Theory Comput. Systems **37**, 519–525 (2004)
DOI: 10.1007/s00224-003-1069-7

Theory of Computing Systems

Quadratic Sequential Computations of Boolean Mappings

Serge Burckel and Marianne Morillon

Laboratoire ERMIT, Université de la Réunion,
15 av. René Cassin, BP 7151,
97715 Saint-Denis messag. cedex 9, France
{burckel, mar}@univ-reunion.fr

Abstract. This paper proposes a constructive proof that any mapping on n boolean variables can be computed by a straight-line program made up of n^2 assignments of the n input variables.

1. Introduction

Let n be a positive integer. Denote by $\mathbf{B}_n$ the set $\{0, 1\}^n$. Given a boolean mapping $E\colon \mathbf{B}_n \to \mathbf{B}_n$ we are interested in a sequential computation of $(x_0, \ldots, x_{n-1}) := E(x_0, \ldots, x_{n-1})$. For instance, consider the mapping E on $\mathbf{B}_2$ that maps (a, b) to (b, a). This mapping is linear and bijective. An usual way to compute E in a program is to use a new storage variable c and compute $c := a$; $a := b$; $b := c$. However, it is known that c is not necessary and E is also computed with the program $a := a \oplus b$; $b := a \oplus b$; $a := a \oplus b$. We generalize this kind of computation in the following.

Definition (Sequential Computation). Let n, k be positive integers. For a given mapping $E\colon \mathbf{B}_n \to \mathbf{B}_n$ and a sequence $(f_0, \ldots, f_{kn-1})$ of mappings $f_i\colon \mathbf{B}_n \to \mathbf{B}_1$, the procedure on boolean variables $(x_0, \ldots, x_{n-1})$,

$$\texttt{for}\, j := 0 \,\texttt{to}\, k-1 \,\texttt{do}\, \texttt{for}\, i := 0 \,\texttt{to}\, n-1 \,\texttt{do}\, x_i := f_{jn+i}(x_0, \ldots, x_{n-1}),$$

is a *Sequential Computation* of E if it transforms any vector $(x_0, \ldots, x_{n-1})$ of $\mathbf{B}_n$ into its image by E. Moreover, this computation is *quadratic* when $k = n$.

The existence of finite sequential computations is proved in [1] and the existence of quadratic ones was conjectured. In this paper we prove this fact.

Theorem 1. *For every positive integer n, every mapping $E\colon \mathbf{B}_n \to \mathbf{B}_n$ admits a quadratic sequential computation.*

We prove this result with a representation of the problem in terms of boolean matrices.

Definition (Matrices). Let n, k be two positive integers. A boolean matrix M of columns $[C_0, \ldots, C_k]$ is *n-functional* if for any $n < i \leq k$ column C_i is functional according to the n previous ones: if two rows of M coincide on columns $[C_{i-n}, \ldots, C_{i-1}]$, then they must also be equal on C_i. (Observe that any n-functional boolean matrix is also $(n+1)$-functional.) An *n-table* is a boolean matrix with 2^n rows. For two n-tables $U = [C_0, \ldots, C_k]$ and $V = [D_0, \ldots, D_h]$, the n-table $U * V$ is $[C_0, \ldots, C_k, D_0, \ldots, D_h]$. For an $(n+1)$-table M, denote by $\lceil M \rceil$ and $\lfloor M \rfloor$ the n-tables made up of respectively the upper and lower half of M. We also write $M = \lceil M \rceil / \lfloor M \rfloor$. Denote by $\mathbf{V}_n$ the n-table made up of all the vectors of $\mathbf{B}_n$ in the lexicographical order. Denote by Π_n^0 the column made up of 2^n zeros, by Π_n^1 the column made up of 2^n ones, and by Π_{n+1}^{01} the column Π_n^0 / Π_n^1. A column Δ is *balanced* if $\lceil \Delta \rceil$ and $\lfloor \Delta \rfloor$ both contain as many zeros as ones.

For instance, we have

$$\Pi_{n+1}^0 = \Pi_n^0 / \Pi_n^0, \ \Pi_{n+1}^1 = \Pi_n^1 / \Pi_n^1,$$
$$\Pi_n^{01} / \Pi_n^{01} \text{ is balanced but } \Pi_n^{01} \text{ is not balanced,}$$
$$\mathbf{V}_{n+1} = (\Pi_n^0 * \mathbf{V}_n) / (\Pi_n^1 * \mathbf{V}_n) = \Pi_{n+1}^{01} * (\mathbf{V}_n / \mathbf{V}_n).$$

Lemma 2 (Surgeries). *Let n be a positive integer.*

(*replacement*) *The replacement of a row by another row and the permutation of rows both preserve the n-functionality of a boolean matrix.*

(*induction*) *For $i \in \mathbf{B}_1$, let M_i be an n-functional n-table and let P_i be the n-table obtained by inserting a column Π_n^i before the first column and every n columns in M_i. The n-tables P_0, P_1 and the $(n+1)$-table P_0 / P_1 are $(n+1)$-functional.*

(*matching*) *For any n-table V with n columns and any n-functional n-tables $U * V$ and $V * W$, the n-table $U * V * W$ is also n-functional.*

Proof. (*replacement*) Obvious. (*induction*) Each inserted column in P_0 is constant, that is, functional according to its $n+1$ previous columns. Any other column of P_0 is, by hypothesis, functional according to its n previous columns in M_0 that necessarily appear now in the $n+1$ previous ones in P_0. Hence P_0 is $(n+1)$-functional. The same argument holds for P_1. In $P = P_0 / P_1$, the inserted columns Π_n^0 in P_0 and Π_n^1 in P_1 distinguish the blocks of $(n+1)$ consecutive columns and P is also $(n+1)$-functional. (*Matching*) In $U * V * W$, the n-functionality comes from $U * V$ in the first columns and from $V * W$ in the remaining ones. □

2. Construction

Let $E\colon \mathbf{B}_n \to \mathbf{B}_n$ with $n \geq 1$. According to [1], the mapping E admits a quadratic sequential computation if and only if there exists an n-functional n-table T made of $n+n^2$ columns that begins with $\mathbf{V}_n$, the vectors of $\mathbf{B}_n$, and ends with the n-table $[E_0, \ldots, E_{n-1}]$ that represents the respective images by E of those vectors. We construct T by induction on n. For $n = 1$, it is obvious since the boolean matrix

$$T = \begin{bmatrix} 0 & E(0) \\ 1 & E(1) \end{bmatrix}$$

is a trivial solution to the problem. We explain the key ideas for the inductive step by showing how to compute a solution for $n = 3$ using the case $n = 2$.

Assume we have found a 3-table $[E'_0, E'_1, E'_2]$ such that $E'_0 = \Pi_3^{01}$ and the 3-table $[E'_0, E'_1, E'_2, E_0, E_1, E_2]$ is 3-functional. Then we can use the case $n = 2$ twice in order to complete the following 3-table T such that $\lceil T \rceil$ and $\lfloor T \rfloor$ both become 3-functional:

$$T = \left[\begin{array}{cccccc|c|cccc}
 & \text{case} & n{=}2 & & \text{case} & n{=}2 & E'_0 = \Pi_3^{01} & E'_1 & E'_2 & E_0 & E_1 & E_2 \\
\mathbf{0} & 0 & 0 & \mathbf{0} & - & - & \mathbf{0} & * & * & a_0 & a_1 & a_2 \\
\mathbf{0} & 0 & 1 & \mathbf{0} & - & - & \mathbf{0} & * & * & b_0 & b_1 & b_2 \\
\mathbf{0} & 1 & 0 & \mathbf{0} & - & - & \mathbf{0} & * & * & c_0 & c_1 & c_2 \\
\mathbf{0} & 1 & 1 & \mathbf{0} & - & - & \mathbf{0} & * & * & d_0 & d_1 & d_2 \\
 & \text{case} & n{=}2 & & \text{case} & n{=}2 & & & & & & \\
\mathbf{1} & 0 & 0 & \mathbf{1} & - & - & \mathbf{1} & * & * & e_0 & e_1 & e_2 \\
\mathbf{1} & 0 & 1 & \mathbf{1} & - & - & \mathbf{1} & * & * & f_0 & f_1 & f_2 \\
\mathbf{1} & 1 & 0 & \mathbf{1} & - & - & \mathbf{1} & * & * & g_0 & g_1 & g_2 \\
\mathbf{1} & 1 & 1 & \mathbf{1} & - & - & \mathbf{1} & * & * & h_0 & h_1 & h_2
\end{array}\right]$$

From (induction) and (matching), the table T is 3-functional.

Hence, the main difficult step is to find for any n-table $[E_0, \ldots, E_{n-1}]$ an n-functional n-table $[E'_0, \ldots, E'_{n-1}, E_0, \ldots, E_{n-1}]$ such that $E'_0 = \Pi_n^{01}$. This fact will be proved by induction and deduced from the existence of a balanced column Δ that makes the n-table $[\Delta, E_0, \ldots, E_{n-1}]$ n-functional. However this condition is too strong in general: for instance, when all the rows of $[E_0, \ldots, E_{n-1}]$ are 0^n except for the first one, that is $0^{n-1}1$, then $\lfloor \Delta \rfloor$ must be constant. On the other hand, it is not very difficult to construct such a *balanced* column Δ when all the rows of $[E_0, \ldots, E_{n-1}]$ are different and represent a bijection on $\mathbf{B}_n$: for all the rows mx with $m \in \mathbf{B}_{n-1}$ and $x \in \mathbf{B}_1$ such that $m\bar{x}$ appears in the same half of the boolean matrix, complete them by xmx and $\bar{x}m\bar{x}$. Now, the number of rows mx in the upper half such that $m\bar{x}$ appears in the lower half is necessarily even (for $n \geq 2$). For half of them complete by $0mx$ and $1m\bar{x}$ and complete the others by $1mx$ and $0m\bar{x}$. We are done. However, in order to complete the proof, we need to find a similar construction of a balanced column Δ for a larger class that we define here.

Definition (Semi-bijection). For $n \geq 2$, an n-table $S = [S_0, \ldots, S_{n-1}]$ is *semi-bijective* if any vector of $\mathbf{B}_n$ occurs at most once in each half of S. This implies that there are nine

possible *types* for the occurrences of rows mx and $m\bar{x}$ in S with $m \in \mathbf{B}_{n-1}$ and $x \in \mathbf{B}_1$:

mx	mx		mx					
$m\bar{x}$	$m\bar{x}$		$m\bar{x}$	mx	mx	mx	mx	
mx		mx	mx	mx	$m\bar{x}$	mx		mx
$m\bar{x}$		$m\bar{x}$				$m\bar{x}$		
0	1	2	3	4	5	6	7	8

In the above representation, the horizontal line separates the halves of S and we indicate in which halves the rows mx and $m\bar{x}$ appear.

Lemma 3. *For every $n \geq 2$ and every semi-bijective n-table S, there exists a balanced column Δ such that $\Delta * S$ is n-functional.*

Proof. For every type $t \in \{0, 1, \ldots, 8\}$ let λ_t be the number of times this type t occurs in S. For each occurrence of type t, we propose some possible completion rules R_t^i in order to define Δ such that the boolean matrix $\Delta * S$ is n-functional. The values of Δ appear in the first column.

$0mx$	$0mx$		$0mx$	$1mx$			
$1m\bar{x}$	$1m\bar{x}$		$1m\bar{x}$	$0m\bar{x}$	$1mx$	$0mx$	
$0mx$		$0mx$	$0mx$	$1mx$	$0mx$	$1mx$	
$1m\bar{x}$		$1m\bar{x}$					
R_0^1	R_1^1	R_2^1	R_3^1	R_3^2	R_4^1	R_4^2	
$1mx$	$0mx$	$1mx$	$0mx$	$1mx$	$0mx$		
$0m\bar{x}$	$1m\bar{x}$	$1mx$	$0mx$			$0mx$	$1mx$
		$0m\bar{x}$	$1m\bar{x}$				
R_5^1	R_5^2	R_6^1	R_6^2	R_7^1	R_7^2	R_8^1	R_8^2

It remains to choose the rules that make Δ balanced. Let a_t^i be the number of times the rule R_t^i is used in the construction of Δ. For any $x \in \mathbf{B}_1$, denote by σ^x the number of x's in $\lceil \Delta \rceil$ and by σ_x the number of x's in $\lfloor \Delta \rfloor$. Considering the way the rules R_t^i affect $\sigma^0, \sigma^1, \sigma_0, \sigma_1$, we obtain

$$\begin{aligned}
\sigma^0 &= \lambda_0 + \lambda_1 + \lambda_3 + a_4^2 + a_5^2 + a_6^2 + a_7^2,\\
\sigma_0 &= \lambda_0 + \lambda_2 + \lambda_6 + a_3^1 + a_4^1 + a_5^1 + a_8^1,\\
\sigma^1 &= \lambda_0 + \lambda_1 + \lambda_3 + a_4^1 + a_5^1 + a_6^1 + a_7^1,\\
\sigma_1 &= \lambda_0 + \lambda_2 + \lambda_6 + a_3^2 + a_4^2 + a_5^2 + a_8^2.
\end{aligned}$$

If Δ is balanced, then $\sigma^0 = \sigma^1$ and $\sigma_0 = \sigma_1$ must hold, that is to say $a_4^2 + a_5^2 + a_6^2 + a_7^2 = a_4^1 + a_5^1 + a_6^1 + a_7^1$ and $a_3^1 + a_4^1 + a_5^1 + a_8^1 = a_3^2 + a_4^2 + a_5^2 + a_8^2$. Since $n \geq 2$ and

$$\sigma^0 + \sigma^1 = 2\lambda_0 + 2\lambda_1 + 2\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 = 2^{n-1},$$

$$\sigma_0 + \sigma_1 = 2\lambda_0 + 2\lambda_2 + 2\lambda_6 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_8 = 2^{n-1},$$

the positive integers $\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7$ and $\lambda_3 + \lambda_4 + \lambda_5 + \lambda_8$ are even. For every $t \in \{3, \ldots, 8\}$, let π_t be the remainder of λ_t modulo 2. There are 16 possible parity cases and for each one we define convenient integers a_t^i with the following:

Case	π_3	π_4	π_5	π_6	π_7	π_8	δ_3	δ_4	δ_5	δ_6	δ_7	δ_8
1	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	1	1	0	0	0	0	+1	−1	0
3	0	0	1	0	1	1	0	0	+1	0	−1	−1
4	0	0	1	1	0	1	0	0	−1	+1	0	+1
5	0	1	0	0	1	1	0	−1	0	0	+1	+1
6	0	1	0	1	0	1	0	−1	0	+1	0	+1
7	0	1	1	0	0	0	0	−1	+1	0	0	0
8	0	1	1	1	1	0	0	−1	+1	+1	−1	0
9	1	0	0	0	0	1	+1	0	0	0	0	−1
10	1	0	0	1	1	1	+1	0	0	+1	−1	−1
11	1	0	1	0	1	0	+1	0	−1	0	+1	0
12	1	0	1	1	0	0	+1	0	−1	+1	0	0
13	1	1	0	0	1	0	+1	−1	0	0	+1	0
14	1	1	0	1	0	0	+1	−1	0	+1	0	0
15	1	1	1	0	0	1	+1	−1	+1	0	0	−1
16	1	1	1	1	1	1	+1	−1	−1	+1	+1	+1

Define for every, $t \in \{3, \ldots, 8\}$,

$$a_t^1 = (\lambda_t - \delta_t)/2,$$
$$a_t^2 = (\lambda_t + \delta_t)/2.$$

In all 16 cases the previous table shows that a_t^1 and a_t^2 are non-negative integers such that $a_t^1 + a_t^2 = \lambda_t$ and $\delta_4 + \delta_5 + \delta_6 + \delta_7 = 0$ and $\delta_3 + \delta_4 + \delta_5 + \delta_8 = 0$ hold. Observe that such a definition of the δ_t's is not unique. This one satisfies $\delta_3 = \pi_3$, $\delta_4 = -\pi_4$, $\delta_6 = \pi_6$. We obtain the relations

$$a_4^2 + a_5^2 + a_6^2 + a_7^2 = a_4^1 + a_5^1 + a_6^1 + a_7^1 = (\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7)/2,$$
$$a_3^1 + a_4^1 + a_5^1 + a_8^1 = a_3^2 + a_4^2 + a_5^2 + a_8^2 = (\lambda_3 + \lambda_4 + \lambda_5 + \lambda_8)/2,$$

that imply that Δ is balanced. □

An anonymous referee proposed this alternative and simpler argument.

Proof. Consider an undirected graph G whose nodes are the rows of the n-table S and whose edges are $(mx, m\bar{x})$; that is, two nodes are adjacent if they differ only in the last bit. By semi-bijectivity, every node is adjacent to at most one other node in its own half of the table and at most one node in the other half. The induced subgraph on the nodes in the upper half form a matching, and there are an even number of nodes, so it can be completed to a perfect matching, and similarly for the nodes in the lower half. Let G' be this extended graph. In G' every node is adjacent to exactly one other node in its own

half of the table and at most one node in the other half. There are no odd cycles in G' because along any path, the edges must alternate between edges connecting nodes in the same half and edges connecting nodes in different halves. Since there are no odd cycles, the graph is 2-colorable, and any 2-coloring gives a balanced Δ. □

Now we can perform the main step for the induction.

Lemma 4. *For every integer $n \geq 1$ and every n-table $[E_0, \ldots, E_{n-1}]$, there exists an n-functional n-table $[E'_0, \ldots, E'_{n-1}, E_0, \ldots, E_{n-1}]$ such that $E'_0 = \Pi_n^{01}$.*

Proof. We proceed by induction on n. For $n = 1$, it is obvious. Assume that $n \geq 2$. First, we transform the table $[E_0, \ldots, E_{n-1}]$ into a semi-bijective one with the following procedure. While there exists a row that appears twice in some half of the table, replace it by another row that appears nowhere. At the end of this process, we obtain a semi-bijective n-table $[S_0, \ldots, S_{n-1}]$. Lemma 3 gives a balanced column Δ such that $M = [\Delta, S_0, \ldots, S_{n-1}]$ is n-functional. Let $M_0 = [\Pi_{n-1}^0, s_0, \ldots, s_{n-1}]$ be the sequence of the rows of M that begin with $\Delta = 0$ and let $M_1 = [\Pi_{n-1}^1, t_0, \ldots, t_{n-1}]$ be the sequence of the rows of M that begin with $\Delta = 1$. Observe that since Δ is balanced, $\lceil M_0 \rceil$ and $\lceil M_1 \rceil$ both come from $\lceil M \rceil$ and $\lfloor M_0 \rfloor$ and $\lfloor M_1 \rfloor$ both come from $\lfloor M \rfloor$. By the induction hypothesis, there exist two $(n-1)$-functional $(n-1)$-tables $[s'_0, \ldots, s'_{n-2}, s_0, \ldots, s_{n-2}]$ and $[t'_0, \ldots, t'_{n-2}, t_0, \ldots, t_{n-2}]$ such that $s'_0 = t'_0 = \Pi_{n-1}^{01}$. From (induction) and (matching), the n-table

$$[s'_0, \ldots, s'_{n-2}, \Pi_{n-1}^0, s_0, \ldots, s_{n-2}, s_{n-1}]/[t'_0, \ldots, t'_{n-2}, \Pi_{n-1}^1, t_0, \ldots, t_{n-2}, t_{n-1}]$$

is n-functional. Permute the rows of this n-table in order to have $[S_0, \ldots, S_{n-1}]$ as the last columns and Π_n^{01} as the first one. Duplicate in each half of this new n-table some rows in order to have $[E_0, \ldots, E_{n-1}]$ as the last columns. We obtain an n-table that still begins with column Π_n^{01} and is still n-functional (replacement). We are done. □

Proof of Theorem 1. We proceed by induction on n. The case $n = 1$ is obvious: any mapping $E\colon \mathbf{B}_1 \to \mathbf{B}_1$ admits a quadratic sequential computation of length 1: $x_0 := E(x_0)$. Assume $n > 1$ and consider a mapping $E\colon \mathbf{B}_n \to \mathbf{B}_n$. Using Lemma 4, let $T = [E'_0, E'_1, \ldots, E'_{n-1}, E_0, \ldots, E_{n-1}]$ be an n-functional n-table such that $E'_0 = \Pi_n^{01}$. We have $\lceil T \rceil = [\Pi_{n-1}^0, e'_1, \ldots, e'_{n-1}, e_0, \ldots, e_{n-1}]$ and $\lfloor T \rfloor = [\Pi_{n-1}^1, f'_1, \ldots, f'_{n-1}, f_0, \ldots, f_{n-1}]$. Using the induction hypothesis, there exists two $(n-1)$-functional $(n-1)$-tables U_0 and U_1 made up of $(n-1) + (n-1)^2$ columns that both begin with $\mathbf{V}_{n-1}$ and respectively end with $[e'_1, \ldots, e'_{n-1}]$ and $[f'_1, \ldots, f'_{n-1}]$. Insert column Π_n^{01} as the first column and each n columns in U_0/U_1. We obtain (induction) an n-functional table U made up of n^2 columns that begins with $\Pi_n^{01} * (\mathbf{V}_{n-1}/\mathbf{V}_{n-1}) = \mathbf{V}_n$ and ends with $\Pi_n^{01} * ([e'_1, \ldots, e'_{n-1}]/[f'_1, \ldots, f'_{n-1}]) = [E'_0, \ldots, E'_{n-1}]$. Since T is n-functional, the table $U * [E_0, \ldots, E_{n-1}]$ is n-functional (matching) and gives a quadratic sequential computation of E. □

3. Conclusion

First, in the quadratic sequential computations that we have built in this paper, any mapping $f_i\colon \mathbf{B}_n \to \mathbf{B}_1$ can be used in the program. On the other hand, following an idea of Piccard in [3], the existence of sequential computations that only use three types of functions has been proved in [2]. However, such restricted computations cannot be quadratic and not even of polynomial length: an obvious enumeration of the tables shows that the number of possible sequential computations of length $q(n)$ using $p(n)$ functions is bounded by $p(n)^{q(n)}$. That is not enough to obtain the number 2^{n2^n} of possible mappings $E\colon \mathbf{B}_n \to \mathbf{B}_n$ when p and q are both polynomial functions and n is large enough.

Second, it is interesting to point out that the construction of the proof implies that almost half of the performed assignments have the trivial form $x_i := x_i$.

Moreover, some experiments on computers suggest that the bound n^2 could be improved to $2n$ for bijective mappings and to $3n$ for arbitrary mappings.

Acknowledgment

The authors thank an anonymous referee for the alternative proof of Lemma 3 and for many other comments that improved this paper.

References

[1] S. Burckel, Closed iterative calculus; *Theoretical Computer Science*, **158** (1996), 371–378.

[2] S. Burckel and M. Morillon, Three generators for minimal writing-space computations, *Theoretical Informatics and Applications*, **34** (2000), 131–138.

[3] S. Piccard, Sur les fonctions définies dans les ensembles finis quelconques, *Fundamenta Mathematicae*, **24** (1935), 298–301.

Received January 31, 2002, *and in final form June* 20, 2003. *Online publication May* 3, 2004.