HAL open science

The Block Neighborhood

Pablo Arrighi, Vincent Nesme

To cite this version:

Pablo Arrighi, Vincent Nesme. The Block Neighborhood. Journées Automates Cellulaires 2010, Dec 2010, Turku, Finland. pp.43-53. hal-00542488

HAL Id: hal-00542488

https://hal.science/hal-00542488v1

Submitted on 2 Dec 2010

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Journées Automates Cellulaires 2010 (Turku), pp. 43-53

THE BLOCK NEIGHBORHOOD

PABLO ARRIGHI [1] AND VINCENT NESME [2]

[1] Université de Grenoble, LIG, 220 rue de la chimie, 38400 Saint-Martin-d'Hères, France
E-mail address: pablo.arrighi@imag.fr
URL: http://membres-lig.imag.fr/arrighi/

[2] Quantum information theory, Universität Potsdam, Karl-Liebknecht-Str. 24/25, 14476 Potsdam, Germany
E-mail address: vnesme@gmail.com
URL: http://www.itp.uni-hannover.de/~nesme/

Abstract. We define the block neighborhood of a reversible CA, which is related both to its decomposition into a product of block permutations and to quantum computing. We give a purely combinatorial characterization of the block neighborhood, which helps in two ways. First, it makes the computation of the block neighbourhood of a given CA relatively easy. Second, it allows us to derive upper bounds on the block neighborhood: for a single CA as function of the classical and inverse neighborhoods, and for the composition of several CAs. One consequence of that is a characterization of a class of "elementary" CAs that cannot be written as the composition of two simpler parts whose neighborhoods and inverse neighborhoods would be reduced by one half.

Introduction

Otherwise decent people have been known to consider reversible cellular automata (RCAs) and look for ways to decompose them into a product of reversible blocks permutations. One big incentive for doing so is to ensure structural reversibility, as was the concern in [Mar84], as it helps to design RCAs (see for instance [MH89, MU92]), whereas determining from its local transition function whether a CA is reversible is undecidable [Kar90].

Sadly, the relation is not clearly understood between both frameworks; several articles tackle this problem [Kar96, Kar99, DL01], whose conclusion, in a nutshell, is the following. It is always possible, by increasing the size of the alphabet, to simulate a d-dimensional CA by a reversible block CA of depth at most $d+1$. In the case of dimensions 1 and 2, up to shifts, no additional space and no coding is needed; it is still an open problem whether the same can be said in higher dimensions.

We will be here concerned with the size of the blocks, or rather, with the information on the neighborhood that is deducible purely geometrically from a block structure decomposition.

2000 ACM Subject Classification: F.1.1.
Key words and phrases: cellular automata, neighborhood, quantum, block representation.

creative commons

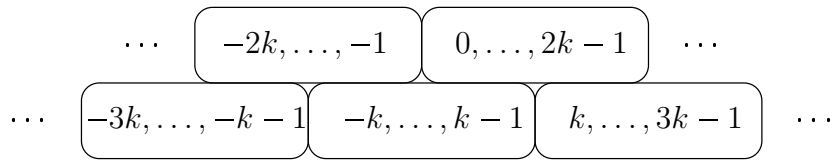

Figure 1: The geometric neighborhood in a block structure.

If we just know that the CA is defined by such a structure, we can deduce, for instance, that the cell 0 has an influence only on the cells $-2k, \dots, 2k-1$, which means the neighborhood of this CA has to be included in $[\![-2k+1; 2k]\!]$. But it is also true that the cells $-k$ and $k-1$ influence only the cells $-2k, \dots, 2k-1$, so the translation invariance tells us more: we can deduce that the neighborhood of this CA is included in $[\![-k; k]\!]$. Another way to look at it is to modify slightly the block structure, and update cell 0 once and for good on the first step, so that the new structure would look something like Figure 2.

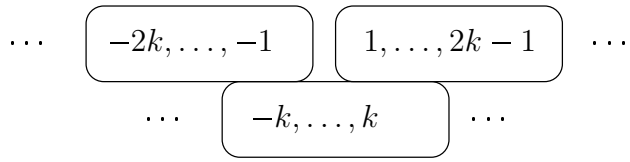

Figure 2: Block structure with a tooth gap.

If we concentrate only on the central block on the first line and the fact that no block of the second line acts on cell 0 and ask what can then be the minimal size of the central block, we get to Figure 3 and our definition of the block neighborhood in Definition 1.4. Section 1 is devoted to the basic properties of this neighborhood, in particular Proposition 1.5 gives an expression of it in terms of combinatorics on words.

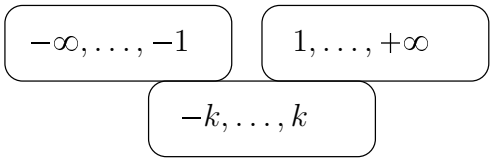

Figure 3: Simplified block structure.

So, how large must this central block be? Since it does all the work updating the state of cell 0, it should at least include the neighborhood of this cell. But there is a dual way to look at Figure 2 when it is turned upside-down. What we know see is a block decomposition of the inverse CA, where the first step updates the complement of $[\![-k; k]\!]$, so we also have a condition involving the neighborhood of the inverse CA, which has little to no relation to that of the CA itself. Hence, there is something non trivial to say about that, and these considerations will be developed in Section 2, where the two results needed for bounding block neighborhoods are stated. Proposition 2.1 is not new — although it is the first time that it is put in direct relation with block decomposition — but Corollary 2.2 and Proposition 2.3 are.

A last caveat: while this article is written in a purely classical perspective, everything it deals with also has to do with quantum CAs (QCAs). The definition

of QCAs we are dealing with was introduced in [SW04] as the natural extension of the usual definition of CAs to a universe ruled by reversible quantum laws. It is founded on the same principles that rule usual CAs: discrete space-time, translation invariance, locality; in particular, QCAs have a similar notion of neighborhood. It was already proven in that first article that reversible CAs can be naturally embedded into a quantum setting, turning them into QCAs. However, curiously enough, the neighborhood of these QCAs — the quantum neighborhood — was not shown to be equal to that of the original CAs; rather, a nontrivial bound was given (which is to be found as Proposition 2.1 of the present article). It was then made explicit in [ANW08] that the quantum neighborhood can indeed, and typically will, be strictly larger than the original one.

The authors tried to translate into purely classical terms a definition of the quantum neighborhood of quantized reversible CAs, and found the expression of Proposition 1.5, before realizing the close connection to block structures. In retrospect, the link is hardly surprising, since a construction was given in [ANW] that uses auxiliary space to write a CA in a block structure, where each block acts on exactly the quantum neighborhood — the construction is given in the quantum case, but applies to the classical case, mutatis mutandis. Notions such as semicausality (Definition 1.3) and semilocalizability (Definition 1.4) are also imported from the quantum world, cf. [ESW02].

So, in good conscience, the block neighborhood could be called the quantum neighborhood, but since in the final version no explicit reference to the quantum model needs to be made, the name sounded a bit silly. Nevertheless, if other natural neighborhoods were to be defined in relation to block structures, let it be said that the neighborhood we define and study in this article will always deserve "quantum" as a qualifier.

Notations

- Σ is the alphabet.
- $a.b$ denotes the concatenation of words a and b.
- $a|_X$ is the restriction of word a on a subset of indices X.
- $a = b|_X$ means that words a and b coincide on X.
- $\bar{X}$ denotes the complement of X, usually in $\mathbb{Z}$.
- For $A, B \subseteq \mathbb{Z}$, $A + B$ is their Minkowski sum $\{a + b \mid a \in A, b \in B\}$; similarly with $A - B$.
- $[\![x; y]\!]$ is the integer interval $[x; y] \cap \mathbb{Z}$.
- fg denotes the composition of CAs f and g.
- ffl denotes the operation reversing the order in a tuple : $\mathrm{ffl}(x_1, x_2, \ldots, x_n) = (x_n, x_{n-1}, \ldots, x_1)$. It acts similarly on $\Sigma^{\mathbb{Z}}$ by $\mathrm{ffl}(a)_n = a_{-n}$.

1. Definitions

Definition 1.1. For a bijection f whose domain and range are written as products, its dual is defined by $\tilde{f} = \mathrm{ffl} f^{-1} \mathrm{ffl}$. This applies in particular to the case where f is a CA. In this case $\tilde{f}$ is the conjugation of f by the central symmetry.

For instance, shifts are self-dual. Clearly, $f \mapsto \tilde{f}$ is an involution. In the remainder of this article, each time a notion (like a function or a property) is defined in term of a CA f, its dual, denoted by adding a tilde, is defined in the same way in term of $\tilde{f}$.

Definition 1.2. The (classic) neighborhood $\mathcal{N}(f)$ is the smallest subset A of $\mathbb{Z}$ such that $v|_A$ determines $f(v)|_0$.

The dual neighborhood $\tilde{\mathcal{N}}$ is thus defined by $\tilde{\mathcal{N}}(f) = \mathcal{N}(\tilde{f})$. The following two definitions are imported from [ESW02], where they are shown to be equivalent in the quantum case.

Definition 1.3. A function $f : A \times B \to C \times D$ is semicausal if its projection C depends only on A, i.e. if there exists $g : A \to C$ such that $f(a, b)_C = g(a)$.

Definition 1.4. A bijection $f : A \times B \to C \times D$ is (reversibly) semilocalizable if there exists a seevit E and bijections $g : A \to C \times E$ and $h : D \to B \times E$ such that $f(a, b) = (g_C(a), \tilde{h}(g_E(a), b))$, as illustrated in Figure 4.

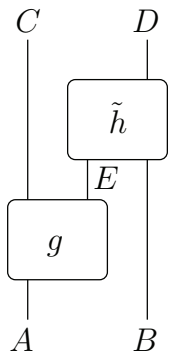

Figure 4: a semilocalizable bijection

Semilocalizability is, as the name suggests, an asymmetric property, in the sense that applying a symmetry on Figure 4 along a vertical axis, i.e. swapping A with B and C with D, breaks the semilocalizability. However, a transformation that preserves the property is the central symmetry, which corresponds to taking the dual of f: the notion of semilocalizability is self-dual.

Proposition 1.5. *$f : A \times B \to C \times D$ is semilocalizable if and only if the three following conditions are met:*

(1) *f is semicausal;*
(2) *$\tilde{f}$ is semicausal;*
(3) *for every $a, a' \in A$ and $b, b' \in B$, if $f(a, b)_D = f(a', b)_D$ then $f(a, b')_D = f(a', b')_D$.*

Proof. Suppose f is semilocalizable. Then obviously from Figure 4 both f and $\tilde{f}$ are semicausal. Let $a, a' \in A$ and $b, b' \in B$ such that $f(a, b)_D = f(a', b)_D$. That means $h^{-1}(b, g_E(a)) = h^{-1}(b, g_E(a'))$ therefore $g_E(a) = g_E(a')$, and it follows immediately $f(a, b')_D = f(a', b')_D$.

Suppose now conditions (1), (2), (3) are met. Let $\sim_A$ be the binary relation on A defined by $a \sim_A a'$ iff $\forall b \in B\ f(a, b) = f(a', b)$. Note that because of (3) this is

equivalent to $\exists b \in B\ f(a,b) = f(a',b)$ (except if $B = \varnothing$, which is too trivial a case to worry about), from which we deduce

$$\forall c, c' \in C\ \forall d \in D \quad \tilde{f}(d,c) \sim_A \tilde{f}(d,c') \tag{1.1}$$

It is clearly an equivalence relation, so using the fact that f is semicausal we can define $g : A \to C \times (A/\sim_A)$ by $g(a) = (f(a,b)_C, [a])$, where b is an arbitrary element of B and $[a]$ is the class of a in $A/\sim_A$. One can define dually $\sim_D$ on D and define $h : D \to B \times (D/\sim_D)$ by $h(d) = (\tilde{f}(d,c)_B, [d])$.

It remains to be proven that $\alpha : \begin{pmatrix} A/\sim_A & \to & D/\sim_D \\ [a] & \mapsto & [f(a,b)_D] \end{pmatrix}$ is a well-defined bijection. To prove that it is well-defined, we need to show that for every $a, a' \in A$ such that $a \sim_A a'$ and every $b, b' \in B$, $f(a,b)_D \sim_D f(a',b')_D$, which is easily done in two small steps. First, by definition of $\sim_A$, $f(a,b)_D = f(a',b)_D$. Then, by the dual of (1.1), $f(a',b)_D \sim_D f(a',b')$. We now prove that α is bijection by showing that its inverse is its dual, defined by $\tilde{\alpha}([d]) = [\tilde{f}(d,c)_A]$, so that $\tilde{\alpha}\alpha([a]) = [\tilde{f}(f(a,b)_D, c)_A]$. Since this value is independent of c, we can try in particular with $c = f(a,b)_C$, where it is clear that we get $[a]$. ∎

Definition 1.6. For a CA f on the alphabet Σ and X, Y two subsets of $\mathbb{Z}$, let $\mathbf{Q}_X^Y(f)$ be the property: "f seen as a function from $\Sigma^X \times \Sigma^{\bar{X}}$ to $\Sigma^Y \times \Sigma^{\bar{Y}}$ is semilocalizable".

Some property are obvious from the definition of semilocalizability, especially from Figure 4. Let us give two basic examples.

Lemma 1.7. *If $\mathbf{Q}_X^Y(f)$ holds, then so does $\mathbf{Q}_{X'}^{Y'}(f)$ for every $X' \supseteq X$ and $Y' \subseteq Y$.*

- For a CA seen as a function from $\Sigma^X \times \Sigma^{\bar{X}}$ to $\Sigma^Y \times \Sigma^{\bar{Y}}$, being semicausal means $X \supseteq Y + \mathcal{N}(f)$; the semicausality of $\tilde{f}$ means $X \supseteq Y + \tilde{\mathcal{N}}(f)$.

The following property, however, is easier to prove with Proposition 1.5 in mind.

Lemma 1.8. *If $\mathbf{Q}_X^Y(f)$ and $\mathbf{Q}_{X'}^Y(f)$, then $\mathbf{Q}_{X\cap X'}^Y(f)$.*

Proof. Let a, b be words on $X \cap X'$, and u, v words on $\overline{X \cap X'}$, and suppose $f(a.u) = f(b.u)|_{\bar{Y}}$. Let u' be the word on $\overline{X \cap X'}$ that is equal to u on $X \backslash X'$, v elsewhere. According to $\mathbf{Q}_X^Y(f)$, $f(a.u') = f(b.u')|_{\bar{Y}}$; we then conclude from $\mathbf{Q}_{X'}^Y(f)$ that $f(a.v) = f(b.v)|_{\bar{Y}}$. ∎

Not that we get immediately the following corollary from the selfduality of semilocalizability: if $\mathbf{Q}_X^Y(f)$ and $\mathbf{Q}_X^{Y'}(f)$, then $\mathbf{Q}_X^{Y\cup Y'}(f)$.

We have now established all the properties on $\mathbf{Q}_X^Y(f)$ required to define the block neighborhood.

Definition 1.9. The block neighborhood $\mathcal{BN}(f)$ of f is the smallest X such that $\mathbf{Q}_X^{\{0\}}(f)$ holds.

The word "neighborhood" is not gratuitous. In fact, $\mathbf{Q}_X^Y(f)$ behaves exactly like "X includes the neighborhood of Y for some CA f' such that $\mathcal{N}(f') = \mathcal{BN}(f)$", as stated in the next lemma. The idea is that $\mathcal{BN}$ characterizes a notion of dependency that is very similar to the usual one characterized by $\mathcal{N}$.

Lemma 1.10. *$\mathbf{Q}_X^Y(f)$ is equivalent to $X \supseteq Y + \mathcal{BN}(f)$.*

Proof. Suppose $X \supseteq Y + \mathcal{BN}(f)$. By translation invariance, for all $y \in Y$, we have $\mathbf{Q}^{\{y\}}_{\{y\}+\mathcal{BN}(f)}(f)$, which, according to Lemma 1.7, implies $\mathbf{Q}^{\{y\}}_{X}(f)$. Invoking now the dual of Lemma 1.8, we get $\mathbf{Q}^{Y}_{X}(f)$.

For the reciprocal, suppose now $\mathbf{Q}^{Y}_{X}(f)$. According to Lemma 1.7, we have, for every $y \in Y$, $\mathbf{Q}^{\{y\}}_{X}(f)$; but that is, by definition of $\mathcal{BN}$, equivalent to $X \supseteq \{y\} + \mathcal{BN}(f)$, so we must have $X \supseteq Y + \mathcal{BN}(f)$. ∎

So, the block neighborhood is just one kind of neighborhood. However, $\mathcal{BN}$ has by contruction one property that $\mathcal{N}$ does not share: it is self-dual. It is not enough to make interesting, and many questions are left open at this point. We just know $\mathcal{BN} \supseteq \mathcal{N} \cup \tilde{\mathcal{N}}$, but do we have a lower bound on $\mathcal{BN}$? Is it always finite? The answer is in Corollary 2.2. How do the block neighborhoods compose? It can be easily inferred from Figure 4 that $\mathcal{BN}(gf) \subseteq \mathcal{BN}(g) + \mathcal{BN}(f)$, which is certainly good news, but Proposition 2.3 provides much more interesting bounds.

2. Main theorem

Proposition 2.1. $\mathcal{BN} \subseteq \mathcal{N} - \mathcal{N} + \tilde{\mathcal{N}}$.

Sanity check: $\mathcal{N} - \mathcal{N} + \tilde{\mathcal{N}}$ contains indeed $\mathcal{N}$ because $\mathcal{N} \cap \tilde{\mathcal{N}} \neq \varnothing$, which follows from $\{0\} = \mathcal{N}(ff^{-1}) \subseteq \mathcal{N}(f) - \tilde{\mathcal{N}}(f)$.

Proof. The proof of this proposition can be essentially found in [SW04], where the result is stated as Lemma 4, albeit in a foreign formalism. Another avatar of the proposition and its proof can be found in the form of Lemma 3.2 of [AN08]. In order to keep this article self-contained, we give yet another proof.

Let us then prove $\mathbf{Q}^{\{0\}}_{\mathcal{N}(f)-\mathcal{N}(f)+\tilde{\mathcal{N}}(f)}(f)$. Let a, b be words on $\mathcal{N}(f) - \mathcal{N}(f) + \tilde{\mathcal{N}}(f)$ and u, v words on its complement such that $f(a.u) = f(b.u)|_{\overline{\{0\}}}$. Applying f^{-1} to that equality we get $a.u = b.u|_{\overline{\tilde{\mathcal{N}}(f)}}$, which implies of course $a.v = b.v|_{\overline{\tilde{\mathcal{N}}(f)}}$, from which we obtain $f(a.v) = f(b.v)|_{\overline{-\mathcal{N}(f)+\tilde{\mathcal{N}}(f)}}$. On the other hand, $f(w)|_{-\mathcal{N}(f)+\tilde{\mathcal{N}}(f)}$ is a function of $w|_{\mathcal{N}(f)-\mathcal{N}(f)+\tilde{\mathcal{N}}(f)}$, so $f(a.u) = f(a.v)|_{-\mathcal{N}(f)+\tilde{\mathcal{N}}(f)}$ and $f(b.u) = f(b.v)|_{-\mathcal{N}(f)+\tilde{\mathcal{N}}(f)}$, which in the end proves $f(a.v) = f(b.v)|_{\overline{\{0\}}}$. ∎

Rather surprisingly, this bound is not self-dual, which allows us to reinforce it immediately.

Corollary 2.2. $\mathcal{BN} \subseteq (\mathcal{N} - \mathcal{N} + \tilde{\mathcal{N}}) \cap (\tilde{\mathcal{N}} - \tilde{\mathcal{N}} + \mathcal{N})$.

Proposition 2.3. *Let $f_1, \dots f_n$ be reversible CAs. Then*

$$\mathcal{BN}(f_n \cdots f_1) \subseteq \bigcup_{k=1}^{n} \left(\tilde{\mathcal{N}}(f_n \cdots f_{k+1}) + \mathcal{BN}(f_k) + \mathcal{N}(f_{k-1} \cdots f_1) \right).$$

This formula could seem at first glance not to be self-dual, and therefore obviously suboptimal, but there is more to the duality than just putting and removing tildes. Since $\widetilde{fg} = \tilde{g}\tilde{f}$, we have $\widetilde{\mathcal{BN}}(f_n \cdots f_1) = \mathcal{BN}(\tilde{f}_1 \cdots \tilde{f}_n)$; it is from here straightforward to check that the formula is indeed self-dual.

Proof. Let $\mathcal{V} = \bigcup_{k=1}^{n} \left(\tilde{\mathcal{N}}(f_n \cdots f_{k+1}) + \mathcal{BN}(f_k) + \mathcal{N}(f_{k-1} \cdots f_1) \right)$; we have to prove $\mathbf{Q}^{\{0\}}_{\mathcal{V}}(f)$. Let a, b be words on $\mathcal{V}$, u, v words on $\bar{\mathcal{V}}$, and assume $f_n \cdots f_1(a.u) = f_n \cdots f_1(b.u)|_{\overline{\{0\}}}$.

For $k \in [\![0;n]\!]$, let $\mathcal{C}_k = \tilde{\mathcal{N}}(f_n \cdots f_{k+1})$; for $k \in [\![1;n]\!]$, let $\mathcal{K}_k = \mathcal{C}_k + \mathcal{BN}(f_k)$ and $\mathcal{D}_k = \mathcal{N}(f_{k-1} \cdots f_1)$. For $k \in [\![1;n]\!]$, let $\mathcal{V}_k = \mathcal{K}_k + \mathcal{D}_k$; by definition, $\mathcal{V} = \bigcup_{k=1}^{n} \mathcal{V}_k$.

We will prove by induction the following hypothesis $(\mathcal{H}_k)$ for $k \in [\![0;n]\!]$:

- $f_k \cdots f_1(a.u) = f_k \cdots f_1(b.u)|_{\overline{\mathcal{C}_k}}$ and
- $f_k \cdots f_1(a.v) = f_k \cdots f_1(b.v)|_{\overline{\mathcal{C}_k}}$.

Since we already know $a.u = b.u|_{\overline{\mathcal{C}_0}}$, it follows immediately $a.v = b.v|_{\overline{\mathcal{C}_0}}$, so $(\mathcal{H}_0)$ is true.

Suppose $(\mathcal{H}_k)$ for some $k \in [\![0;n-1]\!]$. Let $a' = f_k \cdots f_1(a.u)|_{\mathcal{K}_{k+1}}$ and $b' = f_k \cdots f_1(b.u)|_{\mathcal{K}_{k+1}}$; since $\mathcal{K}_{k+1} + \mathcal{D}_{k+1} \subseteq \mathcal{V}$, a' and b' are respectively equal to $f_k \cdots f_1(a.v)|_{\mathcal{K}_{k+1}}$ and $f_k \cdots f_1(b.v)|_{\mathcal{K}_{k+1}}$. Let us define $u' = f_k \cdots f_1(a.u)|_{\overline{\mathcal{K}_{k+1}}}$ and $v' = f_k \cdots f_1(a.v)|_{\overline{\mathcal{K}_{k+1}}}$. We have

$$\mathcal{C}_k = \tilde{\mathcal{N}}(f_n \cdots f_{k+1}) \subseteq \tilde{\mathcal{N}}(f_n \cdots f_{k+2}) + \tilde{\mathcal{N}}(f_{k+1}) \subseteq \mathcal{C}_{k+1} + \mathcal{BN}(f_{k+1}) = \mathcal{K}_{k+1}.$$

We can therefore deduce from $(\mathcal{H}_k)$ that u' and v' are respectively equal to $f_k \cdots f_1(b.u)|_{\overline{\mathcal{K}_{k+1}}}$ and $f_k \cdots f_1(b.v)|_{\overline{\mathcal{K}_{k+1}}}$. By definition of $\mathcal{C}_{k+1}$, since $f_n \cdots f_1(a.u) = f_n \cdots f_1(b.u)|_{\overline{\{0\}}}$, we have $f_k \cdots f_1(a.u) = f_k \cdots f_1(b.u)|_{\overline{\mathcal{C}_k}}$, which is the first point of $(\mathcal{H}_{k+1})$. Since $\mathcal{K}_{k+1} = \mathcal{C}_{k+1} + \mathcal{BN}(f_{k+1})$, according to Lemma 1.10, we have $\mathbf{Q}_{\mathcal{K}_{k+1}}^{\mathcal{C}_{k+1}}(f_{k+1})$. We therefore deduce the second point of $(\mathcal{H}_{k+1})$.

So in the end we get $(\mathcal{H}_n)$, which concludes the proof because $\mathcal{C}_n = \{0\}$. ∎

Corollary 2.4. *Suppose $\mathcal{N}(f) \subseteq [\![-\alpha;\beta]\!]$ and $\tilde{\mathcal{N}}(f) \subseteq [\![-\gamma;\delta]\!]$. Then $\mathcal{BN}(f^k) \subseteq [\![-(k+1)\max(\alpha,\gamma) - \min(\beta,\delta)\,;(k+1)\max(\beta,\delta) + \min(\alpha,\gamma)]\!]$.*

For $X \subseteq \mathbb{R}$, let X^* be its convex hull and for $\lambda \in \mathbb{R}$, $\lambda X = \{\lambda x \mid x \in X\}$. We get, for any reversible CA, the asymptotic relation $\lim_{k\to+\infty} \frac{1}{k}\mathcal{BN}(f^k)^* \subseteq \mathcal{N}(f)^* \cup \tilde{\mathcal{N}}(f)^*$. Let us assume we are in the case $\lim_{k\to+\infty} \frac{1}{k}\mathcal{N}(f^k)^* = \mathcal{N}(f)^*$ and $\lim_{k\to+\infty} \frac{1}{k}\tilde{\mathcal{N}}(f^k)^* = \tilde{\mathcal{N}}(f)^* \cup \tilde{\mathcal{N}}(f)^*$. Then what this means informally is that condition (3) in Proposition 1.5 applied to f^k becomes less restrictive as k grows, and fades at the limit.

It is interesting to note the relation with Kari's constructions in [Kar96] and [Kar99]. We will briefly discuss the latter; it is of course stated in dimension 2, but that is not an obstacle to comparison, as the same construction can be made in dimension 1, or our analysis generalized to dimension 2 (cf. section 3.2). Let us place ourselves in dimension 1. Let f be a CA whose neighborhood and dual neighborhood are both included in $[\![-1;1]\!]$. In this case, Corollary 2.4 implies $\mathcal{BN}(f^k) \subseteq [\![-(k+2);k+2]\!]$. Kari proves that there is an embedding φ and a CA g such that $f = \varphi g \varphi^{-1}$, where g fulfills by construction $\mathcal{BN}(g) \subseteq [\![-1;1]\!]$. Kari's construction therefore contains an asymptotically optimal bound on $\mathcal{BN}(f^k)$.

Corollary 2.5. *If the neighborhoods and dual neighborhoods of f and g are included in $[\![-n;n]\!]$, then $\mathcal{BN}(fg) \subseteq [\![-4n;4n]\!]$.*

The contraposition is actually more interesting. Consider h, whose neighborhood and dual neighborhood are both included in $[\![-n;n]\!]$; its block neighborhood has to be contained in $3[\![-n;n]\!]$. It seems perfectly reasonable to assume that h could be a composition of two more elementary reversible cellular automata f and g having strictly smaller neighborhoods, containing $\frac{1}{2}[\![-n;n]\!]$ but close to it. Actually, if no restriction is imposed on the behaviour of f^{-1} and g^{-1}, maybe even allowing f

and g to be nonreversible, it is certainly possible to decompose h in such a way by increasing the size of the alphabet. However, if the dual neighborhoods of f and g are also required to be close to $\frac{1}{2}[\![-n;n]\!]$, then such a decomposition will not be possible if $\mathcal{BN}(h)$ is too large. For instance, if $\mathcal{BN}(h)$ is not contained in $\frac{5}{2}[\![n;n]\!]$, then $\mathcal{N}(f)$, $\tilde{\mathcal{N}}(f)$, $\mathcal{N}(g)$ and $\tilde{\mathcal{N}}(g)$ cannot all be included in $\frac{5}{8}[\![-n;n]\!]$. In this sense, h can be considered "elementary".

3. Remarks

We gather in this section several unrelated observations about the block neighborhood.

3.1. Subtraction Automata

Suppose Σ can be provided with a binary operation $\cdot - \cdot$ such that:

- there exists an element of Σ denoted 0 such that $x = y$ is equivalent to $x - y = 0$;
- f is an endomorphism of $(\Sigma^{\mathbb{Z}}, -)$, where $-$ is defined component-wise on $\Sigma^{\mathbb{Z}}$.

We say in this case f admits a subtraction. For instance, linear automata as defined in [GNW10] admit subtractions.

Proposition 3.1. *Automata with subtractions have minimal block neighborhoods. In other words, for any automaton f admitting a subtraction, $\mathcal{BN}(f) = \mathcal{N}(f) \cup \tilde{\mathcal{N}}(f)$.*

Proof. Let A be any subset of $\mathbb{Z}$, a, b be words on A, u, v words on $\bar{A}$, and suppose $f(a.u) = f(b.u)$. Then $f(a.v) - f(b.v) = f(a.v - b.v) = f((a-b).0) = f(a.u - b.u) = f(a.u) - f(b.u) = 0$. ∎

3.2. Generalization

We can actually drop many properties of the CAs that are irrelevant to the notions developed in this article. We don't need translation invariance. We don't need the alphabet to be finite. We don't need the neighborhoods to be finite. We don't need the domain and range cell structures to be identical. In this abstract setting, a "reversible automaton" is a bijection from $\prod_{i\in I} X_i$ to $\prod_{j\in J} Y_j$ and $\mathcal{N}(f)$ is a function from $\mathcal{P}(J)$ to $\mathcal{P}(I)$ which to $B \subseteq J$ associates the minimal subset A of I such that $f(x)|_B$ depends only on $x|_A$. In general, a function $\alpha : \prod_{i\in I} X_i \to \prod_{j\in J} Y_j$ is a *neighborhood scheme* if for all Y, $\alpha(Y) = \bigcup_{X\subseteq Y} \alpha(X)$; $\mathcal{N}(f)$ is of course one example of a neighborhood scheme. The usual definition of the neighborhood in the case of a cellular automaton corresponds here to $\mathcal{N}(f)(\{0\})$. Any function $\alpha : \mathcal{P}(J) \to \mathcal{P}(I)$ has a transpose $\alpha^\dagger : \mathcal{P}(I) \to \mathcal{P}(J)$ defined by $\alpha^\dagger(A)$ being the largest subset B of J such that $\alpha(B) \subseteq A$. We have indeed $(\alpha^\dagger)^\dagger = \alpha$, and for usual one-dimensional CAs, † corresponds to $\mathcal{N} \mapsto -\mathcal{N}$.

There is not anymore any good notion of duality on automata, but $\tilde{\mathcal{N}}(f)$ can be defined as $\mathcal{N}^\dagger(f^{-1})$. Of course the definition of $\mathcal{BN}(f)$ cannot make any reference to 0, instead $\mathcal{BN}(f)(B)$ is now the smallest subset of I fulfilling $\mathbf{Q}_A^B(f)$. The self-duality of $\mathcal{BN}$ is of course still valid. Lemmas 1.7 and 1.8 state respectively that $\mathcal{BN}$ is well-defined and that it is a neighborhood scheme.

Lemma 1.10 (used once at the end of the proof of Proposition 2.3) becomes "$\mathbf{Q}_X^Y(f)$ is equivalent to $X \supseteq \bigcup_{y\in Y} \mathcal{BN}(f)(Y)$", which is precisely the definition of $\mathcal{BN}$; it can therefore be forgotten, as the triviality it is now. Proposition 2.1 becomes $\mathcal{BN} \subseteq \mathcal{N} \circ \mathcal{N}^\dagger \circ \tilde{\mathcal{N}}$, Corollary 2.2 changes accordingly, and Proposition 2.3 remains true when "+" is substituted with "$\circ$". It follows that indecomposability results such as Corollary 2.5 are extremely robust: they cannot be overcome by increasing the size of the alphabet or relaxing the translational invariance. It also shows of course the limitations of this method, namely that it is utterly unable to exploit these parameters.

3.3. Optimality

The bounds presented in Corollary 2.2 and Proposition 2.3 seem peculiar enough as to be suspect of non-optimality. However, we have been unable to come up with a better approximation, and would rather tend to think that they cannot be improved. We will concentrate on Corollary 2.2 alone, whose optimality is conjectured in the following statement.

Conjecture 3.2. For any subsets X, Y and Z of $\mathbb{Z}$ such that $X \cup Y \subseteq Z \subseteq (X-X+Y)\cap(Y-Y+X)$, if there exists a CA f such that $\mathcal{N}(f) = X$ and $\tilde{\mathcal{N}}(f) = Y$, then there exists a CA g such that $\mathcal{N}(g) = X$, $\tilde{\mathcal{N}}(g) = Y$ and $\mathcal{BN}(g) = Z$.

This section will be devoted to proving the following weaker version:

Proposition 3.3. *Conjecture 3.2 is true when $Z \subseteq \{2y - x \mid x, y \in X \cap Y\}$. In particular it is true if X and Y are equal intervals.*

Proof. Given that there is by hypothesis a CA f such that $\mathcal{N}(f) = X$ and $\tilde{\mathcal{N}}(f) = Y$, we only need to prove that for every $z \in Z$ there exists a CA g_z such that $\mathcal{N}(g_z) \subseteq X$, $\tilde{\mathcal{N}}(g_z) \subseteq Y$ and $z \in \mathcal{N}(g_z) \subseteq Z$. Then the proposition is proven by considering the direct sum of f and all these g_z's.

The Toffoli automaton presented in [ANW08] (definition 12), defined by $\Sigma = (\mathbb{Z}/2\mathbb{Z})^2$ and $T(v)_0 = (v_0^2 + v_0^1 v_1^1, v_1^1)$, will serve as the basic constructing tool for g_z. Its inverse is given by $T^{-1}(v)_0 = \left(v_{-1}^2, v_0^1 + v_{-1}^2 v_0^2\right)$, so we clearly have $\mathcal{N}(T) = \tilde{\mathcal{N}}(T) = \{0; 1\}$. Let us prove $\mathcal{BN}(T) = [\![0; 2]\!]$, by proving first that $\mathbf{Q}_{\mathbb{N}}^{\mathbb{N}}(T)$ is true, and then that $\mathbf{Q}_{\{0;1\}}^{\{0\}}(T)$ is false. Let then a, b be words on $\mathbb{N}$ and u, v words on its complement, and suppose $T(a.u) = T(b.u)_{\mathbb{N}}$. In particular, $T(a.u)_{-1}^2 = T(b.u)_{-1}^2$, which implies $a_0^1 = b_0^1$, so we get immediately $T(a.v) = T(b.v)_{\mathbb{N}}$, which proves $\mathbf{Q}_{\mathbb{N}}^{\mathbb{N}}(T)$. Consider now the words $a = (0,0)(0,0)$ and $b = (0,0)(1,1)$ on $\{0; 1\}$, and u, v the words on its complement that are $(0,0)$ everywhere except in position 2, where $u_2 = (1,0)$. We have $T(a.u) = T(b.u)_{\overline{\{0\}}}$ but $T(a.v)_1 = (0,0)$ while $T(b.v)_1 = (1,0)$, therefore $\mathbf{Q}_{\{0;1\}}^{\{0\}}(T)$ is false.

This CA can be obviously expanded into an automaton T_l such that $\mathcal{N}(T_l) = \tilde{\mathcal{N}}(T_l) = \{0; l\}$ and $\mathcal{BN}(T_l) = \{0; l; 2l\}$.

More generally, for any nonempty intervals X and Z of $\mathbb{Z}$ such that $X \subseteq Z \subseteq X - X + X$, there is a CA f such that $\mathcal{N}(f) = \tilde{\mathcal{N}}(f) = X$ and $\mathcal{BN}(f) = Z$. We can engineer such an f by considering the direct sum of several CAs. First, for each element $x \in X$, consider the shift by $-x$: the sum of all these shifts is a CA g such that $\mathcal{N}(g) = \tilde{\mathcal{N}}(g) = \mathcal{BN}(g) = X$. Then, for each element $z \in Z$, choose x and y in

$X \cap Y$ such that $z = 2y - x$. The automaton $g_z = \sigma^x T_{y-x}$, where σ is the elementary shift to the left, is then such that $\mathcal{N}(T_l) = \tilde{\mathcal{N}}(T_l) = \{x; y\}$ and $\mathcal{BN}(T_l) = \{x; y; z\}$, which concludes the proof. ■

Conclusion

Of course a lot of questions remain. Are the upper bounds on the block neighborhood given in this article optimal under all circumstances? And is it possible to make these bounds more efficient by including as parameters the size of the alphabet and the requirement that the transformations be translation invariant? This would probably require a whole different technique.

Something happened in this article that is increasingly common: after a theory grows a quantum extension (in this case QCAs join the family of CAs) and new tools and techniques are invented to study the quantum setup, they come back to the classical setup (semilocalizability comes to mind, and a lot of others are disguised as combinatorial properties) and bring various insights, simpler proofs and/or new results.

The block neighborhood is nothing else than the quantum neighborhood. It shows what had been grasped until then only intuitively: whereas CAs can be defined by their local transition functions, QCAs are intrisically block-structured. In that sense, working on QCAs is a lot like working on CAs with a restricted bag of tools that includes only local permutations — duplication or destruction of information are stricly forbidden. It also means that, even staying in a purely classical framework, finding this kind of constructions is worthwhile and meaningful, even in the case where a result is already known to be attainable by another method. Not only will the construction be nicer in a purely abstract way, because it will employ only elementary means: it will also have the benefit of being immediately transposable to the quantum case.

Acknowledgements

The authors would like to thank Jarkko Kari for showing them, to their amazement, how the neighborhood and the inverse neighborhood of CAs depend so little on each other, even in the iterated dynamics. They also gratefully acknowledge the support of the Deutsche Forschungsgemeinschaft (Forschergruppe 635) and the EU (project QICS).

References

[AN08] Pablo Arrighi and Vincent Nesme. Quantization of cellular automata. In Bruno Durand, editor, *Proceedings of the First Symposium on Cellular Automata "Journées Automates Cellulaires" JAC 2008*, Exploratory paper track, pages 204–215, Uzès France, 04 2008. ISBN 978-5-94057-377-7.

[ANW] Pablo Arrighi, Vincent Nesme, and Reinhard F. Werner. Unitarity plus causality implies localizability. To appear in *Journal of Computer and System Sciences*. `arXiv:0711.3975v3`.

[ANW08] Pablo Arrighi, Vincent Nesme, and Reinhard F. Werner. One-dimensional quantum cellular automata over finite, unbounded configurations. In *Language and Automata Theory and Applications: Second International Conference, LATA 2008, Tarragona, Spain, March 13-19, 2008. Revised Papers*, pages 64–75, Berlin, Heidelberg, 2008. Springer-Verlag.

[DL01] Jérôme Durand-Lose. Representing reversible cellular automata with reversible block cellular automata. In Robert Cori, Jacques Mazoyer, Michel Morvan, and Rémy Mosseri, editors, *Discrete Models: Combinatorics, Computation, and Geometry, DM-CCG '01*, volume AA of *Discrete Mathematics and Theoretical Computer Science Proceedings*, pages 145–154, 2001.

[ESW02] T. Eggeling, Dirk Schlingemann, and Reinhard F. Werner. Semilocal operations are semilocalizable. *Europhysics Letters*, 57(6):782–788, 2002.

[GNW10] Johannes Gütschow, Vincent Nesme, and Reinhard F. Werner. The fractal structure of cellular automata on abelian groups. 2010.

[Kar90] Jarkko Kari. Reversibility of 2d cellular automata is undecidable. *Physica D*, 45(1-3):386–395, 1990.

[Kar96] Jarkko Kari. Representation of reversible cellular automata with block permutations. *Mathematical Systems Theory*, 29(1):47–61, 1996.

[Kar99] Jarkko Kari. On the circuit depth of structurally reversible cellular automata. *Fundam. Inf.*, 38(1-2):93–107, 1999.

[Mar84] Norman Margolus. Physics-like models of computation. *Physica D*, 10:81–95, 1984.

[MH89] Ken'ichi Morita and Masateru Harao. Computation universality of one-dimensional reversible (injective) cellular automata. *IEICE Transactions on Information and Systems, E*, 72:758–762, 1989.

[MU92] Ken'ichi Morita and Satoshi Ueno. Computation-universal models of two-dimensional 16-state reversible cellular automata. *IEICE Transactions on Information and Systems, E*, 75:141–147, 1992.

[SW04] Benjamin Schumacher and Reinhard F. Werner. Reversible quantum cellular automata. 05 2004. `arXiv:quant-ph/0405174`.

This work is licensed under the Creative Commons Attribution-NoDerivs License. To view a copy of this license, visit `http://creativecommons.org/licenses/by-nd/3.0/`.