A Formalisation of Algorithms for Sorting Network
Laurent Théry

To cite this version:
Laurent Théry. A Formalisation of Algorithms for Sorting Network. 2022. hal-03585618v2

HAL Id: hal-03585618
https://inria.hal.science/hal-03585618v2
Preprint submitted on 2 Mar 2022

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.
A Formalisation of Algorithms for Sorting Network

Laurent Théry
Laurent.Thery@sophia.inria.fr

Abstract

This notes explains how standard algorithms that construct sorting networks have been formalised and proved correct in the COQ proof assistant using the SSREFLECT extension.

1 Introduction

A network is composed of a number of lines. By analogy to electronic circuit, each line has an input value before entering the network and an output value when leaving the network. The building block of a network is a comparator. A comparator connects two lines

\[
\begin{array}{c}
\text{a}_1 \\
\text{a}_2
\end{array} \quad \quad \quad \quad
\begin{array}{c}
\text{a}'_1 \\
\text{a}'_2
\end{array}
\]

A connector works as follows. The output value of the upper line is the minimum of the input values, \( \text{a}'_1 = \min(\text{a}_1, \text{a}_2) \). The output value of the lower line is the maximum of the two lines, \( \text{a}'_2 = \max(\text{a}_1, \text{a}_2) \).

A network is a collection of connectors. Here, we are interested into networks that sort their inputs, i.e. they return sorted outputs. An example of a network that sorts 3 inputs is the following
Whatever the initial values $a_1$, $a_2$ and $a_3$ are, we have $a'_1 \leq a'_2 \leq a_3$. In the rest of the paper we are interested in proving the correctness of some recursive algorithms that build sorting network. We first explain how we have formalised networks. Then, we present 3 algorithms:

- an algorithm that builds the bitonic sorting network;

- an algorithm that builds the odd-even merge sorting network;

- an algorithm that builds the odd-even exchange sorting network.

2 The formalisation

In the formalisation, we are using material that comes from the Mathematical Component Library. In order to make the presentation understandable by someone not familiar with this library, we summarize in the appendices A, B, C and D the notions that have been used for this formalisation.

To represent the state of lines, we are using the tuple type and are working on an arbitrary orderedType $A$. So if the network has $m$ lines, the state of lines is represented by a $m$-tuple $A$. We allow connectors to work simultaneously on several disjoint pairs of lines. If we consider the following sequence composed of 3 connectors

$$
\begin{align*}
& a_1 & a'_1 \\
& a_2 & a'_2 \\
& a_3 & a'_3 \\
& a_4 & a'_4 \\
\end{align*}
$$
the first two are independent so can be performed in parallel while the third one must be kept separated as it shares some lines with the previous two. Making the parallelism explicit, we get the following drawing with only 2 connectors.

```
\begin{tikzpicture}
  \draw (0,0) -- (2,0) -- (2,2) -- (0,2) -- (0,0);
  \draw (2,0) -- (4,0) -- (4,2) -- (2,2) -- (2,0);
  \draw (0,2) -- (2,2);
  \draw (2,2) -- (4,2);
  \node at (0,0) {$a_1$};
  \node at (2,0) {$a_1'$};
  \node at (0,2) {$a_2$};
  \node at (2,2) {$a_2'$};
  \node at (0,4) {$a_3$};
  \node at (2,4) {$a_3'$};
  \node at (0,6) {$a_4$};
  \node at (2,6) {$a_4'$};
\end{tikzpicture}
```

A connector is then encoded as a record that contains a function \( \text{clink} \) that takes a line (an element of \( I_m \)) and returns its associated line. The function is the identity for lines that are not connected. The requirement of the lines to be associated in disjoint pairs is encoded in the \( \text{cfinv} \) field which asks for \( \text{clink} \) to be involutive. A network is then a list of connectors.

```latex
Record connector (m : nat) := connector_of {
  clink : {ffun I_m => I_m};
  cfinv : [forall i, clink (clink i) == i]
}. 

Definition network := seq (connector m).
```

An example of such a connector is the one that swaps the value of two line \( i \) and \( j \). Its definition is done in three steps. We first define the link function, we prove that it is involutive, and we finally build the connector.

```latex
Definition clink_swap (i j : I_m) : {ffun I_m => I_m} :=
  [ffun x => if x == i then j else if x == j then i else x].
Lemma clink_swap_proof (i j : I_m):
  [forall k, clink_swap i j (clink_swap i j k) == k].
Definition cswap i j := connector_of (clink_swap i j).
```
In the following, a variable $c$ always represents a connector, $n$ a network, $s$ a sequence and $t$ a tuple. The first operation on connector and network is the one that computes output values. The function $cfun$ applies a connector $c$ to a tuple $t$ and the function $nfun$ applies a network $n$ to a tuple $t$.

### Definition

\[
\text{Definition } cfun c t :=
\begin{align*}
\text{tuple if } & i \leq \text{clink } c i \\
& \text{then min } (\text{tnth } t i)(\text{tnth } t(\text{clink } c i)) \\
& \text{else max } (\text{tnth } t i)(\text{tnth } t(\text{clink } c i)) \mid i < m
\end{align*}
\]

### Definition

\[
\text{Definition } nfun n t := \text{foldl } (\text{fun } t c => cfun c t) t n.
\]

The function $cfun$ performs the swap between values of connected lines, while $nfun$ simply iterates the application of $cfun$.

The first obvious property of connector and network is that they only permute their outputs. This is proved by the following theorems

### Lemma

\[
\text{Lemma } \text{perm}_c c t : \text{perm}_eq (cfun c t) t.
\]

\[
\text{Lemma } \text{perm}_n n t : \text{perm}_eq (nfun n t) t.
\]

Another interesting property is the regularity with respect to the order. If we take two arbitrary ordered types $A$ and $B$ and $f$ a function from $A$ to $B$ that behaves well with the order ($f x \leq_B f y$ iff $x \leq_A y$) we have the following properties for $\min$ and $\max$:

### Lemma

\[
\text{Lemma } \text{min}_homo (x y : A) : f (\text{min } x y) = \text{min } (f x) (f y).
\]

\[
\text{Lemma } \text{max}_homo (x y : A) : f (\text{max } x y) = \text{min } (f x) (f y).
\]

These properties can then be easily lifted at the level of connector and network.

### Definition

\[
\text{Definition } tmap f t := [\text{tuple } f (\text{tnth } t i) \mid i < m].
\]

\[
\text{Lemma } \text{tmap\_connector} c (t : m.-\text{tuple } A) : tmap f (cfun c t) = cfun c (tmap f t).
\]

\[
\text{Lemma } \text{tmap\_network} n (t : m.-\text{tuple } A) : tmap f (nfun n t) = nfun n (tmap f t).
\]

We are now ready to define the notion of sorting network. It is defined as a qualifier so we express the fact the $n$ is a sorting network by the expression
"n is sorting". Thanks to the regularity with respect to the order, we can limit the definition of being a sorting network to the one of sorting all the boolean tuples. As, if we consider m lines, there are only a finite number of such tuples (2^m to be precise), this property is decidable and can be encoded as a boolean.

\begin{verbatim}
Definition sorting :=
[qualify n | [forall r : m.-tuple bool, sorted <= (nfun n r)]].
\end{verbatim}

We now need to show that this encoding covers exactly the usual notion of sorting network. If we consider an arbitrary ordered type A, a network is sorting if and only if it sorts all the tuples of elements of A. This is known as the zero-one principle. One direction is straightforward. If there is at least two elements in A sorting all the tuples in A implies our definition.

\begin{verbatim}
Lemma sorted_sorting n (x1 x2 : A):
  x1 != x2 => (forall t : m.-tuple A, sorted <= A (nfun n t)) => n is sorting.
\end{verbatim}

Given a boolean tuple t, if we consider the function f from boolean to A that returns min x1 x2 on false and max x1 x2 on true. Applying f on the tuple t1 gives us a tuple t1 of elements of A. If we apply n of t1, it returns a sorted tuple t2. Now, if we consider g from A to bool defined as g x = false if x <= min x1 x2 and true otherwise. It is easy to show that g behaves well with the orders and is the left inverse of f (we have g (f b) = b), so tmap g t2 is the result of applying the network n to t and is sorted.

Conversely, we have to reason by contradiction.

\begin{verbatim}
Lemma sorting_sorted n (t : m.-tuple A): n is sorting => sorted <= A (nfun n t)).
\end{verbatim}

Let us take an arbitrary tuple t of elements of A. Applying the network n on t gives a tuple t1. Suppose that t1 is not sorted. This means that there exists an i such that t1[i] > t1[i + 1]. If we consider h from A to bool that returns false to elements strictly smaller than t1[i] and true otherwise. Again, h behaves well with the orders. So, tmap h t is a boolean tuple t whose application to n gives tmap h t1 which is not sorted by construction. This
is in contradiction with our assumption of \( n \) being a sorting network, so \( t_1 \) must be sorted.

Now, we are ready to build sorting networks. We first need building blocks. A key block is the one that glues together two networks: given a network \( n_1 \) with \( m_1 \) lines and a network \( n_2 \) with \( m_2 \) lines, it creates a network with \( m_1 + m_2 \) lines that behaves like \( n_1 \) on the top lines and \( n_2 \) on the bottom lines. There are different ways to do this. We favour the one that tries to fuse together connectors. This is the one that will be handy for building our sorting network later. So, at connector level, we have a connector \( c_1 \) with \( m_1 \) lines and a connector \( c_2 \) with \( m_2 \) lines and we want to build a connector of \( m_1 + m_2 \) lines. The first step is to build the associated \( \text{clink} \). This requires some surgery with ordinals. Then, we need to prove that this new \( \text{clink} \) is involutive and we finally get our \( \text{cmerge} \) operation.

\[
\text{Definition } \text{clink}_\text{merge} \ m_1 \ m_2 \ (c_1 : \text{connector } m_1) \ (c_2 : \text{connector } m_2) :=
\text{fun } i \Rightarrow \text{match } \text{split } i \text{ with } \\
| \text{inl } x \Rightarrow \text{lshift } (_ (\text{clink } c_1 \ x)) \\
| \text{inr } x \Rightarrow \text{rshift } (_ (\text{clink } c_2 \ x)) \\
\text{end}.
\]

\[
\text{Lemma } \text{clink}_\text{merge}_\text{proof} \ m_1 \ m_2 \ (c_1 : \text{connector } m_1) \ (c_2 : \text{connector } m_2) :
\forall i, (\text{clink}_\text{merge} \ c_1 \ c_2) \text{ proof } (\text{clink}_\text{merge} \ c_1 \ c_2 \ i) = i.
\]

\[
\text{Definition } \text{cmerge} \ m_1 \ m_2 \ (c_1 : \text{connector } m_1) \ (c_2 : \text{connector } m_2) :=
\text{connector_of } (\text{clink}_\text{merge}_\text{proof} \ c_1 \ c_2).
\]

Lifting this to network is easier. We create the sequence of pairs of connectors of \( n_1 \) and \( n_2 \) and on each of these pairs we apply \( \text{cmerge} \).

\[
\text{Definition } \text{nmerge} \ m_1 \ m_2 \ (n_1 : \text{network } m_1) \ (n_2 : \text{network } m_2) :=
\text{seq } \text{cmerge} \ i.1 \ i.2 \ |\ i <\text{ zip } n_1 \ n_2.
\]

Note that this construction really makes sense of \( n_1 \) and \( n_2 \) have the same numbers of connectors. Otherwise the \text{zip} operation looses some connectors of the longest network. As a matter of fact, in the following, we mostly use the duplication operator that glues together two identical pieces.
Another way of gluing network is the one based on parity. Given $n_1$ and $n_2$, we build a network $n$ whose even lines are ruled by $n_1$ and the odd ones by $n_2$. We first need to introduce the division by 2 and the even and odd doubling at the level of ordinals.

\[
\text{Definition } \text{idiv2 } m : 'I_(m + m) \Rightarrow 'I_m := \\
\quad \text{if } m \text{ is } m_1 +1 \text{ then fun } i \Rightarrow \text{inZp}(i/2) \text{ else fun } i \Rightarrow i.
\]

\[
\text{Definition } \text{elift } m : 'I_m \Rightarrow 'I_(m + m) := \\
\quad \text{if } m \text{ is } m_1 +1 \text{ then fun } i \Rightarrow \text{inZp}(i*2) \text{ else fun } i \Rightarrow i.
\]

\[
\text{Definition } \text{olift } m : 'I_m \Rightarrow 'I_(m + m) := \\
\quad \text{if } m \text{ is } m_1 +1 \text{ then fun } i \Rightarrow \text{inZp}(i*2 +1) \text{ else fun } i \Rightarrow i.
\]

Then, we can introduce the parity merge for connectors.

\[
\text{Definition } \text{clink} \_\text{eomerge } m \left( c_1 : \text{connector } m \right) \left( c_2 : \text{connector } m \right) := \\
\quad \left[ \text{fun } i : 'I_(m + m) \Rightarrow \\
\quad \quad \text{if odd } i \text{ then } \text{olift } \left( \text{clink} \_\text{eomerge } c_2 \left( \text{idiv2 } i \right) \right) \\
\quad \quad \text{else } \text{elift } \left( \text{clink} \_\text{eomerge } c_1 \left( \text{idiv2 } i \right) \right) \right].
\]

\[
\text{Lemma } \text{clink} \_\text{eomerge} \_\text{proof } m \left( c_1 : \text{connector } m \right) \left( c_2 : \text{connector } m \right) : \\
\quad \text{forall } i, \left( \text{clink} \_\text{eomerge } c_1 c_2 \left( \text{clink} \_\text{eomerge } c_1 c_2 \right) \right) \Rightarrow i].
\]

\[
\text{Definition } \text{ceomerge } m \left( c_1 : \text{connector } m \right) \left( c_2 : \text{connector } m \right) := \\
\quad \text{connector} \_\text{of } \left( \text{clink} \_\text{eomerge} \_\text{proof } c_1 c_2 \left) \right).
\]

Finally we can get the parity duplication

\[
\text{Definition } \text{neomerge } m \left( n_1 : \text{network } m \right) \left( n_2 : \text{network } m \right) := \\
\quad \left[ \text{seq } \text{ceomerge } i.1 i.2 | i \leftarrow \text{zip } n_1 n_2 \right].
\]

\[
\text{Definition } \text{neodup } m \left( n : \text{network } m \right) : \text{network } (m + m) := \text{neomerge } n n.
\]
It is composed of 6 connectors (the drawing of some links have been slightly shifted to the right so they don’t overlap). The key ingredient of this network is the half-cleaner. It is a connector for \( m + m \) lines, that links the line \( i \) to the line \( i + m \) for \( i < m \).

\[
\text{Definition } \text{clink\_half\_cleaner} \ m : \{ \text{ffun } I_\_ (m + m) \Rightarrow I_\_ (m + m) \} := \\
\begin{array}{l}
\text{ffun } i => \\
\text{match split } i \text{ with} \\
\mid \text{inl } x => rshift \_ x \\
\mid \text{inr } x => lshift \_ x \\
\text{end}. 
\end{array}
\]

\[
\text{Lemma } \text{clink\_half\_cleaner\_proof} \ m : \\
[\forall i : I_\_ (m + m), \text{clink\_half\_cleaner\_} (\text{clink\_half\_cleaner\_} i) == i].
\]

\[
\text{Definition } \text{half\_cleaner} \ m := \text{connector\_of } (\text{clink\_half\_cleaner\_proof} \ m).
\]

This connector has an interesting behaviour when given as input a so-called bitonic tuple. Technically, a sequence of elements is bitonic if there is one of its rotation that is increasing then decreasing.

\[
\text{Definition } \text{bitonic} := [\text{qualify } s | \\
[\exists \, r : I_\_ (\text{size } s).+1, \\
\exists \, n : I_\_ (\text{size } s).+1, \\
\text{let } s_1 := \text{rot } r \, s \text{ in } \text{sorted} \leq (\text{take } n \, s_1) \&\& \text{sorted} \geq (\text{drop } n \, s_1)]].
\]
Fortunately for sequences of booleans the characterisation is simpler: a sequence of booleans is bitonic if it has at most 2 flips.

**Lemma bitonic BoolP** 
\[
(s : \text{seq bool}) : \\
\text{reflect} (\exists t, \\
\text{let: } (b, i, j, k) := t \text{ in } s = \text{nseq } i \ b \ +\ +\ \text{nseq } j \ (\neg b) \ +\ +\ \text{nseq } k \ b) \\
(s \text{ is bitonic}).
\]

When applied to a bitonic sequence, the half-cleaner returns a tuple whose right half contains only `true` and the left half is bitonic or the left half contains only `false` and the right half is bitonic.

**Lemma bitonic halfCleaner** 
\[
m (t : (m + m) \text{-tuple bool}) : \\
t \text{ is bitonic} \Rightarrow \\
\text{let } t_1 := \text{cfun} (\text{halfCleaner } m) \ t \text{ in} \\
((\text{take } m \ t_1 = \text{nseq } n \ false) \ && (\text{drop } m \ t_1 \text{ is bitonic})) \\
\| \\
((\text{drop } m \ t_1 = \text{nseq } n \ true) \ && (\text{take } m \ t_1 \text{ is bitonic})).
\]

The proof proceeds by case analysis. As the tuple contains only 2 flips, there are two easy cases when these two flips are both in a single half. When it is in the left half, we have

| left half | \(b\) | \(b\) | \(b\) | \(\overline{b}\) | \(\overline{b}\) | \(\overline{b}\) | \(\overline{b}\) | \(b\) | \(b\) | \(b\) |
| right half | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) |
| min | \(b\) | \(b\) | \(b\) | \(F\) | \(F\) | \(F\) | \(F\) | \(b\) | \(b\) | \(b\) |
| max | \(b\) | \(b\) | \(b\) | \(T\) | \(T\) | \(T\) | \(T\) | \(b\) | \(b\) | \(b\) |

so the property holds. By symmetry this is the same if the two flips are on right half.

| left half | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) | \(b\) |
| right half | \(b\) | \(b\) | \(b\) | \(\overline{b}\) | \(\overline{b}\) | \(\overline{b}\) | \(\overline{b}\) | \(b\) | \(b\) | \(b\) |
| min | \(b\) | \(b\) | \(b\) | \(F\) | \(F\) | \(F\) | \(F\) | \(b\) | \(b\) | \(b\) |
| max | \(b\) | \(b\) | \(b\) | \(T\) | \(T\) | \(T\) | \(T\) | \(b\) | \(b\) | \(b\) |
In the remaining cases, each half has a flip. Suppose the flip in the left half occurs first, we have:

<table>
<thead>
<tr>
<th>left half</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>right half</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>min</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>F</td>
</tr>
<tr>
<td>max</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>T</td>
</tr>
</tbody>
</table>

and the property holds again. Finally the flip in the right half occurs first, we have

<table>
<thead>
<tr>
<th>left half</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
<th>b</th>
</tr>
</thead>
<tbody>
<tr>
<td>right half</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
</tr>
<tr>
<td>min</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>F</td>
</tr>
<tr>
<td>max</td>
<td>T</td>
<td>T</td>
<td>T</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>b</td>
<td>T</td>
</tr>
</tbody>
</table>

This ends the proof.

The next observation is that if we recursively apply on the resulting halves the half-cleaner, we end up getting a sorted list: we progressively add false on the left part or true on the right one. Being able to perform this recursion on halves implies that the initial number of lines must be a power of 2. In our case, in order to insert a half-cleaner we need to have a type of the form connector \((m + m)\). This means that it is mandatory for the typechecker to succeed that \(2^{m+1}\) converts to \(2^m + 2^m\). This is not the case with the exponential function of the library. So we define our own version that we write \(2^n\) in the following.

```
Fixpoint '2^m := if m is m1.+1 then '2^m1 + '2^m1 else 1.
```

We can then define the recursive function.

```
Fixpoint half_cleaner_rec m : network '2^m :=
    if m is m1.+1 then half_cleaner '2^m1 :: ndup (half_cleaner_rec m1)
    else [::].
```

We can then easily prove its expected behaviour.
and show that it is logarithmic and creates a network of $m$ connectors.

The recursive half-cleaner requires to have a bitonic entry. If we try to build a recursive algorithm, calling it first on the top-half lines and then on the bottom-half lines, we get two sorting outputs. Gluing them directly does not give a bitonic entry. There are possibly too many flips. Each half that is sorted contains potentially a flip and there is the potential flip at their intersection. Instead, the trick is to glue them together but reversing the second one. This leads to a bitonic entry. So, a reverse version of the half-cleaner is created that performs this reversal. Graphically, it looks like this.

On the left-hand side there is the standard half-cleaner. On the right-hand side there is the reverse version where the link to the bottom lines have been reverse. For example, the line 1 is linked to the line 5 on the left part. It is now linked to the line 8 on the right part. There is a $\text{rev\_ord}$ function for ordinals. We use it to implement the reverse half-cleaner, so the line $i$ is connected to line $m - i$: 
Definition \texttt{clink\_rhalf\_cleaner} \texttt{m} : \{ \texttt{fun} \texttt{I\_m} \Rightarrow \texttt{I\_m} \} := [\texttt{fun} \texttt{i} \Rightarrow \texttt{rev\_ord} \texttt{i}].

Lemma \texttt{clink\_rhalf\_cleaner\_proof} \texttt{m} :
\begin{align*}
& \texttt{[\forall i : I\_m + m), clink\_rhalf\_cleaner\_i} = \texttt{i}. \\
& \texttt{Definition rhalf\_cleaner} \texttt{m} := \texttt{connector\_of (clink\_rhalf\_cleaner\_proof m)}. \\
\end{align*}

Now, we can use the reverse half-cleaner before calling the recursive half-cleaner.

Definition \texttt{rhalf\_cleaner\_rec} \texttt{n} : \texttt{network \_2^n} :=
\begin{align*}
& \texttt{if} \texttt{n is n\_1 + 1 then rhalf\_cleaner \_2^{n\_1} :} \texttt{ndup (half\_cleaner\_rec n\_1)} \\
& \texttt{else [::].} \\
\end{align*}

The call to the reverse half-cleaner produces on the top-half lines either only \texttt{true} values so there is no problem or a reverse of a bitonic but it is also ok, the reverse of a bitonic is a bitonic. The same holds for the bottom-half lines. So, we get the expected theorem.

Lemma \texttt{sorted\_rhalf\_cleaner\_rec} \texttt{m} \texttt{(t : \_2^{m\_1} \_tuple bool)} :
\begin{align*}
& \texttt{sorted} \leq (\texttt{take \_2^{m\_1} t}) \Rightarrow \texttt{sorted} \leq (\texttt{drop \_2^{m\_1} t}) \rightarrow \\
& \texttt{sorted} \leq (n\texttt{fun (rhalf\_cleaner\_rec m\_1 + 1)} t). \\
\end{align*}

Now, we can build the recursion

Fixpoint \texttt{bsort} \texttt{m} : \texttt{network \_2^m} :=
\begin{align*}
& \texttt{if} \texttt{m is m\_1 + 1 then ndup (bsort m\_1) ++ rhalf\_cleaner\_rec m\_1 + 1} \\
& \texttt{else [::].} \\
\end{align*}

and get the final results.

Lemma \texttt{sorting\_bsort} \texttt{m} : \texttt{bsort m is sorting.}

Lemma \texttt{size\_bsort} \texttt{m} : \texttt{size (bsort m) = (m * m\_1 + 1)./2.}

Here is the complete code of the algorithm.
4 Knuth’s Exchange Odd Even Sorter

Here is the drawing of the odd-even sorter.

This is still a recursive algorithm but this time it is not based on a top-half, bottom-half partition but an even and odd partition. We add them as basic operations on sequences.
There are two components of this sorter. The first one is the one that connects even line to one of their odd neighbour.

We first have 4 copies with jump 4 then 2 copies with jump 2 finally 1 copy with jump 1. The copy with jump 1 on the right shows the structure: even lines are linked to their down neighbour. In order to encode it, we need to introduce the notion of neighbour for ordinals.

**Definition** \(\text{inext} m\) : \(\text{I}_m\) \(\to\) \(\text{I}_m\) :=
- if \(m\) is \(m_1+1\) then fun \(i\) => \(\text{inZp}(\text{if } i == m_1 \text{ then } i \text{ else } i.+1)\)
- else fun \(i\) => \(i\).

**Definition** \(\text{ipred} m\) : \(\text{I}_m\) \(\to\) \(\text{I}_m\) :=
- if \(m\) is \(m_1+1\) then fun \(i\) => \(\text{inZp}(i.-1)\) else fun \(i\) => \(i\).

We can define the connector.

**Definition** \(\text{clink\_eswap} m\) : \{ffun \(\text{I}_m\) \(\to\) \(\text{I}_m\}\) :=
- [ffun \(i\) : \(\text{I}_m\) => if odd \(i\) then \(\text{ipred} i\) else \(\text{inext} i\)].

**Lemma** \(\text{clink\_eswap\_proof} m\) :
- [forall \(i\) : \(\text{I}_m\), \(\text{clink\_eswap} (\text{clink\_eswap} _i) == i\)].

**Definition** \(\text{ceswap} m\) := connector of (\(\text{clink\_eswap\_proof} m\)).

If we look at the effect of applying this connector to a tuple of booleans, if the even lines and the odd lines are sorted, this property is preserved plus the even part contains more \texttt{false} than the odd part:
The second connector is the one that connects the odd lines with a $k$ jump ($k$ is odd) to the even lines.

There are 2 copies with jump 1, then one copy with jump 3 and one copy with jump 1. Again, we define first the operation on ordinals.

We then create the connector.
Definition \( \text{clink\_odd\_jump} m k \) :=
if odd \( k \) then [ffun \( i \rightarrow \) if odd \( i \) then iadd \( k \) \( i \) else isub \( k \) \( i \)]
else [ffun \( i \rightarrow \) \( i \)].

Lemma \( \text{clink\_odd\_jump\_proof} m k \) :
[forall \( i : I_m \), \( \text{clink\_odd\_jump\_proof} m k (\text{clink\_odd\_jump\_proof} m k \( i \)) = \( i \)].

Definition \( \text{codd\_jump} m k \) :=
connector_of (\( \text{clink\_odd\_jump\_proof} m k \)).

This time, the false values are moving from the even lines to the odd lines and we can quantify exactly how much.

Note that here we make use of the fact that \( m - n = 0 \) if \( n \geq m \).

Now, the idea of the algorithm is to reduce the difference between the number of false between the odd and the even part so that the list becomes sorted.

Note that here we make use of the fact that \( m - n = 0 \) if \( n \geq m \).

This is done by recursively halving the jump and we get the expected result.
We can now put together the recursion, the even swap and the recursive jump to get the sorter.

\[
\begin{align*}
\text{Fixpoint } & \text{knuth}_\text{exchange} \ m : \ \text{network }'2^m' := \\
& \quad \text{if } m \text{ is } m_1.+1 \text{ then} \\
& \quad \quad \text{neodup } (\text{knuth}_\text{exchange} \ m_1) ++ \text{ceswap } :: \ \text{knuth}_\text{jump}_\text{rec} \ '2^m' \ m_1 \ (('2^m_1).-1) \\
& \quad \text{else } [::]. \\
\text{Lemma } & \text{sorting}_\text{knuth}_\text{exchange} \ m : \ \text{knuth}_\text{exchange} \ m \text{ is sorting}. \\
\text{Lemma } & \text{size}_\text{knuth}_\text{exchange} \ m : \ \text{size } (\text{knuth}_\text{exchange} \ m) = (m * m.+1)./2.
\end{align*}
\]

Here is the complete code of the algorithm.

\[
\begin{align*}
\text{Fixpoint } & \text{knuth}_\text{jump}_\text{rec} \ m \ k \ r : \ \text{network } m := \\
& \quad \text{if } k \text{ is } k_1.+1 \text{ then } \text{codd}_\text{jump}_r :: \ \text{knuth}_\text{jump}_\text{rec} \ m \ k_1 \ (\text{uphalf}_r).-1 \\
& \quad \text{else } [::]. \\
\text{Fixpoint } & \text{knuth}_\text{exchange} \ m : \ \text{network } '2^m' := \\
& \quad \text{if } m \text{ is } m_1.+1 \text{ then} \\
& \quad \quad \text{neodup } (\text{knuth}_\text{exchange} \ m_1) ++ \text{ceswap } :: \ \text{knuth}_\text{jump}_\text{rec} \ '2^m' \ m_1 \ (('2^m_1).-1) \\
& \quad \text{else } [::].
\end{align*}
\]

5 Batcher’s Odd Even Sorter

The last algorithm we are going to consider is using both the top-bottom recursion and an even-odd recursion. For 8 lines, we get.
This sorter uses only two connectors. The \textit{cswap} connector is used in the base case for sorting two lines. The \textit{codd\_jump} connector with a jump of one is used at the end of the iteration to get the sorted result when it is sure that the numbers of \textit{false} of the even part exceeds of at most 2 the ones of the odd part.

\begin{center}
\textbf{Definition} \textit{batcher\_merge} \textit{m} : \textit{connector} \textit{m} := \textit{codd\_jump} 1.
\end{center}

\begin{center}
\textbf{Lemma \textit{sorted\_batcher\_merge}} \textit{m} (\textit{t} : (\textit{m} + \textit{m}).\textit{-tuple bool}) :
\end{center}

\begin{itemize}
\item noF (\textit{otake} \textit{t}) \leq noF (\textit{etake} \textit{t}) \leq (noF (\textit{otake} \textit{t})).+2 ->
\item \textit{sorted\_\leq} (\textit{etake} \textit{t}) -> \textit{sorted\_\leq} (\textit{otake} \textit{t}) ->
\item \textit{sorted\_\leq} (\textit{cfun batcher\_merge} \textit{t}).
\end{itemize}

In order to sort the odd and even parts, the sorter uses an odd and even recursion.

\begin{center}
\textbf{Fixpoint} \textit{batcher\_merge\_rec\_aux} \textit{m} : \textit{network} \textit{\`2m.+1} :=
\end{center}

\begin{itemize}
\item if \textit{m} is \textit{m} 1.+1 then \textit{rcons} (\textit{neodup} (\textit{batcher\_merge\_rec\_aux} \textit{m} 1)) \textit{batcher\_merge}
\item else [:: \textit{cswap} \textit{ord0} \textit{ord\_max}].
\end{itemize}

\begin{center}
\textbf{Definition} \textit{batcher\_merge\_rec} \textit{m} :=
\end{center}

\begin{itemize}
\item if \textit{m} is \textit{m} 1.+1 then \textit{batcher\_merge\_rec\_aux} \textit{m} 1 else [::].
\end{itemize}

The idea is the following. If the top-half and the bottom-half are sorted, their respective odd and even part differ at most of one in the number of \textit{false} (the odd part being the smallest). When taking the odd part and even part of all the lines, it then differs of at most 2. After sorting them, we are within the conditions of theorem \textit{sorted\_batcher\_merge}. As having top-half and bottom-half sorted is preserved by taking the odd or the even part, we get the following theorem.

\begin{center}
\textbf{Lemma \textit{sorted\_nfun\_batcher\_merge\_rec}} \textit{m} (\textit{t} : \textit{\`2m.+1}.\textit{-tuple bool}) :
\end{center}

\begin{itemize}
\item \textit{sorted\_\leq} (\textit{take} \textit{\`2m} \textit{t}) -> \textit{sorted\_\leq} (\textit{drop} \textit{\`2m} \textit{t}) ->
\item \textit{sorted\_\leq} (\textit{nfun} (\textit{batcher\_merge\_rec\_aux} \textit{m}) \textit{t}).
\end{itemize}

We are almost done. We can use top-bottom recursion to fulfill the conditions of theorem \textit{sorted\_nfun\_batcher\_merge\_rec}.

18
Fixpoint \( \text{batcher} \ m : \ network \ 2^m := \)
  \[
  \begin{array}{l}
  \text{if } m \text{ is } m.+1 \text{ then } \text{ndup} \ (\text{batcher} \ m) ++ \text{batcher}_\text{merge}_\text{rec} \ m.+1 \\
  \text{else } ::.
  \end{array}
  \]

and we get the expected properties.

Lemma \( \text{sorting}_\text{batcher} \ m : \ \text{batcher} \ m \text{ is sorting.} \)

Lemma \( \text{size}_\text{batcher} \ m : \ \text{size} \ (\text{batcher} \ m) = (m + m.+1)/2. \)

Here is the complete code of the algorithm.

Fixpoint \( \text{batcher}_\text{merge}_\text{rec}_\text{aux} \ m : \ network \ 2^m.+1 := \)
  \[
  \begin{array}{l}
  \text{if } m \text{ is } m.+1 \text{ then } \text{rcons} \ (\text{neodup} \ (\text{batcher}_\text{merge}_\text{rec}_\text{aux} \ m)) \ \text{batcher}_\text{merge} \\
  \text{else } :: \ \text{cswap} \ \text{ord0} \ \text{ord_max}.
  \end{array}
  \]

Definition \( \text{batcher}_\text{merge}_\text{rec} \ m := \)
  \[
  \begin{array}{l}
  \text{if } m \text{ is } m.+1 \text{ then } \text{batcher}_\text{merge}_\text{rec}_\text{aux} \ m \text{ else } ::.
  \end{array}
  \]

Fixpoint \( \text{batcher} \ m : \ network \ 2^m := \)
  \[
  \begin{array}{l}
  \text{if } m \text{ is } m.+1 \text{ then } \text{ndup} \ (\text{batcher} \ m) ++ \text{batcher}_\text{merge}_\text{rec} \ m.+1 \\
  \text{else } ::.
  \end{array}
  \]

6 Extension

A standard extension is to use oriented comparator. Graphically, the orientation indicates which line gets the maximum of the two lines. This means that, so far, we have been using comparator with the arrow down.

\[
\begin{array}{c}
  a_1 \\
  \downarrow \\
  a_2 \\
\end{array}
\quad
\begin{array}{c}
  a'_1 \\
  \downarrow \\
  a'_2 \\
\end{array}
\]

Instead, with the arrow up, the value of the upper line is the maximum of the input values, \( a'_1 = \max(a_1, a_2) \), and the output value of the lower line is the minimum of the two lines, \( a'_1 = \max(a_1, a_2) \).
In our formalisation, this means that we need to add an extra component that keeps the orientation of the link. This is the field \( \text{cflip} \) that associates a boolean to every line. The field \( \text{cflipinv} \) ensures that associated lines have identical flip value.

\[
\begin{array}{c}
\begin{array}{c}
\text{Record} \ \text{connector} \ (m : \text{nat}) := \text{connector}_m \ {\{}
\begin{array}{c}
\text{clink} : \{\text{ffun} \ I_m \ \rightarrow \ I_m\};
\text{cflip} : \{\text{ffun} \ I_m \ \rightarrow \ \text{bool}\};
\text{cfinv} : \{\forall i, \text{clink(}\text{clink}\ i) = i\};
\text{cflipinv} : \{\forall i, \text{cflip(}\text{clink}\ i) = \text{cflip}\ i\}\};
\end{array}
\{\}}.
\end{array}
\end{array}
\]

These modifications change the way we define \( \text{cfun} \)

\[
\begin{array}{c}
\begin{array}{c}
\text{Definition} \ \text{cfun} \ c : t :=
\begin{array}{c}
\{\text{tuple} \ \text{let} \ \text{min} := \text{min}(\text{nth}\ t\ i) \ (\text{nth}\ t\ (\text{clink}\ c\ i)) \ \text{in}
\text{let} \ \text{max} := \text{max}(\text{nth}\ t\ i) \ (\text{nth}\ t\ (\text{clink}\ c\ i)) \ \text{in}
\text{if} \ i \leq \text{clink}\ c\ i \ \text{then if} \ c\text{flip}\ c\ i \ \text{then} \ \text{max} \ \text{else} \ \text{min} \ \text{else if} \ c\text{flip}\ c\ i \ \text{then} \ \text{min} \ \text{else} \ \text{max} \ | \ i < m\}.
\end{array}
\end{array}
\end{array}
\]

The main algorithm that benefits from having this new capability is the bitonic sorter.
The drawing is more regular since it uses the `half_cleaner` connector only.

**Lemma** `cflip_default m (clink : {ffun I_→_m} (b : bool) : [forall i, [ffun => b] (clink i) == [ffun => b] i])`.  
**Definition** `half_cleaner b m := connector_of (clink_half_cleaner_proof m) (cflip_default (clink_half_cleaner m) b)`.  

It is now possible to write a version of the bitonic sorter `bfsort` that uses the flip.

**Fixpoint** `half_cleaner_rec b m : network '2^m :=  
  if m is m_1.+1 then half_cleaner b '2^m_1 :: ndup (half_cleaner_rec b m_1)  
  else [:].`.  
**Fixpoint** `bfsort (b : bool) m : network '2^m :=  
  if m is m_1.+1 then nmerge (bfsort b m_1) (bfsort (¬b) m_1) ++  
    half_cleaner_rec b m_1.+1  
  else [:].`.  
**Lemma** `size_bfsort b m : size (bfsort b m) = (m * m.+1)/2`.  
**Lemma** `sorting_bfsort m : bfsort false m is sorting`.

### 7 Conclusion

In this paper, we have shown how to formalise different sorting algorithms for networks. We have been following mostly what is presented in chapter 28.
of [2]. Another source of inspiration was [1]. We have been using intensively the zero-one principle. Most of the proof are done manipulating booleans. It looks a bit like magic. The formalisation is available at

https://github.com/thery/mathcomp-extra

It consists of 5 files. The file `more_tuple` contains some addition to the Mathematical Library. It is 1000-line long. The file `nsort` contains the definition of network and some basic connectors. It is 700-line long. The file `bitonic` deals with the bitonic sorter. It is 500-line long. The file `bjsort` deals with the exchange sorter. It is 200-line long. The file `batcher` deals with the exchange sorter. It is 200-line long.

From the specification point of view, we believe that having explicit networks and using dependent types for this gives us a very concise presentation of the algorithms. All the usual index manipulations are hidden inside the `ndup` and `neodup` building blocks. From the proving point of view, the difficult part in the bitonic sort is proving the specification of the half-cleaner. From the other sorters, the only delicate thing is the manipulation of `codd_jump` connectors. The introduction of the function `noF` makes the specification and proof easier.

References


A Basic

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x = y )</td>
<td>propositional equality between ( x ) and ( y )</td>
</tr>
<tr>
<td>( x == y )</td>
<td>boolean equality between ( x ) and ( y ) that must belong to an eqType</td>
</tr>
<tr>
<td><code>reflect P b</code></td>
<td>equivalence between the propositions ( P ) and ( (b = \text{true}) )</td>
</tr>
<tr>
<td><code>n.1</code></td>
<td>add one to the natural number ( n )</td>
</tr>
<tr>
<td><code>n.*2</code></td>
<td>double the natural number ( n )</td>
</tr>
<tr>
<td><code>n./2</code></td>
<td>half the natural number ( n )</td>
</tr>
<tr>
<td><code>uphalf n</code></td>
<td>half the natural number ( n + 1 )</td>
</tr>
<tr>
<td><code>odd n</code></td>
<td>true if ( n ) is odd, ( \text{false} ) otherwise</td>
</tr>
<tr>
<td><code>(l, r)</code></td>
<td>the pair composed of ( r ) and ( l )</td>
</tr>
<tr>
<td><code>p.1</code></td>
<td>the first component of the pair ( p )</td>
</tr>
<tr>
<td><code>p.2</code></td>
<td>the second component of the pair ( p )</td>
</tr>
<tr>
<td><code>[\text{qualify } x \mid P]</code></td>
<td>if ( A := [\text{qualify } x \mid P] ), ( x ) is ( A ) is equivalent to ( P )</td>
</tr>
</tbody>
</table>

B Fintype

<table>
<thead>
<tr>
<th><code>[\forall x, P]</code></th>
<th>( P ) (in which ( x ) can appear) is true for all values of ( x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( I__n )</td>
<td>the finite subType of integers ( i &lt; n )</td>
</tr>
<tr>
<td><code>ord0</code></td>
<td>the ( i : I__n.1 ) with value 0</td>
</tr>
<tr>
<td><code>ord_max</code></td>
<td>the ( i : I__n.1 ) with value ( n )</td>
</tr>
<tr>
<td><code>\text{inZp}</code></td>
<td>the natural projection from nat into the integers mod ( p ), represented</td>
</tr>
<tr>
<td>( \text{as 'I}_p ). Here ( p ) is implicit, but must be of the form ( n.1 )</td>
<td></td>
</tr>
<tr>
<td><code>rev_ord i</code></td>
<td>the complement to ( n.-1 ) of ( i : I__n )</td>
</tr>
<tr>
<td><code>lshift n j</code></td>
<td>the ( i : 'I_{(m+n)} ) with value ( j : 'I_m )</td>
</tr>
<tr>
<td><code>rshift m k</code></td>
<td>the ( i : 'I_{(m+n)} ) with value ( m+k ), ( k : 'I_n )</td>
</tr>
<tr>
<td><code>split i</code></td>
<td>( i ) has type ( 'I_{(m+n)} )</td>
</tr>
<tr>
<td></td>
<td>it returns ( \text{inl } j ) when there exists ( j ) such</td>
</tr>
<tr>
<td></td>
<td>that ( i = \text{lshift } n ) ( j )</td>
</tr>
<tr>
<td></td>
<td>it returns ( \text{inr } k ) when there exists ( k ) such</td>
</tr>
<tr>
<td></td>
<td>that ( i = \text{rshift } m ) ( k )</td>
</tr>
<tr>
<td><code>{\text{ffun } A \Rightarrow B}</code></td>
<td>type for functions with a finite domain (( A ) should be a fintype)</td>
</tr>
<tr>
<td><code>{\text{ffun } x \Rightarrow E}</code></td>
<td>definition of a function with a finite domain (( x ) may appear in ( E ))</td>
</tr>
</tbody>
</table>
C Sequences

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[]</code></td>
<td>the empty sequence</td>
</tr>
<tr>
<td><code>x : s</code></td>
<td>the sequence starting with <code>x</code> followed by <code>s</code></td>
</tr>
<tr>
<td><code>rcons s x</code></td>
<td>the sequence starting with <code>s</code> and ended by <code>x</code></td>
</tr>
<tr>
<td>`seq E</td>
<td>i &lt;- I`</td>
</tr>
<tr>
<td><code>size s</code></td>
<td>the number of items (length) in <code>s</code></td>
</tr>
<tr>
<td><code>count P s</code></td>
<td>the number of items of <code>s</code> for which <code>P</code> holds</td>
</tr>
<tr>
<td><code>nseq n x</code></td>
<td>a sequence of <code>n</code> <code>x</code>'s</td>
</tr>
<tr>
<td><code>head x0 s</code></td>
<td>the head (zero'th item) of <code>s</code> if <code>s</code> is non-empty, else <code>x0</code></td>
</tr>
<tr>
<td><code>behead s</code></td>
<td><code>s</code> minus its head</td>
</tr>
<tr>
<td><code>last x s</code></td>
<td>the last element of <code>x : s</code> (which is non-empty)</td>
</tr>
<tr>
<td><code>belast x s</code></td>
<td><code>x : s</code> minus its last item</td>
</tr>
<tr>
<td><code>s1 ++ s2</code></td>
<td>the concatenation of <code>s1</code> and <code>s2</code></td>
</tr>
<tr>
<td><code>take n s</code></td>
<td>the sequence containing only the first <code>n</code> items of <code>s</code> (or all of <code>s</code> if <code>size s ≤ n</code>)</td>
</tr>
<tr>
<td><code>drop n s</code></td>
<td><code>s</code> minus its first <code>n</code> items (`` if <code>size s ≤ n</code>)</td>
</tr>
<tr>
<td><code>rot n s</code></td>
<td><code>s</code> rotated left <code>n</code> times (or <code>s</code> if <code>size s ≤ n</code>)</td>
</tr>
<tr>
<td><code>zip s t</code></td>
<td>itemwise pairing of <code>s</code> and <code>t</code> (dropping any extra items)</td>
</tr>
<tr>
<td><code>foldl f a s</code></td>
<td>the left fold of <code>s</code> by <code>f</code>, i.e. <code>f (f ... (f a x1) ... x_{n-1}) x_n</code></td>
</tr>
<tr>
<td><code>perm_eq s1 s2</code></td>
<td><code>s2</code> is a permutation of <code>s1</code>, i.e., <code>s1</code> and <code>s2</code> have the items (with the same repetitions), but possibly in a different order</td>
</tr>
<tr>
<td><code>sorted e s</code></td>
<td><code>s</code> is an <code>e</code>-sorted sequence: either <code>s = []</code>, <code>s = [: : x]</code>, or <code>s = x :: y :: s1</code> with <code>e x y</code> and <code>(y :: s1)</code> is <code>e</code>-sorted</td>
</tr>
</tbody>
</table>

D Tuple

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>n.-tuple T</code></td>
<td>the type of <code>n</code>-tuples of elements of type <code>T</code></td>
</tr>
<tr>
<td>`[tuple E</td>
<td>i &lt; n]`</td>
</tr>
<tr>
<td><code>tnth t i</code></td>
<td>the <code>i</code>'th component of <code>t</code>, where <code>i : I_n</code></td>
</tr>
</tbody>
</table>