INFORMATIQUE THÉORIQUE ET APPLICATIONS

SERGE BURCKEL
MARIANNE MORILLON

Three generators for minimal writing-space computations

Informatique théorique et applications, tome 34, nº 2 (2000), p. 131-138
<http://www.numdam.org/item?id=ITA_2000__34_2_131_0>

Theoretical Informatics and Applications
Theoret. Informatics Appl. **34** (2000) 131–138

THREE GENERATORS FOR MINIMAL WRITING-SPACE COMPUTATIONS

SERGE BURCKEL[1] AND MARIANNE MORILLON[1]

Abstract. We construct, for each integer n, three functions from $\{0,1\}^n$ to $\{0,1\}$ such that any boolean mapping from $\{0,1\}^n$ to $\{0,1\}^n$ can be computed with a finite sequence of assignations only using the n input variables and those three functions.

AMS Subject Classification. 68Q, 06E30, 03D15.

Let n be a positive integer. A $n,1$-map is a mapping from $\{0,1\}^n$ to $\{0,1\}$ and a n,n-map is a mapping from $\{0,1\}^n$ to $\{0,1\}^n$. Given a n,n-map E, the computer scientist's problem is to write a program that computes from any vector $(x_0,\dots,x_{n-1})$ in $\{0,1\}^n$ its image $(y_0,\dots,y_{n-1}) = E(x_0,\dots,x_{n-1})$; such a program uses N variables $x_0,\dots,x_{n-1},\dots,x_{N-1}$ and consists of a finite sequence of k assignations: $\texttt{for } i=0 \texttt{ to } k-1 \texttt{ do } x_{v_i} := f_i(x_0,\dots,x_{N-1})$ where $0 \le v_i < N$, f_i is a $n,1$-map and $(x_0,\dots,x_{n-1}) = (y_0,\dots,y_{n-1})$ holds at the end of the computation. Observe that a n,n-map $E = (E_0,\dots,E_{n-1})$, where each $n,1$-map E_i is the i-th component of E, is not (in general) computed by the program: $\texttt{for } i=0 \texttt{ to } n-1 \texttt{ do } x_i := E_i(x_0,\dots,x_{n-1})$. However, E is computed by the following program using $N = 2n-1$ variables:

1) copy almost all the initial vector: $\texttt{for } i=0 \texttt{ to } n-2 \texttt{ do } x_{n+i} := x_i$;
2) use the safe copy: $\texttt{for } i=0 \texttt{ to } n-1 \texttt{ do } x_i := E_i(x_n,\dots,x_{2n-2},x_{n-1})$.

For example, the $2,2$-map T such that $T(x_0,x_1) = (x_1,x_0)$ (exchange) is not computed by the program: $x_0 := T_0(x_0,x_1), x_1 := T_1(x_0,x_1)$ (that computes the different $2,2$-map $(x_0,x_1) \mapsto (x_1,x_1)$) but T is usually computed by a program using $N = 3 > n$ variables:

$$x_2 := f_0(x_0,x_1,x_2), x_0 := f_1(x_0,x_1,x_2), x_1 := f_2(x_0,x_1,x_2)$$

where f_i is the i-th projection for any $i \in \{0,1,2\}$.

Keywords and phrases: Boolean functions, models of computations.

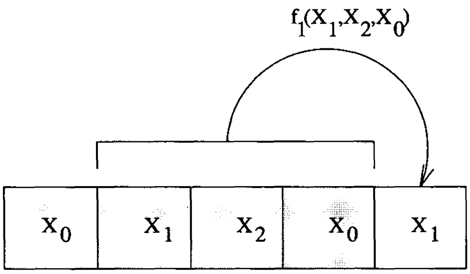
[1] Département de Mathématiques et d'Informatique, 15 avenue René Cassin, Université de la Réunion, 97490 Saint-Denis, France; e-mail: `burckel@univ-reunion.fr`, `mar@univ-reunion.fr`

It is pertinent to ask the following question: *is there a way to compute any n,n-map using no more than the n initial variables (i.e. $N \leq n$)?* For example, it is well known that the above exchange mapping T is computed by the following program: $x_0 := f_0(x_0,x_1), x_1 := f_1(x_0,x_1), x_0 := f_2(x_0,x_1)$ where f_0, f_1, f_2 are all equal to the XOR $2,1$-map. In [2], we give a positive answer to the above question and prove that any n,n-map E admits such a sequential decomposition, however, the length of this decomposition can be exponential according to n. In [3], we give an effective general construction of length exactly n^2 using at most n variables. Since both constructions in [2] and [3] rely on assignations using arbitrary mappings f_j, the following question is natural: *is there a set of mappings that generates any sequential decomposition with a minimal number of variables?*

A result of Piccard (see [4]) implies that, for any finite set G, there are three mappings such that any mapping $E : G \longrightarrow G$ has a decomposition into those three mappings (a transposition, an identification and a circular shifting). We will use this idea. However, this will require some refinements since we are interested in decompositions of n,n-maps into $n,1$-maps (and not into n,n-maps). In this paper we construct for any n, three $n,1$-maps T_n, C_n, S_n that enable to build a sequential decomposition of any n,n-map.

Definition. Let n be a positive integer. For any positive integer i, we denote by $i[n]$ the remainder of i modulo n. Let F be a set of $n,1$-maps. A n,n-map E has a *sequential decomposition over F* if there exists a positive integer k and nk mappings $f_0, \dots, f_{nk-1}$ in F such that, for any $(x_0,\dots,x_{n-1})$ in $\{0,1\}^n$ and $(y_0,\dots,y_{n-1}) = E(x_0,\dots,x_{n-1})$, the program: $\texttt{for } i = 0 \texttt{ to } nk-1 \texttt{ do } x_{i[n]} := f_i(x_{i[n]}, x_{(i+1)[n]}, \dots, x_{(i+n-1)[n]})$ ends with $(x_0,\dots,x_{n-1}) = (y_0,\dots,y_{n-1})$. The integer nk is the *length* of this decomposition. A set F is *n-generator* (resp. *n-bijector*) if any (resp. any bijective) n,n-map has a sequential decomposition over F.

Observe that any n-generator set is also n-bijector. The previous definition is a little bit different from [2]. Let us explain it: at any step, some variable x_i is affected by means of the values of the n ones considered from x_i:



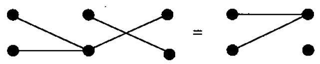
For instance, any affectation of the form $x_i := x_i$ corresponds in the sequential decomposition to the first projection $n,1$-map.

The functions f_i involved in a sequential decomposition may be quite different. For any arbitrary large integer n, the cardinal of some n-generator set F could be arbitrary large as well. The exchange mapping of two variables can be computed as $x_0 := Q(x_0, x_1); x_1 := Q(x_1, x_0); x_0 := Q(x_0, x_1); x_1 := P(x_1, x_0)$ where Q is the 2,1-map such that $Q(a, b) = 0$ if and only if $(a = b)$ and P is the first projection 2,1-map with $P(a, b) = a$. We only need those 2 different 2,1-maps for the exchange of two variables. But the set $\{P, Q\}$ cannot be used for any 2,2-map. It is not n-generator and even not n-bijector as well. Since $Q(0,0) = P(0,0) = 0$, the assignation $(x_0, x_1) = (0,0)$ can never change during any computation. We will construct in the sequel two functions that enable to exchange and to perform any bijection over two variables. Observe that this set will be $\{\bar{P}, \bar{Q}\}$. We are going to prove the following main result:

Theorem 1. *For every positive integer n, there exists a n-generator set of cardinal 3 (resp. of cardinal 2 for $n = 1$) and a n-bijector set of cardinal 2 (resp. of cardinal 1 for $n = 1$). Moreover, these cardinals are minimal.*

The case $n = 1$ is obvious. Consider the two 1,1-maps S, C such that $S(0) = 1$, $S(1) = 0$ and $C(0) = C(1) = 1$. The set $\{S, C\}$ is 1-generator since all the 4 possible 1,1-maps can be obtained by compositions of S and C. For example, the program $x_0 := C(x_0); x_0 := S(x_0)$ maps any x_0 to 0. The set $\{S\}$ is 1-bijector. The identity map is computed with the sequence $x_0 := S(x_0); x_0 := S(x_0)$.

Consider an arbitrary ordering of $\{0,1\}^n$. A transposition (resp. collapsing) consists in the exchange (resp. identification) of two consecutive elements. Notice that there are 2^n different such elementary operations. Any n,n-map E can be decomposed into a finite sequence of transpositions and collapsings. For the collapsings, one could identify two consecutive elements to the first one or to the second one. Both possibilities are equivalent up to a transposition:



Any finite sequence of n,1-maps defines a n,n-map as follows.

Definition. Let F be a n,1-map. The n,n-map $\widetilde{F}$ *induced* by F satisfies the relations $\widetilde{F}(aM) = Mb$ if and only if $F(aM) = b$ for any M in $\{0,1\}^{n-1}$ and a, b in $\{0,1\}$. Let $L = (F_1, \ldots, F_k)$ be a finite sequence of n,1-maps. This sequence induces the n,n-map $\widetilde{L} = \widetilde{F_k} \circ \ldots \circ \widetilde{F_1}$.

For example, the 2,1-maps F, G such that:

$$F(00) = 1; F(01) = 1; F(10) = 1; F(11) = 0$$

$$G(00) = 0; G(01) = 1; G(10) = 0; G(11) = 1$$

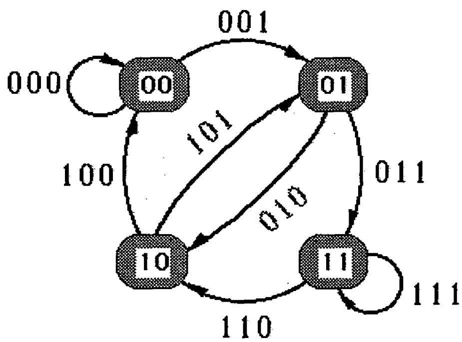
enable to induce the 2,2-maps

$$\widetilde{F}(00) = 01; \widetilde{F}(01) = 11; \widetilde{F}(10) = 01; \widetilde{F}(11) = 10$$
$$\widetilde{G}(00) = 00; \widetilde{G}(01) = 11; \widetilde{G}(10) = 00; \widetilde{G}(11) = 11$$
$$\widetilde{(F,G)}(00) = 11; \widetilde{(F,G)}(01) = 11; \widetilde{(F,G)}(10) = 11; \widetilde{(F,G)}(11) = 00.$$

Adapting the result of [2] to this definition, a n, n-map E has a sequential decomposition if and only if there exists a finite sequence L of $n, 1$-maps such that $E = \widetilde{L}$ and L has a length multiple of n. Then, for theorem 1, we will construct 3 different functions over which there exists sequences that induce any transposition and any collapsing. Following the construction of Sophie Piccard about mappings over finite sets (see [4]), any one of the 2^n different transpositions (resp. collapsings) can be computed by means of just a particular one and a circular shifting. According to the work in [2], this circular shifting is induced by some $n, 1$-map constructed from some Eulerian circuit in the de Bruijn graph B_n. Let S_n be this map. We will modify S_n in order to construct a function T_n (resp. C_n) that nearly induces a transposition (resp. collapsing). So, the set $\{T_n, C_n, S_n\}$ will be n-generator.

Let us recall the definition of the de Bruijn graph B_n (see [1]). This graph is composed of 2^{n-1} vertices labeled with the different elements of $\{0,1\}^{n-1}$ and of 2^n edges labeled with the different elements of $\{0,1\}^n$. There is an edge labeled aMb from the vertex aM to the vertex Mb for every $a, b \in \{0,1\}$ and every element M of $\{0,1\}^{n-2}$.

Example. The graph B_3 is



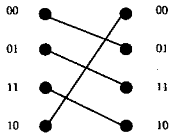
The interesting property is that any graph B_n contains an Eulerian circuit (in fact $2^{2^{n-1}-n}$). The two ones of B_3 are:

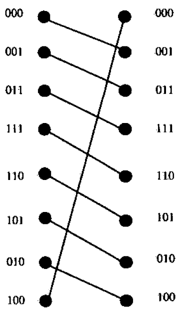
$$(000, 001, 011, 111, 110, 101, 010, 100, 000)$$
$$(000, 001, 010, 101, 011, 111, 110, 100, 000).$$

Any such circuit enables to construct a circular shift function in the following way.

Definition. Let $(M_0, M_1, \ldots, M_{2^n})$ be an Eulerian circuit of the de Bruijn graph B_n (with $M_0 = M_{2^n} = 0^n$). The associated circular shift S_n is the $n, 1$-map that maps M_i to the last letter of M_{i+1} for $0 \leq i < 2^n$.

Graph representation of $\widetilde{S_2}$ and $\widetilde{S_3}$ (from the first Eulerian circuit in B_3):



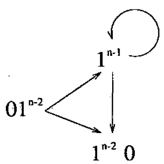


We need some information about every Eulerian circuit in B_n in order to have some invariant regularities on the function S_n.

Lemma 2. *For any positive integer $n \geq 2$, any Eulerian circuit in B_n necessarily contains the two subsequences: $(01^{n-1}, 1^n, 1^{n-1}0)$ and $(10^{n-1}, 0^n, 0^{n-1}1)$. The relations $S_n(01^{n-1}) = 1, S_n(1^n) = 0, S_n(10^{n-1}) = 0, S_n(0^n) = 1$ always hold.*

Proof. Observe that for any $n \geq 2$ the graph B_n contains the edges:

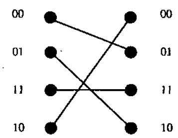
$$(01^{n-2}, 1^{n-1}); (01^{n-2}, 1^{n-2}0); (1^{n-1}, 1^{n-2}0); (1^{n-1}, 1^{n-1}).$$

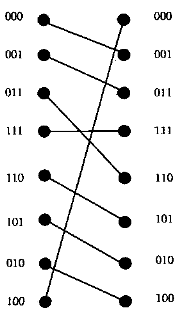


Any path from 0^{n-1} to 1^{n-1} must use the edge $(01^{n-2}, 1^{n-1})$ labeled 01^{n-1}. Then the only possibility to use the edge $(1^{n-1}, 1^{n-1})$ labeled 1^n is to use it next. Then we have to take the edge $(1^{n-1}, 1^{n-2}0)$ labeled $1^{n-1}0$. We obtain the other subsequence by symmetry and the relations on S_n directly follow. $\square$

Definition. The $n, 1$-map T_n satisfies $T_n(01^{n-1}) = 0$ and $T_n(1^n) = 1$ and $T_n(M) = S_n(M)$ for any other element $M \in \{0,1\}^n$.

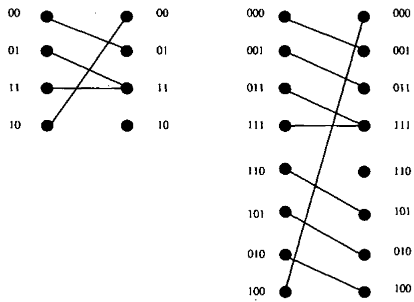
Graph representation of $\widetilde{T_2}$ and $\widetilde{T_3}$:





Definition. The $n,1$-map C_n satisfies $C_n(1^n) = 1$ and $C_n(M) = S_n(M)$ for any other element $M \in \{0,1\}^n$.

Graph representation of $\widetilde{C_2}$ and $\widetilde{C_3}$:



The n,n-maps $\widetilde{S_n}$ and $\widetilde{T_n}$ are permutations on $\{0,1\}^n$. Let us compute their respective orders. This will give a useful Arithmetical property for the proof.

Lemma 3. *For any $n \geq 2$, the sequence of S_n (resp. T_n) repeated 2^n (resp. $2^n - 1$) times induces the identity n,n-map.*

Proof. Observe that $\widetilde{S_n}$ maps any element of $\{0,1\}^n$ to the next one in the Eulerian circuit. Composed 2^n times, we obtain the identity map. The n,n-map $\widetilde{T_n}$ is a circular permutation on $\{0,1\}^n \backslash \{1^n\}$ and it leaves unchanged the element 1^n. Repeated $2^n - 1$ times, we also obtain the identity map. □

We can now prove the main result.

Proof of Theorem 1. We prove that for any integer n, the particular set $\{T_n, C_n, S_n\}$ is n-generator. By construction, any transposition (resp. collapsing) is the composition of a finite number of $\widetilde{S_n}$ and $\widetilde{T_n}$ (resp. $\widetilde{C_n}$) and again a finite number of $\widetilde{S_n}$. As any n,n-map E is the composition of some transpositions and collapsings, E is induced by a finite sequence L on T_n, C_n, S_n. But it remains a problem of index. The length l of this sequence L must be multiple of n in order to have a sequential decomposition and affect the good variables at the end. For example, for $n = 2$, the first projection P induces the exchange mapping since $\widetilde{P}(x_0, x_1) = (x_1, x_0)$. But the corresponding program $x_0 := P(x_0, x_1) = x_0$ does nothing. So, the length of the sequence is crucial. For that aim, we are going to add a subsequence that induces the identity n,n-map such that the total length is a multiple of n. We show now that it is always possible. Using Lemma 3, an obvious arithmetical argument is available. Assume n is odd, so n is coprime with 2^n and for any positive integer h, there exists a positive integer q such that $q.2^n \equiv h[n]$. Then, one can always add a certain number of identities, that each consists of 2^n times S_n, in order to obtain an equivalent calculus of length $l + q2^n \equiv 0[n]$ that gives a sequential decomposition. Assume now, n is even. In that case, n is not coprime with 2^n. We are going to use some T_n sequences of length $2^n - 1$ that each induces the identity n,n-map. As n can be not coprime with 2^{n-1} as well (for example $n = 6, 2^n - 1 = 63$), we also need some S_n sequences. For any $n \geq 2$, 2^n is coprime with $2^n - 1$. For any positive integer h, there exist two positive integers q_0, q_1 such that $q_0.2^n + q_1.(2^n - 1) \equiv h[n]$. Then, one can always add a certain number of identities, that each consists of 2^n times S_n or $2^n - 1$ times T_n, in order to obtain an equivalent calculus of length $l + q_0.2^n + q_1.(2^n - 1) \equiv 0[n]$ that gives a sequential decomposition. Let us consider now the restriction to bijective mappings. Those are particular ones and can be constructed over $\{T_n, C_n, S_n\}$. Since $\widetilde{C_n}$ is not one-to-one, C_n do not appear in any sequence for any bijection and $\{T_n, S_n\}$ is a n-bijector set. For the minimality, observe that for any n, 1-map U, any two different induced mappings $\widetilde{U^p}$ and $\widetilde{U^q}$ commute since $\widetilde{U^p} \circ \widetilde{U^q} = \widetilde{U^{p+q}} = \widetilde{U^q} \circ \widetilde{U^p}$. Hence, the set $\{U\}$ is not n-bijector for $n \geq 2$ since there are bijections that do not commute. So the cardinal of any n-bijector set is at least 2 for $n \geq 2$. Now, any n-generator set contains at least one n, 1-map V such that the induced map $\widetilde{V}$ is not one-to-one. Hence, the cardinal of any n-generator set is at least 3 for $n \geq 2$. □

For any n, the Boolean functions T_n, C_n, S_n are effective. For example, $S_2(a, b) = \bar{a}$, $T_2(a, b) = (\bar{a} \wedge \bar{b}) \vee (a \wedge b)$, $C_2(a, b) = \bar{a} \vee b$. Observe that $S_2 = \bar{P}$ and $T_2 = \bar{Q}$ and, as we said in the introduction, $\{\bar{P}, \bar{Q}\}$ is a 2-bijector set. For $n = 3$, one has $S_3(a, b, c) = (\bar{a} \wedge \bar{b}) \vee (\bar{a} \wedge c) \vee (a \wedge b \wedge \bar{c})$, $T_3(a, b, c) = T_2(a, b)$, $C_3(a, b, c) = T_2(a, b) \vee (b \wedge c)$. It could be useful to have such expressions for any n. As T_n, C_n depend on S_n, we only need to have some Boolean expression of the n, n-map that maps a vertex to the next one in some Eulerian circuit of the graphs B_n.

Any n, n-map E can be coded by a finite word in $\{T, C, S\}^*$ (and in $\{T, S\}^*$ for bijections) that represents its sequential decomposition. For the two variables exchange, the sequence $SSTST$ induces the Exchange mapping but, as we have seen in the proof, it does not represent a sequential decomposition since its length is 5 and gives the calculus from $(x_0, x_1) = (0, 1)$:

$$x_0 := S(0,1) = 1, x_1 := S(1,1) = 0,$$
$$x_0 := T(1,0) = 0, x_1 := S(0,0) = 1, x_0 := T(0,1) = 0$$

that leaves the vector $(0, 1)$ unchanged. According to the proof, this calculus can be completed with the identity induced by TTT

$$x_1 := T(1,0) = 0, x_0 := T(0,0) = 1, x_1 := T(0,1) = 0$$

and $SSTSTTTT$ represents a sequential decomposition of length 8 for the exchange. Observe there are shorter calculus: $STSSTT$ and $TTSSTS$ of length 6. What about this length in general?

As any n, n-map $\widetilde{T_n}, \widetilde{C_n}, \widetilde{S_n}$ maps an element of the Eulerian circuit to the next one (or to the second next one for $\widetilde{T_n}$ on 01^{n-1}) any n, n-map that maps the element 0^n to the previous one 10^{n-1} will require at least $2^n - 2$ steps that is exponential according to n. In a recent work [3], we prove that any n, n-map has a sequential decomposition in exactly n^2 steps.

The authors wish to thank some anonymous referee for his comments and for pointing out the link with Sophie Piccard's theorem.

References

[1] N.G. de Bruijn, A combinatorial problem. *Indag. Math.* **8** (1946) 461–467.
[2] S. Burckel, Closed Iterative Calculus. *Theoret. Comput. Sci.* **158** (1996) 371–378.
[3] S. Burckel and M. Morillon, *Computing Without Copying* (submitted).
[4] S. Piccard, Sur les fonctions définies dans les ensembles finis quelconques. *Fund. Math.* **24** (1935) 298–301.

Communicated by D. Niwinski.
Received June 14, 1999. Accepted April 18, 2000.