Quadratic Sequential Computations.

Abstract. This paper proposes a constructive proof that any boolean mapping on $n$ variables can be computed via a sequential program made of exactly $n^2$ assignments of the $n$ input variables.

1. Introduction.

Let $n$ be a positive integer. Denote $B_n$ the set $\{0, 1\}^n$. Given a boolean function $E : B_n \rightarrow B_n$ and a vector $x = (x_0, \ldots, x_{n-1})$ of $B_n$, a sequential computation of the vector $E(x)$ is generally performed in the following way: one first copies the data $x_0, \ldots, x_{n-1}$ in some safe memory, then, one successively computes the new value for $x_0, x_1, \ldots$ referring to the safe copy. During this kind of computation, the initial vector $x$ is modified, hence one has to refer to the safe copy in order to use the right data. Nevertheless, there are well known boolean functions that can be computed without copying the data. For example the exchange function $E : B_2 \rightarrow B_2$ defined by $E(x_0, x_1) = (x_1, x_0)$ can be computed using just those two variables and the boolean sum $+$ on $B_1$ ($0 + 0 = 1 + 1 = 0$ and $0 + 1 = 1 + 0 = 1$): the following four successive assignments perform the exchange of $x_0$ and $x_1$: $x_0 := x_0 + x_1; x_1 := x_0 + x_1; x_0 := x_0 + x_1; x_1 := x_1$. This computation is built out of two successive blocks of assignments for each of the two variables. More generally, it has been proved (see [1]) that every boolean function can be computed without copying the data; but the method given in [1] leads to a number of assignments which is exponential in the number of variables. Meanwhile, it was conjectured in [1] that every boolean function with $n$ variables can be computed with no more than $n^2$ assignments of those variables only. In this paper, we prove this conjecture. More precisely, for every boolean function $E$ with $n$ variables, we provide a way to compute $E$, in $n$ blocks of $n$ successive assignments of the variables such that the first $n - i$ assignments in the $i$-th block are identities: $x_0 := x_0, \ldots, x_{n-i-1} := x_{n-i-1}$. Hence, during the computation, there will be at least $(n-1) + \ldots + 1 = n(n-1)/2$ identities.

The paper is organized as follows: we first give definitions (Section 2), then expose the idea of the proof (Section 3), and finally we prove our result (Sections 4 and 5). At the end of the paper (Section 6), we apply our algorithm to a particular boolean function from $B_3$ to $B_3$. 

1
2. Definitions and notations.

**Notation.** For every integers \( k, n \) such that \( 0 \leq k < n \), denote by \( p^n_k \) the \((n, 1)\)-map such that for every \( (x_0, \ldots, x_{n-1}) \in \mathcal{B}_n \), \( p^n_k(x_0, \ldots, x_k, \ldots, x_{n-1}) = x_k \); for every \((m, n)\)-map \( E \), denote by \( E_k \) the \( k \)-th component \( p^m_k \circ E \).

**Definition. (sequential computation).** Let \( n, k \) be positive integers. For any positive integer \( i \), denote by \( i[n] \) the remainder of \( i \) modulo \( n \). A \((n, k)\)-map is a mapping from \( \mathcal{B}_n \) to \( \mathcal{B}_k \). Let \( E \) be an \((n, n)\)-map. We say that a sequence \((f_0, \ldots, f_{k-1})\) of \((n, 1)\)-maps *computes* \( E \) if the following program with variables \((x_0, \ldots, x_{n-1})\) initialized to some \( m \in \mathcal{B}_n \):

\[
\text{for } i = 0 \text{ to } k-1 \text{ do } x_{i[n]} := f_i(x_{i[n]}, x_{(i+1)[n]}, \ldots, x_{(i+n-1)[n]})
\]

ends with \((x_0, \ldots, x_{n-1}) = E(m)\).

This program is a *sequential computation* of \( E \) of length \( k \) and is *quadratic* when \( k = n^2 \).

In [1], it is proved that every \((n, n)\)-map has a sequential computation and it was conjectured the existence of a quadratic one. In this paper, we prove this fact.

**Theorem 1.** For every positive integer \( n \), every \((n, n)\)-map \( E \) admits a quadratic sequential computation. Moreover, if we divide this computation in \( n \) successive blocks of \( n \) assignments, the first \( n-i \) ones in the \( i \)-th block are identities. So, there are at least \( n(n-1)/2 \) identities among the \( n^2 \) assignments.

**Definition. (matrices).** For every finite set \( I \), denote by \(|I|\) the cardinal of \( I \). For every matrix \( M \), \( \mathcal{R}(M) \) is the set of the rows of \( M \) and \( \mathcal{C}(M) \) is the set of the columns of \( M \); for every subset \( S \) of \( \mathcal{R}(M) \), \( M_{|S} \) is the sub-matrix \( M' \) of \( M \) such that \( \mathcal{R}(M') = S \). For two matrices \( M_0, M_1 \) with \(|\mathcal{C}(M_0)| = |\mathcal{C}(M_1)|\), denote by \( M_0 \cup M_1 \) the matrix \( M'' \) such that \( \mathcal{R}(M'') = \mathcal{R}(M_0) \cup \mathcal{R}(M_1) \). For any positive integers \( n, k \) and any finite sequence \((f_0, \ldots, f_{k-1})\) of mappings from \( I \) to \( B_1 \), \([f_0, \ldots, f_{k-1}]\) is the matrix \((f_j(i))_{i \in I, j \in \{0, \ldots, k-1\}}\) and is said \( n \)-functional if for any \( n \leq j < k \), and \( i, i' \in I \):

\[
(f_{j-n}, \ldots, f_{j-1})(i) = (f_{j-n}, \ldots, f_{j-1})(i') \Rightarrow f_j(i) = f_j(i')
\]

Observe that if a matrix is \( n \)-functional, it is also \((n + 1)\)-functional.
Lemma 2. (surgeries). For $1 \leq n$, let $M, M_0 = [f_0, \ldots, f_k], M_1 = [g_0, \ldots, g_h]$ be $n$-functional matrices.

(replacement). The matrix $M'$, obtained by replacing some row of $M$ by another row of $M$, is still $n$-functional.

(induction). For $x = 0, 1$, let $M_x$ be the matrix obtained from $M_x$ by inserting a complete column of $x$'s before the first column and every $n$ columns. The matrices $M'_0, M'_1$ are $(n + 1)$-functional. Moreover, for $k = h$, the matrix $M'' = M_0 \cup M_1$ is also $(n + 1)$-functional.

(matching). If the $n$ last columns $[f_{k-n+1}, \ldots, f_k]$ of $M_0$ are equal to the $n$ first columns $[g_0, \ldots, g_{n-1}]$ of $M_1$ then the matrix $M_{01} = [f_0, \ldots, f_{k-n+1} = g_0, \ldots, f_k = g_{n-1}, \ldots, g_h]$ is also $n$-functional.

Proof. (replacement). Obvious. (induction). Each inserted column in $M'_x$ of index greater than $n + 1$ has constant values $x$ and is defined a fortiori by its $n + 1$ previous columns in $M'_x$. For some column $C'$ of $M'_x$, with index greater than $n + 1$, coming from a column $C$ of $M_x$, the $n$ previous columns of $C$ in $M_x$ enable to define $C$ and appear between the $n + 1$ previous columns of $C'$ in $M'_x$ (one of them has been inserted, say $\Delta$). So $C'$ is defined by its $n + 1$ previous columns and $M'_x$ is $(n + 1)$-functional. For $M'' = M_0 \cup M_1$, the inserted column $\Delta$ enables to separate those parts in $M''$ with a definition by cases. So $M''$ is also $(n + 1)$-functional. (matching). In $M_{01}$, the $n$-functionality comes from $M_0$ for the first columns $[f_0, \ldots, f_k]$ and from $M_1$ for the remaining ones.

3. The idea of the proof.

Let $E$ be an $(n,n)$-map with $n \geq 1$. Let $k$ be a strictly positive integer. If a sequence $\{f_0, \ldots, f_{n-k-1}\}$ of $(n,1)$-maps is a sequential computation of $E$ then the following matrix $[h_0, \ldots, h_{n-1}, h_n, h_{n+1}, \ldots, h_{n+nk-1}]$ is $n$-functional where:

$$h_i = \begin{cases} p^n_i & \text{for } i = 0 \ldots n - 1, \\ f_{i-n} \circ (h_{i-n}, \ldots, h_{i-1}) & \text{for } i \geq n. \end{cases}$$

The first $n$ columns are $p^n_0, \ldots, p^n_{n-1}$, and the $n$ last columns are $E_0, \ldots, E_{n-1}$ : we call it the $n$-functional matrix associated to the sequential computation $(f_0, \ldots, f_{n-k-1})$ of $E$. Reciprocally, if there exists an $n$-functional matrix $M$ with $2n$ rows and $n + nk$ columns such that the first $n$ columns are $p^n_0, \ldots, p^n_{n-1}$, and the $n$ last columns are $E_0, \ldots, E_{n-1}$, then there exists a sequential computation
The sequence \( (f_0, \ldots, f_{n \cdot k - 1}) \) of \( E \) such that \( M \) is the \( n \)-functional matrix associated to this computation. In order to build a quadratic sequential computation of \( E \), we have to construct an \( n \)-functional matrix \( M \) with \( 2^n \) rows and \( (n+1)n \) columns, such that the \( n \) first columns are the projections \( p_0^n, \ldots, p_{n-1}^n \) and such that the \( n \) last columns are \( E_0, \ldots, E_{n-1} \). To this end, we will argue by recursion on the number \( n \) of variables. For \( n = 1 \), it is easy. How can we obtain case \( n + 1 \) using case \( n \)? For example how to compute a convenient matrix in case \( n = 3 \) using case \( n = 2 \)? A natural idea is to find \((3,1)\)-maps \( E'_0, E'_1, E'_2 \) such that \( E'_0 = p_0^3 \) and the matrix \([E'_0, E'_1, E'_2, E_0, E_1, E_2]\) is 3-functional, then to use twice the case \( n = 2 \) to complete the following matrix so that the upper half and the lower half both become 3-functional:

\[
\begin{bmatrix}
 p_0^3 & p_1^3 & p_2^3 & \text{case } n=2 & E'_0 = p_0^3 & E'_1 & E'_2 & E_0 & E_1 & E_2 \\
0 & 0 & 0 & 0 & 0 & a_0 & a_1 & a_2 \\
0 & 0 & 1 & 0 & 0 & b_0 & b_1 & b_2 \\
0 & 1 & 0 & 0 & 0 & c_0 & c_1 & c_2 \\
0 & 1 & 1 & 0 & 0 & d_0 & d_1 & d_2 \\
1 & 0 & 0 & 1 & 1 & e_0 & e_1 & e_2 \\
1 & 0 & 1 & 1 & 1 & f_0 & f_1 & f_2 \\
1 & 1 & 0 & 1 & 1 & g_0 & g_1 & g_2 \\
1 & 1 & 1 & 1 & 1 & h_0 & h_1 & h_2 \\
\end{bmatrix}
\]

From Lemma 2 (induction) and (matching), this whole matrix is 3-functional. It remains to prove the existence of a \((3,3)\)-map \( E' \) such that \( E'_0 = p_0^3 \) and the matrix \([E'_0, E'_1, E'_2, E_0, E_1, E_2]\) is 3-functional. Once more, we will argue by recursion on \( n \). Here, dividing the matrix in one upper half and one lower half does not help us since the first column \( p_0^3 \) is equal to 0 in the upper half and 1 in the lower half and \( p_0^2 \) does not appear in the first column of those halves. A better way is to divide the set of rows of the matrix into two other halves \( I \) and \( J \) with as many rows in the upper half as in the lower half. Since the two first rows in \( I \) belong to the upper half of \( M \) and the two last rows in \( I \) belong to the lower half of \( M \), this implies that \( p_0^2 \) appears in the first column of the matrix \( M_I \). In the same way, \( p_0^2 \) appears in the first column of the matrix \( M_J \). Using case \( n = 2 \) it is now possible to find a mapping \( E'_I \) so that the two matrices \([p_0^3, E'_I, E_0, E_1]_I \) and \([p_0^3, E'_I, E_0, E_1]_J \) become 2-functional; this implies that for every \((3,1)\)-map \( E'_2 \), the matrices \([p_0^3, E'_1, E'_2, E_0, E_1]_I \) and \([p_0^3, E'_1, E'_2, E_0, E_1]_J \) are 3-functional. Since we also want the whole matrix \( M \) to be 3-functional this requires to find a special \((3,1)\)-map \( E'_2 = \Delta \) that "separates" \( M_I \) and \( M_J \), \( i.e. \) for every \( i \in I \) and \( j \in J \), \( \Delta(i) \neq \Delta(j) \) and such that \([\Delta, E_0, E_1, E_2]\) is
3-functional). In general for \( n \geq 2 \), there exists no \((n, 1)\)-map \( \Delta \) such that the matrix \([\Delta, E_0, \ldots, E_{n-1}]\) is \( n \)-functional and such that the column \( \Delta \) has half of its 0’s and 1’s in each half of the matrix: for instance, take the \((n, n)\)-map \( E \) such that for any \( m \in \mathcal{B}_n \):

\[
E(m) = \begin{cases} 
(0, \ldots, 0, 0) & \text{if } m = (0, \ldots, 0, 0) \\
(0, \ldots, 0, 1) & \text{if } m \neq (0, \ldots, 0, 0)
\end{cases}
\]

This situation forces \( \Delta \) to be constant in the lower half of the matrix. However, such a balanced \( \Delta \) always exists when \( E \) is bijective. In order to complete the proof, we have to construct such a \( \Delta \) for a larger class of mappings that we call semi-bijections.

4. A preliminary result for a special class of maps.

**Notation.** For any \( x \in \mathcal{B}_1 \), \( \overline{x} \) is the boolean complement of \( x \); for any subset \( A \) of \( \mathcal{B}_n \), \( A[x] \) is the subset of the elements \( m \) of \( A \) such that the first component of \( m \) is \( x \): \( A[x] = \{ m \in A : p_n^0(m) = x \} \). For any mapping \( E \) defined on \( \mathcal{B}_n \), \( E[x] \) is the set \( \{ E(m) ; m \in \mathcal{B}_n[x] \} \); for every subset \( A \) of \( \mathcal{B}_n \), denote by \( E|_A \) the restriction of \( E \) to the set \( A \).

**Definition.** (semi-bijection) For \( n \geq 1 \), an \((n, n)\)-map \( S \) is semi-bijective if \( S|_{\mathcal{B}_n[0]} \) and \( S|_{\mathcal{B}_n[1]} \) are both bijective, that is \( |S[0]| = |S[1]| = 2^{n-1} \).

Observe that any bijective \((n, n)\)-map is semi-bijective. If an \((n, n)\)-map \( S \) is semi-bijective, each \( m \) in \( \mathcal{B}_{n-1} \) has at most four antecedents by \( (S_0, \ldots, S_{n-2}) \), and each of the two elements \((m, 0)\) and \((m, 1)\) of \( \mathcal{B}_n \) occurs at most twice in the range of \( S \) (at most once in the upper half \( S[0] \) and at most once in the lower half \( S[1] \); this implies that there are nine possible types for the occurrences of \( m \) inside the range of \( S \):

\[
\begin{array}{cccccccc}
mx & mx & mx & mx & mx & mx & mx & mx \\
m\overline{x} & m\overline{x} & m\overline{x} & m\overline{x} & m\overline{x} & m\overline{x} & m\overline{x} & m\overline{x} \\
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8
\end{array}
\]

In the above representation, the horizontal line separates the sets \( S[0] \) and \( S[1] \) and we just indicate in which half appear the elements \((m, x)\) and \((m, \overline{x})\) of \( \mathcal{B}_n \).
Definition. (balanced). For \( n \geq 2 \), an \((n, 1)\)-map \( f \) is balanced if the four sets \( f^{-1}(y)[x] = \{ m \in B_n[x] ; f(m) = y \} \) \((x, y \in B_1)\) have the same cardinality (i.e. \( 2^{n-2} \)).

Lemma 3. For every integer \( n \geq 2 \) and for every semi-bijective \((n, n)\)-map \( S \), there exists a balanced \((n, 1)\)-map \( \Delta \) such that the matrix \([\Delta, S_0, \ldots, S_{n-1}]\) is \( n \)-functional.

Proof. For every type \( t = 0, 1, \ldots, 8 \) denote by \( \lambda_t \) the number of times this type occurs in the range of \( S \). For each occurrence of type \( t \), we check all the possible rules \( R^i_t \) in order to define \( \Delta \) such the matrix \([\Delta, S_0, \ldots, S_{n-1}]\) is \( n \)-functional. The values of \( \Delta \) appear in the first column.

\[
\begin{array}{cccccccccc}
0mx & 0mx & 0mx & 0mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx \\
1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx \\
\hline
0mx & 0mx & 0mx & 0mx & 0mx & 0mx & 0mx & 0mx & 1mx & 1mx \\
1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx & 1mx \\
R_0 & R_1 & R_2 & R_3 & R_4 & R_4 & R_4 & R_4 & R_4 & R_4 \\
\hline
1mx & 0mx & 1mx & 0mx & 0mx & 0mx & 0mx & 0mx & 0mx & 0mx \\
R_5 & R_6 & R_7 & R_8 & R_9 & R_9 & R_9 & R_9 & R_9 & R_9 \\
\end{array}
\]

Let \( a^i_t \) be the number of times the rule \( R^i_t \) is used in the construction of \( \Delta \). Moreover, we chose to never use the two rules \( R_4^3 \) and \( R_4^4 \) \((a^3_4 = a^4_4 = 0)\). One has

\[
\begin{cases}
a^1_t = \lambda_t & \text{for } t = 0, 1, 2 \\
a^1_t + a^2_t = \lambda_t & \text{for } 3 \leq t \leq 8
\end{cases}
\]

Goal: Find some construction of \( \Delta \) such that \( \Delta \) is balanced, i.e. the four sets \( \Delta^{-1}(0)[0], \Delta^{-1}(0)[1], \Delta^{-1}(1)[0], \Delta^{-1}(1)[1] \) have same cardinal \( 2^{n-2} \). Considering the way the rules \( R^i_t \) (except \( R_4^3 \) and \( R_4^4 \)) affect those cardinals, we have:

\[
\begin{align*}
|\Delta^{-1}(0)[0]| &= \lambda_0 + \lambda_1 + \lambda_3 + a^2_4 + a^2_5 + a^2_6 + a^2_7 \\
|\Delta^{-1}(0)[1]| &= \lambda_0 + \lambda_2 + \lambda_6 + a^2_3 + a^2_4 + a^2_5 + a^2_8 \\
|\Delta^{-1}(1)[0]| &= \lambda_0 + \lambda_1 + \lambda_3 + a^2_1 + a^2_5 + a^2_6 + a^2_7 \\
|\Delta^{-1}(1)[1]| &= \lambda_0 + \lambda_2 + \lambda_6 + a^2_3 + a^2_4 + a^2_5 + a^2_8
\end{align*}
\]
In order to obtain $\Delta$ balanced, it is sufficient to have $|\Delta^{-1}(0)[0]| = |\Delta^{-1}(1)[0]|$ and $|\Delta^{-1}(0)[1]| = |\Delta^{-1}(1)[1]|$. So, $a_4^1 + a_3^2 + a_5^2 + a_7^2 = a_4^1 + a_5^1 + a_6^1 + a_7^1$ and $a_3^1 + a_4^1 + a_5^1 + a_8^1 = a_3^3 + a_4^3 + a_5^3 + a_8^3$ give the Goal and since $n \geq 2$ and

\[
|\Delta^{-1}(0)[0]| + |\Delta^{-1}(1)[0]| = 2\lambda_0 + 2\lambda_1 + 2\lambda_3 + \lambda_4 + \lambda_5 + \lambda_6 + \lambda_7 = 2^{n-1}
\]

\[
|\Delta^{-1}(0)[1]| + |\Delta^{-1}(1)[1]| = 2\lambda_0 + 2\lambda_2 + 2\lambda_6 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_8 = 2^{n-1}
\]

the positive integers $\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7$ and $\lambda_3 + \lambda_4 + \lambda_5 + \lambda_8$ are even. For $3 \leq t \leq 8$, let $\pi_t = \lambda_t[2]$ be the remainder of $\lambda_t$ modulo 2. There are 16 possible parity cases and in each case, we define integers $\delta_t$ via the following table:

<table>
<thead>
<tr>
<th>CASE</th>
<th>$\pi_3$</th>
<th>$\pi_4$</th>
<th>$\pi_5$</th>
<th>$\pi_6$</th>
<th>$\pi_7$</th>
<th>$\pi_8$</th>
<th>$\delta_3$</th>
<th>$\delta_4$</th>
<th>$\delta_5$</th>
<th>$\delta_6$</th>
<th>$\delta_7$</th>
<th>$\delta_8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>+1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>+1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>+1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
<td>+1</td>
<td>+1</td>
<td>-1</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>+1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>+1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>+1</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>+1</td>
<td>0</td>
</tr>
<tr>
<td>12</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>0</td>
<td>-1</td>
<td>+1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>+1</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>0</td>
</tr>
<tr>
<td>14</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>+1</td>
<td>-1</td>
<td>0</td>
<td>+1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>15</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>+1</td>
<td>-1</td>
<td>+1</td>
<td>0</td>
<td>0</td>
<td>-1</td>
</tr>
<tr>
<td>16</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>+1</td>
<td>-1</td>
<td>-1</td>
<td>+1</td>
<td>+1</td>
<td>+1</td>
</tr>
</tbody>
</table>

Define for $3 \leq t \leq 8$:

\[
\begin{cases}
    a_t^1 = (\lambda_t - \delta_t)/2 \\
    a_t^2 = (\lambda_t + \delta_t)/2
\end{cases}
\]

In all the 16 cases, one can easily check in the table 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 $\delta_t$'s is not unique, but this one satisfies $\delta_3 = \pi_3$, $\delta_4 = -\pi_4$, $\delta_6 = \pi_6$ that are the only linear relations between the $\delta_t$'s and the $\pi_t$'s. Hence, we obtain the relations for our Goal:

\[
\begin{align*}
    a_4^1 + a_3^2 + a_5^2 + a_7^2 &= a_4^1 + a_5^1 + a_6^1 + a_7^1 = (\lambda_4 + \lambda_5 + \lambda_6 + \lambda_7)/2 \\
    a_3^1 + a_4^1 + a_5^1 + a_8^1 &= a_3^3 + a_4^3 + a_5^3 + a_8^3 = (\lambda_3 + \lambda_4 + \lambda_5 + \lambda_8)/2
\end{align*}
\]

and $\Delta$ is balanced. \hfill \blacktriangleleft
5. Proof of the Theorem.

Lemma 4. For every integer \( n \geq 1 \) and for every \((n,n)\)-map \( E \) there exists an \((n,n)\)-map \( E' \) such that \( E'_0 = p^0_n \) and the following matrix is \( n \)-functional:

\[
\begin{bmatrix}
E'_0, \ldots, E'_{n-1}, E_0, \ldots, E_{n-1}
\end{bmatrix}
\]

Proof. We proceed by recursion on \( n \). For \( n = 1 \), this is obvious. Let \( E = (E_0, \ldots, E_n) \) be an \((n+1,n+1)\)-map.

First case: \( E \) is semi-bijective. We first construct a balanced \((n+1,1)\)-map \( \Delta \) which satisfies the conditions of Lemma 3. Denote by \( I \) and \( J \) the two sets \( \Delta^{-1}(0) \) and \( \Delta^{-1}(1) \). From the recursion hypothesis there exists an \( n \)-functional matrix \( A_I = (a_{i,k})_{i \in I, 0 \leq k \leq 2n-1} \) such that the \( n \) last columns are \( E_0|I, \ldots, E_{n-1}|I \), and the first column satisfies \( a_{i,1} = 0 \) if \( i \in I[0] \) and \( a_{i,1} = 1 \) if \( i \in I[1] \); in the same way, there exists an \( n \)-functional matrix \( A_J = (a_{j,k})_{j \in J, 0 \leq k \leq 2n-1} \) such that the \( n \) last columns are \( E_0|J, \ldots, E_{n-1}|J \), and the first column satisfies \( a_{j,1} = 0 \) if \( j \in J[0] \) and \( a_{j,1} = 1 \) if \( j \in J[1] \). Let \( M \) be the matrix with \( 2^{n+1} \) rows and \( 2n+2 \) columns obtained from the union of \( A_I \) and \( A_J \) and the insertion of the column \( \Delta \) at the \( n+1 \)-th column and the addition of a last column \( E_n \). This matrix is \((n+1)\)-functional from Lemma 2 (induction) and (matching). Let \( E' \) be the \((n+1,n+1)\)-map such that \( M = [E'_0, \ldots, E'_{n-1}, E'_n = \Delta, E_0, \ldots, E_{n-1}, E_n] \). Since \( \Delta \) is balanced, \( |I[0]| = |I[1]| \) and \( |J[0]| = |J[1]| \). It follows that \( E'_0 = p^0_n \).

General case. For any \( x \in B_1 \), let \( Z_x \) be a maximal subset of \( B_{n+1}[x] \) such that \( E|Z_x \) is one-to-one. Let \( S = (S_0, \ldots, S_n) \) be a semi-bijective \((n+1,n+1)\)-map that extends \( E|Z_0 \cup Z_1 \). Using the first case, there exists a \((n+1,n+1)\)-map \( S' \) such that \( S'_0 = p^0_n \) and the matrix \([S'_0, S'_1, \ldots, S'_{n-1}, S'_n, S_0, \ldots, S_{n-1}, S_n]\) is \((n+1)\)-functional. Now, duplicate in the upper half (resp. the lower half) of this matrix, some complete rows in order to obtain \([E_0, \ldots, E_{n-1}, E_n]\) in the \( n+1 \) last columns. From Lemma 2 (replacement), those operations give a new \((n+1)\)-functional matrix \([E'_0 = S'_0, p^0_n, E'_1, \ldots, E'_{n-1}, E'_n, E_0, \ldots, E_{n-1}, E_n]\). \( \blacksquare \)

Proof of Theorem 1. We proceed by induction on \( n \). The case \( n = 1 \) is obvious: by definition, any \((1,1)\)-map \( E \) admits a quadratic sequential computation of length \( 1 : x_0 := E(x_0) \). Let \( E = (E_0, \ldots, E_n) \) be an \((n+1,n+1)\)-map. Using Lemma 4, let \( E' \) be an \((n+1,n+1)\)-map such that \( E'_0 = p^0_n \), and the matrix \( T = [E'_0, E'_1, \ldots, E'_n, E_0, \ldots, E_n] \) is \((n+1)\)-functional. For \( x = 0,1 \) let \( e^x = (e^x_1, \ldots, e^x_n) \) be the \((n,n)\)-map such that
for every $1 \leq i \leq n$ and $m \in \mathbf{B}_n$, $e_i^x(m) = E_i^x(x, m)$. Using the recursion hypothesis, $e_i^x$ admits a quadratic sequential computation and there exists a $n$-functional matrix $M_x = [p_0^n, \ldots, p_{n-1}^n, f_0^n, \ldots, f_{n^2-1}^n]$ such that its $n$ last columns are $e_1^x, \ldots, e_n^x$. From Lemma 2 (induction), we obtain an $(n+1)$-functional matrix $[p_0^{n+1}, \ldots, p_{n+1}^{n+1}, F_0, \ldots, F_{n^2-1+n} = E_n^x]$ such that its $n+1$ last columns are $E_0^x, \ldots, E_n^x$. From Lemma 2 (matching), since $T = [E_0^x, E_1^x, \ldots, E_n^x, E_0, \ldots, E_n]$ is also $(n+1)$-functional, the matrix $M = [p_0^{n+1}, \ldots, p_{n+1}^{n+1}, F_0, \ldots, F_{n^2-1+2n}, E_0, \ldots, E_n]$ is $(n+1)$-functional and gives a quadratic sequential computation of $E$. For the second part of the Theorem, for $0 \leq k \leq n-1$, by construction, the first column of $k$-th bloc of $n$ columns in $M$ is $p_0^{n+1}$ and, by recursion, for $1 \leq i < n+1-k$, the $i+1$-th column of $B_k$ is $p_i^{n+1}$. We hence obtain $n + (n-1) + \ldots + 1 = (n+1)n/2$ identities among the $(n+1)^2$ assignments that constitute the quadratic sequential computation of $E$. \hfill

6. An example.

Let us consider the $(3, 3)$-map $E$ which is defined by the following table:

\[
\begin{array}{cccc}
E_0 & E_1 & E_2 \\
0 & 0 & 0 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & 1 \\
0 & 1 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 \\
\end{array}
\]

That gives the following polynomial expression of $E$ (note that every $(n, 1)$-map is polynomial):

$$E(x, y, z) = (xy + yz + xy z, 1 + x + y + z + xy + xz + yz, x + y + z + xz)$$

There are two blocks of three $(3, 1)$-maps to compute.

*We first compute the second block. Using Lemma 4, we will find $(3, 1)$-maps $E'_0, E'_1, E'_2$ such that $E'_0 = p_0^3$ and the matrix $[E'_0, E'_1, E'_2, E_0, E_1, E_2]$ is 3-functional. The sets $Z_0 = \{000, 001, 011\}$ and $Z_1 = \{100, 110, 111\}$ are maximal subsets of $\mathbf{B}_3[0]$ and $\mathbf{B}_3[1]$ such that $E_{|Z_0}$ and $E_{|Z_1}$ are one-to-one. We now consider some semi-bijective $(3, 3)$-map $S = (S_0, S_1, S_2)$ that extends $E_{|Z_0 \cup Z_1}$.
Since $S$ is semi-bijective, we can use Lemma 3 to obtain a balanced (3,1)-map $\Delta$ such that the matrix $[\Delta, S_0, S_1, S_2]$ is 3-functional. Each element $m$ of $B_2$ occurs in the range of $S$ with some type $t$ given in the following table:

<table>
<thead>
<tr>
<th>$m$</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>3</td>
</tr>
<tr>
<td>01</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
</tr>
<tr>
<td>11</td>
<td>8</td>
</tr>
</tbody>
</table>

Using the proof of Lemma 3, $\lambda_3$ and $\lambda_8$ are odd: this is the case no 9 and the table gives $\delta_3 = +1$, $\delta_8 = -1$, $a_3^1 = (\lambda_3 - \delta_3)/2 = 0$, $a_3^2 = (\lambda_3 + \delta_3)/2 = 1$, $a_8^2 = (\lambda_8 - \delta_8)/2 = 1$ and $a_8^2 = (\lambda_8 + \delta_8)/2 = 0$. So, we have to build $\Delta$ using once each rule $R_3^2$ and $R_8^1$. We obtain a balanced (3,1)-map $\Delta$ such that the following matrix $[\Delta, S_0, S_1, S_2]$ is 3-functional:

$$
\begin{bmatrix}
\Delta & S_0 & S_1 & S_2 \\
1 & 0 & 1 & 0 \\
1 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 \\
0 & 0 & 1 & 0 \\
1 & 1 & 0 & 0 \\
0 & 1 & 1 & 0 \\
\end{bmatrix}
$$

We now apply the proof of Lemma 4 in order to find a (3,3)-map $S'$ such that the matrix $[S'_0 = p_0^3, S'_1, S'_2 = \Delta, S_0, S_1, S_2]$ is 3-functional. Define $I = \Delta^{-1}(0) = \{010, 011, 101, 111\}$ and $J = \Delta^{-1}(1) = \{000, 001, 100, 110\}$. We divide the matrix $A = [\Delta, S_0, S_1, S_2]$ in two sub-matrices $A_I$ and $A_J$ with rows indexed by $I$ and $J$. We apply Lemma 4 to complete the two following matrices which are 2 functional:
\[
\begin{bmatrix}
 p_0^3 & S'_0 & S_0 & S_1 & S'_1 \\
 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 1 & 0 & 1 \\
 1 & 1 & 0 & 1 & 1 \\
 1 & 0 & 1 & 1 & 1 \\
\end{bmatrix}
\begin{bmatrix}
 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 0 & 0 \\
 1 & 1 & 0 & 0 & 0 \\
 1 & 0 & 1 & 0 & 0 \\
\end{bmatrix}
\]

Let \( M \) be the matrix with \( 2^3 = 8 \) rows and \( 2 \times 2 + 2 = 6 \) columns which is obtained from the union of \( A_{II} \) and \( A_{IJ} \) by inserting the column \( \Delta \) at the \( n + 1 = 3 \)-th column and adding \( S_2 \) as last column; \( S'_1 \) is the \((3,1)\)-map such that \( M = [p_0^3, S'_1, \Delta, S_0, S_1, S_2] \).

\[
M = \begin{bmatrix}
 S'_0 = p_0^3 & S'_1 & S'_2 = \Delta & S_0 & S_1 & S_2 \\
 0 & 0 & 1 & 0 & 1 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 0 & 0 & 0 & 0 & 0 \\
 0 & 1 & 0 & 1 & 0 & 0 \\
 1 & 1 & 1 & 0 & 0 & 1 \\
 1 & 1 & 0 & 0 & 1 & 0 \\
 1 & 0 & 1 & 1 & 0 & 0 \\
 1 & 0 & 0 & 1 & 1 & 0 \\
\end{bmatrix}
\]

At last, we duplicate the row no 2 in the row no 3 (in the upper half) and row no 5 in row no 6 (in the lower half) in order to obtain \([E_0, E_1, E_2] \) as last columns. From Lemma 2 (replacement), we obtain a new 3-functional matrix :

\[
T = \begin{bmatrix}
 E'_0 & E'_1 & E'_2 & E_0 & E_1 & E_2 \\
 0 & 0 & 1 & 0 & 1 & 0 \\
 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 1 & 1 & 0 & 0 & 1 \\
 0 & 1 & 0 & 1 & 0 & 0 \\
 1 & 1 & 0 & 0 & 1 & 1 \\
 1 & 1 & 0 & 0 & 1 & 1 \\
 1 & 0 & 1 & 1 & 0 & 0 \\
 1 & 0 & 0 & 1 & 1 & 0 \\
\end{bmatrix}
\]

*We now compute the first block.* We apply twice the Theorem for \( n = 2 \). For \( x = 0,1 \) and \( i = 1,2 \), denote by \( e^x_i \) the \((n,1)\)-map such that for every \( m \in B_2 \), \( e^x_i(m) = E'_i(x, m) \). The \((2,2)\)-map \( e^x = (e^x_1, e^x_2) \) admits a quadratic sequential computation : let \( f_0^x, f_1^x, f_2^x, f_3^x \) be \((2,1)\)-maps such that the matrix \([p_0^2, p_1^2, f_0^x, f_1^x, f_2^x, f_3^x] \) is 2-functional and such that its two last columns are \( e^x_1, e^x_2 \).
\[
M_0 = \begin{bmatrix}
0 & 0 & f_0^0 = p_0^0 & f_1^0 = p_1^0 & f_2^0 = e_1^0 & f_3^0 = e_2^0 \\
0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 \\
\end{bmatrix}
\]

\[
M_1 = \begin{bmatrix}
0 & 0 & f_0^1 = p_0^1 & f_1^1 = p_1^1 & f_2^1 = e_1^1 & f_3^1 = e_2^1 \\
0 & 1 & 0 & 0 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 \\
1 & 1 & 1 & 1 & 0 & 0 \\
\end{bmatrix}
\]

From Lemma 2 (induction) and (matching), the following matrix is 3-functional:

\[
\begin{bmatrix}
p_0^3 & p_1^3 & p_2^3 & p_0^3 & p_1^3 & E'_0 & E'_1 & E'_2 & E_0 & E_1 & E_2 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\
1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
\end{bmatrix}
\]

This matrix gives the following quadratic sequential computation of \( E \):

\[
\begin{align*}
x & := x \\
y & := y \\
z & := y + z + xy \\
x & := x \\
y & := x + y + z + xz + yz + xyz \\
z & := 1 + y + z + xy + xyz \\
x & := 1 + z + xy + xz \\
y & := x + y + z \\
z & := 1 + x + yz 
\end{align*}
\]
7. Conclusion.

In the quadratic sequential computations that we have built in this paper, any boolean function can be used. On the other hand, following an idea of Sophie Piccard (see [3]), it has been proved in [2] that for any \( n \), there exist three \((n, 1)\)-maps : \( T_n \), \( C_n \), \( S_n \) such that any \((n, n)\)-map has a sequential computation only using those three functions. However, such a computation cannot be quadratic nor polynomial : the number of possible sequential computations using \( p(n) \) functions of length \( q(n) \) is bounded by \( p(n)q(n) \) that is strictly bounded by the number \( 2^n q(n) \) of possible \((n, n)\)-maps, when \( p, q \) are both polynomials and \( n \) is large enough.


Serge Burckel : C.N.R.S., Institut de Mathématiques de Luminy U.P.R. 9016, Campus de Luminy, 13288 Marseille cedex 9, France.
Marianne Morillon : Département de Mathématiques et Informatique, Université de la Réunion, 15 av. René Cassin, BP 7151, 97715 Saint-Denis Messag. cedex 9, France.

http://www.univ-reunion.fr/~burckel/,
http://www.univ-reunion.fr/~mar/
burckel@iml.univ-mrs.fr,
mar@univ-reunion.fr