $\mathbf{v}$; and combining the results with AND and OR gates.

2.1 Decoders for a and b

Apply Lemma 2.5.4 to obtain a decoder circuit for $\mathbf{a} \in \mathcal{B}^k$ with complexity

$$\begin{aligned}
C_{\Omega_0}\left(f^{(k)}_{\text{decode}}\right) &\leq 2^k + (2k-2)2^{k/2} \\
&\leq 2^k + k2^{1+k/2} \\
D_{\Omega_0}\left(f^{(k)}_{\text{decode}}\right) &\leq \lceil \log_2 k \rceil + 1 \\
&\leq 2 + \log_2 k
\end{aligned}$$

and a decoder circuit for $\mathbf{b} \in \mathcal{B}^{n-k}$ with complexity

$$\begin{aligned}
C_{\Omega_0}\left(f^{(n-k)}_{\text{decode}}\right) &\leq 2^{n-k} + (2(n-k)-2)2^{(n-k)/2} \\
&\leq 2^{n-k} + n2^{1+((n-k)/2)} \\
D_{\Omega_0}\left(f^{(n-k)}_{\text{decode}}\right) &\leq \lceil \log_2 n - k \rceil + 1 \\
&\leq 2 + \log_2 n.
\end{aligned}$$

2.2 Circuit to compute the $r_i(\mathbf{v},\mathbf{a})$ functions

There are p row functions r_i. Fix i, where $1 \leq i \leq p$, and $\mathbf{v} \in \mathcal{B}^s$. If $\mathbf{a} \notin A_i$, then $r_i(\mathbf{v},\mathbf{a}) = 0$. Hence, $r_i(\mathbf{v},\mathbf{a}) = 1$ for at most s values of $\mathbf{a}$, so $r_i(\mathbf{v},\mathbf{a})$ is the OR of at most s of the outputs

from the **a** decoder. This requires $\leq s$ additional gates and additional depth $\leq \lceil \log_2 s \rceil + 1 \leq 2 + \log_2 s$. Computing all of the $r_i(\mathbf{v}, \mathbf{a})$ functions requires $\leq p2^s s$ additional gates, and additional depth $\leq 2 + \log_2 s$, since the functions can all be computed in parallel.

2.3 Circuit to compute the $c_i(\mathbf{v}, \mathbf{b})$ functions

There are p column functions c_i. Fix i, where $1 \leq i \leq p$, and $\mathbf{v} \in \mathcal{B}^s$. We have that $c_i(\mathbf{v}, \mathbf{b}) = 1$ exactly when $g_i(\mathbf{b}) = \mathbf{v}$. Hence, every $\mathbf{b} \in \mathcal{B}^{n-k}$ contributes a single 1 to the output of each of the c_i functions. Define $d_{i\mathbf{v}} : \mathcal{B}^s \to \mathcal{B}$ to be

$$d_{i\mathbf{v}} \quad = \quad c_i(\mathbf{v}, \mathbf{b}).$$

Taking the outputs of the **b** decoder, we can compute all of the $d_{i\mathbf{v}}$ functions, for fixed i and all $\mathbf{v} \in \mathcal{B}^s$, with $\leq 2^{n-k}$ additional OR gates and additional depth $\leq \lceil \log_2(n-k) \rceil + 1 \leq 2 + \log_2 n$. To compute all of the $d_{i\mathbf{v}}(\mathbf{b})$ functions requires $\leq p2^{n-k}$ additional gates, and additional depth $\leq 2 + \log_2 n$, since the functions can all be computed in parallel. Observe also that the computation of the r_i and the c_i occur in parallel.

2.4 Circuit to compute the Lupanov formula

Once the $r_i(\mathbf{v}, \mathbf{a})$ and $c_i(\mathbf{v}, \mathbf{a})$ values are computed, the Lupanov representation of f requires $\leq p2^s$ additional AND gates, all in parallel with additional depth 1; and $\leq p2^s$ additional OR gates with additional depth $\leq \lceil \log_2 p2^s \rceil + 1 \leq 2 + s + \log_2 p$. Combining the sizes, we need $\leq p2^{s+1}$ additional gates. Combining the depths, we need $\leq 3 + s + \log_2 p$ additional circuit depth.

2.5 Circuit complexity

The size of the constructed circuit is at most

$$\psi(n, k, p, s) \quad = \quad (2^k + k2^{1+k/2}) + (2^{n-k} + n2^{1+(n-k)/2}) + p2^s s + p2^{n-k} + p2^{s+1}.$$

The depth of the constructed circuit is at most

$$\begin{aligned} \delta(n, k, p, s) &= \max\{(2 + \log_2 k) + (2 + \log_2 s), (2 + \log_2 n) + (2 + \log_2 n)\} + 3 + s + \log_2 p \\ &= 4 + 2\log_2 n + 3 + s + \log_2 p \\ &= 7 + s + 2\log_2 n + \log_2 p. \end{aligned}$$

3 Upper Bounds on Circuit Complexity

As in the textbook, choose these values for k, p, and s:

$$\begin{aligned} k &= \lceil 3\log_2 n \rceil \\ p &= \left\lceil \frac{2^k}{\lceil n - 5\log_2 n \rceil} \right\rceil \\ s &= \lceil n - 5\log_2 n \rceil. \end{aligned}$$

Here are some relationships that hold for all sufficiently large n:

$$\begin{aligned}
k &\leq 1 + 3\log_2 n \\
2^k &\leq 2n^3 \\
2^k &\geq n^3 \\
s &\leq 1 + (n - 5\log_2 n) \\
2^s &\leq \frac{2^{n+1}}{n^5} \\
p &\leq \frac{2n^3}{1 + n - 5\log_2 n} \\
ps &\leq 2^{k+1} \\
&\leq 4n^3 \\
\log_2 p &\leq 1 + 2\log_2 n.
\end{aligned}$$

For the size complexity of the constructed circuit, we obtain

$$\begin{aligned}
\psi(n,k,p,s) &= (2^k + k2^{1+k/2}) + (2^{n-k} + n2^{1+(n-k)/2}) + p2^s s + p2^{n-k} + p2^{s+1} \\
&\leq \left(2n^3 + 2(1 + 3\log_2 n)n^{3/2}\right) + \left(\frac{2^n}{n^3} + \frac{n2^{1+n/2}}{n^{3/2}}\right) \\
&\quad + \frac{4n^3 2^{n+1}}{n^5} + \frac{2n^3 2^n}{n^3(1 + n - 5\log_2 n)} + \frac{2n^3 2^{n+2}}{n^5(1 + n - 5\log_2 n)} \\
&\leq O(n^3) + O(n^{3/2}\log_2 n) + \frac{2^n}{n^3} + O\left(\frac{2^{n/2}}{n^{1/2}}\right) \\
&\quad + O\left(\frac{2^n}{n^2}\right) + \frac{2^{n+1}}{1 + n - 5\log_2 n} + \frac{2^{n+3}}{n^2(1 + n - 5\log_2 n)} \\
&\leq \frac{2^{n+1}}{1 + n - 5\log_2 n} + O\left(\frac{2^n}{n^2}\right),
\end{aligned}$$

where, as usual, $O(f(n))$ indicates a function of n that grows no faster than $f(n)$ as $n \to \infty$ (see Section 1.2.8).

For the depth complexity of the constructed circuit, we obtain

$$\begin{aligned}
\delta(n,k,p,s) &= 7 + s + 2\log_2 n + \log_2 p \\
&\leq 7 + (1 + n - 5\log_2 n) + 2\log_2 n + (1 + 2\log_2 n) \\
&= n + 9 - \log_2 n \\
&\leq n + O(\log_2 n).
\end{aligned}$$