The complexity of the parity function in unbounded fan-in, unbounded depth circuits

Ingo Wegener*

LS II, FB Informatik, Universität Dortmund, 4600 Dortmund, Germany

Communicated by M.S. Paterson
Received June 1988
Revised February 1989

Abstract


Almost everything is known on the complexity of the parity function in fan-in 2 circuits over various bases. Also the minimal depth of polynomial-size, unbounded fan-in \{\land, \lor, \neg\} circuits for the parity function has been studied. Here the complexity without any depth restriction is considered. For the basis \{\land, \lor, \neg\} almost optimal bounds, and for the basis of NOR gates and the basis of all threshold functions optimal bounds on the number of gates are obtained. For the basis \{\land, \lor, \neg\} the minimal number of wires is determined. For threshold circuits an exponential gap between synchronous and asynchronous circuits is proved. The results not only answer open questions in complexity theory but also have implications for the real-life circuit design.

1. Introduction

There can be no doubt that the parity functions

\[ f_n(x_1, \ldots, x_n) = x_1 \oplus \cdots \oplus x_n \oplus e \quad \text{for } e \in \{0, 1\} \]

are two of the most important Boolean functions in computer science. For example, parity checks are the easiest error detecting codes, the last bit of the sum of \(n\) integers is the parity of the last bits of the integers, and more applications are known. On the other hand, it is difficult to design \(\oplus\)-gates in MOS technology. Therefore, the (circuit) complexity of the parity function has been investigated in many papers. The complexity

*Supported in part by DFG grant We 1066/2-1.
in fan-in 2 circuits is well understood. We give a short review of these results in
Section 2.

In fan-in 2 circuits the number of wires is twice the number of gates. In unbounded
fan-in circuits the number of wires is not determined by the number of gates. Hence,
three complexity measures, namely, depth (longest path from the inputs to the output),
number of gates and number of wires are of interest.

It is well known that the parity functions are those functions which have the most
expensive minimal polynomial. The minimal polynomial consists of all \(2^n - 1\) prime
implicants. On the other hand, the parity functions can be computed by circuits of
linear size and logarithmic depth (even with fan-in 2). Therefore, one may ask for the
minimal depth of unbounded fan-in, polynomial-size circuits over \(\{\wedge, \lor, \neg\}\) for the
parity function. After several papers with ever better lower-bound techniques, Hastad
[3] presented the final result: the minimal depth is

\[
\log n / \log \log n - o(\log n / \log \log n).
\]

This result implies that efficient circuits have depth “almost” \(\log n\). Hence, one
is interested in the minimal size (number of gates) of parity circuits and, furthermore,
whether these circuits may have small, i.e. logarithmic, depth and whether these
circuits may have the minimal number of wires.

For circuits over the basis of NOR gates Lai and Muroga [5] have solved this
problem. Their lower-bound proofs are complicated and for \(n = 2\) and \(n = 3\) are carried
out by a computer. We present simple proofs in Section 3. Our important and new
results are described in Sections 4 and 5.

For circuits over the basis \(\{\wedge, \lor, \neg\}\), where \(\neg\)-gates are free of charge, we present
in Section 4 almost optimal bounds on the number of gates and optimal bounds for
the number of wires. Furthermore, it is proved that circuits cannot have the minimal
number of gates and the minimal number of wires simultaneously.

In Section 5 the basis of all threshold functions is considered. We shall describe in
Sections 5 and 6 why threshold circuits are of great importance not only for theoretical
but also for practical purposes. Optimal synchronous and optimal asynchronous
circuits are presented. The asynchronous circuits have only logarithmic size. The size
of synchronous circuits is at least linear and therefore exponentially larger than the
size of optimal asynchronous circuits. By this result it is shown for the first time that
such an exponential gap is possible in unbounded fan-in circuits. On the other hand, it
is known that asynchronous fan-in 2 circuits of size \(c\) may be simulated by syn-
chronous fan-in 2 circuits of size \(O(c^2)\).

Finally, in Section 6, we discuss practical implications of our results. We propose
a circuit design for parity functions, which, we believe, is an improvement upon all
known circuits.

At the end of this introduction we list some well-known properties of the parity
functions which we apply in the rest of the paper.

- If we replace in a circuit for \(f_n^x\) a variable \(x_i\) by 0 or 1, we obtain a circuit for \(f_n^{x-1}\) or
  \(f_n^{x-1}\), respectively.
If we replace in a circuit for \( f_n^e \) a variable \( x_i \) by another variable \( x_j (j \neq i) \), we obtain a circuit for \( f_{n-2}^e \) on the variables \( x_k (k \notin \{i, j\}) \) since \( x_j \oplus x_j = 0 \).

If we replace in a circuit for \( f_n^e \) some variables but not \( x_i \) by arbitrary constants, the resulting circuit still depends essentially on \( x_i \); in particular, fan-out(\( x_i \)) > 0.

The parity functions are associative and commutative.

2. Fan-in 2 circuits

The following results (always for \( n \geq 2 \)) are part of the classical theory of Boolean circuits.

- Let \( B_2 \) be the set of all 16 Boolean functions on two inputs. Since \( f_2^e \in B_2 \), optimal \( B_2 \)-circuits for \( f_2^e \) contain \( n-1 \) gates.

- Let \( U_2 \) be the set of all 8 Boolean functions \( (x^a \land y^b)^c \), where \( x^1 = x \), \( x^0 = \bar{x} \) and \( a, b, c \in \{0, 1\} \). Schnorr [12] proved that optimal \( U_2 \)-circuits for \( f_n^e \) contain \( 3(n-1) \) gates.

- Redkin [10] proved that optimal \( \{ \land, \lor, \neg \} \) circuits for \( f_n^e \) contain exactly \( 4(n-1) \) gates and that optimal \( \{ \land, \neg \} \) circuits or \( \{ \lor, \neg \} \) circuits for the parity functions contain exactly \( 7(n-1) \) gates.

All these optimal circuits have a simple design. One starts with a binary tree of \( n-1 \) \( \oplus \)-gates and replaces each binary \( \oplus \)-gate by an optimal \( \Omega \)-circuit (for the basis \( \Omega \) considered) for \( f_2^0 \) or \( f_2^1 \).

Fan-in 2 circuits over the basis NOR (dual results hold for NAND circuits) have been investigated implicitly by Lai and Muroga [5]. They proved the necessity of \( 8(n-1) \) wires and therefore, in fan-in 2 circuits, of \( 4(n-1) \) gates. Furthermore, they have designed a fan-in 2 circuit for \( f_2^1 \) with 4 gates. Using \( n-1 \) of these circuits we obtain a fan-in 2 circuit with \( 4(n-1) \) gates for \( f_n^{(n-1) \mod 2} \). Since a NOR gate on one input operates like a NOT gate, we obtain for \( f_n^{n \mod 2} \) a fan-in 2 circuit with \( 4(n-1) + 1 \) gates. We show in Section 3 that this extra gate is necessary for \( n = 2 \).

Since the design technique for all these circuits is a gate-by-gate simulation, all the resulting circuits have logarithmic depth.

3. NOR circuits of unbounded fan-in

NOR gates are easy to design in current technology (MOS or GaAs) and are widely used. It is possible to design NOR gates of large fan-in but, obviously, not of arbitrary fan-in. Nevertheless, it is useful to investigate the complexity of the parity functions in unbounded fan-in NOR circuits. Let \( C_{\text{NOR}}(f) \) be the minimal number of gates in a NOR circuit for \( f \). Lai and Muroga [5] proved the following theorem.
Theorem 3.1. $C_{\text{NOR}}(f_n^*) = 3n-2$ for $n \geq 3$, $C_{\text{NOR}}(f_2^1) = 4$ and $C_{\text{NOR}}(f_2^0) = 5$.

The upper bound is proved by a clever cascading technique. It is possible to design circuits with logarithmic depth $(2 \lceil \log n \rceil + 1)$, optimal number of $3n-2$ gates and gates whose fan-in is bounded by 4. Hence, these circuits have practical relevance. We will compare these circuits with our threshold circuits in Section 6.

It is interesting to note that these circuits have been designed with the aid of a computer. For $n = 2$ and $n = 3$ a search algorithm for optimal circuits has been used. A systematic search is even for this small number of variables, too expensive. Therefore, branch-and-bound methods have been used [4, 7, 8]. But this procedure has one unsatisfying consequence. One knows that no better circuit can exist, because one cannot find such a circuit but one does not understand the reasons why there is no better circuit. For $n \geq 4$ the proof in [5] is carried out by induction. We present a proof for $n = 2$ which shows why there are no better circuits and we can now start the induction step for $n = 3$. Moreover, our proof is simpler and shorter than the proof in [5]. For the case $n = 2$ we allow at first also OR gates. OR gates are useful only as terminal gates. Otherwise, we may eliminate the OR gate $G$ and may use the inputs of $G$ directly as inputs in all direct successor gates of $G$.

Lemma 3.2. $C_{\text{NOR, OR}}(f_2^\sigma) \geq 4$.

Proof. $f_2^0$ and $f_2^1$ have the same complexity. By replacing the last gate of type NOR or OR by a gate of the other type, we obtain the other parity function. Hence, for one of the two parity functions there is an optimal circuit consisting of NOR gates only.

The fan-in of the last gate is at least 2, since otherwise the other parity function can be computed by a circuit with one gate less. Hence, $x_1 \oplus x_2 \oplus e = \text{NOR}(g_1, \ldots, g_r)$ and $r \geq 2$. The input functions $g_j$ are functions in $\mathbb{B}_2$.

The constant 0 is useless, the functions $1, x_1^\sigma, x_2^\sigma, x_1^\sigma \vee x_2^\sigma$ have the property that we can replace one variable by a constant in such a way that the output of the NOR gate is a constant. This is impossible for the parity function. Finally, because of the optimality of the circuit, no parity function is an input of the last gate.

Hence, the last gate has two inputs, i.e. $r = 2$, either $x_1 x_2$ and $\overline{x_1 x_2}$ or $\overline{x_1 x_2}$ and $x_1 \overline{x_2}$. If some parity function could be computed with 3 NOR gates, one of these two combinations would be computable with 2 NOR gates. With one NOR gate only $x_1 \overline{x_2} = \text{NOR}(x_1, x_2)$ is computable. Hence, $x_1 x_2$ has to be computable by one NOR gate from $x_1, x_2$ and $\overline{x_1 x_2}$. $x_1$ cannot be an input since $x_1 = 1$ would force the output of the gate to 0, the same holds for $x_2$. Finally, $\text{NOR}(\overline{x_1 x_2}) \neq x_1 x_2$. \hfill \Box

Lemma 3.3. $C_{\text{NOR}}(f_2^0) \geq 5$.

Proof. We assume that 4 gates are sufficient. Then $x_1 \oplus x_2$ is computed at the last gate and, by Lemma 3.2, the circuit does not compute $x_1 \oplus x_2 \oplus 1$ at some other gate. By the same arguments as in the proof of Lemma 3.2, we conclude that the inputs of
the last gate are \( x_1, x_2 \) and \( \bar{x}_1, \bar{x}_2 \). Without loss of generality \( \bar{x}_1, \bar{x}_2 \) is computed at the first gate. It is sufficient to show that \( x_1, x_2 \) cannot be computed from \( x_1, x_2 \) and \( \bar{x}_1, \bar{x}_2 \) with 2 NOR gates.

By the proof of Lemma 3.2, one gate is not sufficient. We assume that 2 gates are sufficient. Then the first gate computes \( g \) as the NOR of a subset of \( \{ x_1, x_2, \bar{x}_1, \bar{x}_2 \} \), and the second gate computes \( x_1, x_2 \) as the NOR of a subset of \( \{ g, \bar{x}_1, \bar{x}_2 \} \) since \( x_1 \) or \( x_2 \) cannot be an input of a NOR gate computing \( x_1, x_2 \) as has been argued in the proof of Lemma 3.2. \( g \) is one of the functions \( 1, \bar{x}_1, \bar{x}_2, x_1 \vee x_2, \bar{x}_1 \bar{x}_2, x_1 x_2, \bar{x}_1 \bar{x}_2, 0 \). Again, the constants are useless, \( \bar{x}_1 \bar{x}_2 \) is already computed and \( x_1 \vee x_2 \) cannot be an input of a NOR gate computing \( x_1 x_2 \). By symmetry, we have to consider only the cases \( g = \bar{x}_1 \) and \( g = x_1 \). If \( g \) or \( \bar{x}_1 \bar{x}_2 \) is the single input of a NOR gate, we obviously do not compute \( x_1, x_2 \). Finally, \( \text{NOR}(g, \bar{x}_1 \bar{x}_2) = x_1 \neq x_1 x_2 \).

**Lemma 3.4.** \( C_{\text{NOR, OR}}(f_n^*) \geq 3n - 2 \) for \( n \geq 2 \).

**Proof.** For \( n = 2 \), the claim is proved in Lemma 3.2. Again, it is sufficient to consider only NOR circuits. For \( n \geq 3 \), we consider some parity function \( f_n^* \) where \( C_{\text{NOR}}(f_n^*) \leq C_{\text{NOR}}(f_n^*) \) and an optimal NOR circuit for \( f_n^* \). At first we show that no variable \( x_i \) can have fan-out 1. Otherwise, let \( G \) be the only successor of \( x_i \). If \( \text{fan-in}(G) = 1 \), we eliminate \( G \) and obtain a circuit for \( f_n^* \) with one gate less. This is a contradiction. If \( \text{fan-in}(G) \geq 2 \), let \( h \) be one of the other inputs of \( G \). \( h \) cannot depend on \( x_i \), and, because of optimality, \( h \) is not a constant. We fix all variables \( x_j \) \((j \neq i)\) in such a way that \( h \) is replaced by 1. The resulting circuit is independent of \( x_i \). This is a contradiction.

**Case 1:** \( \exists x_i : \text{fan-out}(x_i) \geq 3 \). \( x_i = 1 \) eliminates at least 3 gates and we can use the induction hypothesis.

**Case 2:** \( \forall x_i : \text{fan-out}(x_i) = 2 \). Let \( G \) be some gate whose inputs are all variables.  

**Case 2.1:** There is such a gate \( G \) where \( \text{fan-in}(G) \geq 2 \). Let \( x_i \) and \( x_j \) be two of the inputs of \( G \). Let \( G_i \) and \( G_j \) be the other successors of \( x_i \) and \( x_j \) respectively. \( x_i = 1 \) eliminates \( G_i \) and \( G \). We obtain a circuit for \( f_{n-1}^* \) where \( \text{fan-out}(x_j) = 1 \). If \( \text{fan-in}(G_j) \geq 2 \), we obtain a contradiction by the same arguments as used directly before Case 1. Hence, \( \text{fan-in}(G_j) = 1 \). We eliminate \( G_j \) and obtain a circuit for \( f_{n-1}^*(x_i \rightarrow 1, x_j \rightarrow x_j \oplus 1) \). Since we have eliminated 3 gates, we can use the induction hypothesis.

**Case 2.2:** All gates \( G \) whose inputs are all variables have fan-in 1.

If one of these gates, whose input is e.g. \( x_i \), has fan-out at least 2, then \( x_i = 0 \) eliminates at least 3 gates and we can use the induction hypothesis. Otherwise, let \( G' \) be the first gate of the circuit whose fan-in is at least 2. Then \( G' \) has some input which is a negated variable and at least some other input which is a literal \( x_i^* \). \( x_i = 0 \) eliminates 2 gates, namely, \( G' \) and the gate where \( x_i \) is computed, and the fan-out of \( x_j \) is reduced to 1. We can continue as in Case 2.1. \( \square \)
4. Circuits of gates of AND-type and unbounded fan-in

Here we consider the basis \( U_\alpha \) containing gates for \((x_1^{a(1)} \land \cdots \land x_m^{a(m)})^b, a(1), \ldots, a(m), b \in \{0, 1\}\) and arbitrary \( m \). This is a natural generalization of the basis \( U_2 \) (see Section 2). This model is equivalent to the assumption that we have \( \land \)-gates of arbitrary fan-in and that negations are free of charge. By De Morgan's laws also \( \lor \)-gates of arbitrary fan-in are available. We denote by \( C_{U, \land}(f^e_n) \) and \( C_{U, \lor}(f^e_n) \) the minimal number of gates and wires, respectively, in \( U_\alpha \)-circuits for \( f^e_n \). Since negations are free of charge, \( f^e_n \) and \( f^e_n \) have the same complexity.

**Theorem 4.1.**

(i) \( 2n-1 \leq C_{U, \land}(f^e_n) \leq \lceil 5(n-1)/2 \rceil \) for \( n \geq 2 \).

(ii) \( C_{U, \lor}(f^e_n) = 6(n-1) \) for \( n \geq 2 \).

(iii) \( U_\alpha \)-circuits for \( f^e_n \) with \( 6(n-1) \) wires have \( 3(n-1) \) gates of fan-in 2, i.e. for \( n \geq 3 \) no circuit has simultaneously the minimal number of gates and wires.

**Proof.** We start with the upper bounds.

\[
x_1 \oplus x_2 = (x_1 \land \bar{x}_2) \lor (\bar{x}_1 \lor x_2)
\]

can be computed with 3 gates and 6 wires implying the upper bound of \( 6(n-1) \) wires.

\[
x_1 \oplus x_2 \oplus x_3 = x_1 \bar{x}_2 \bar{x}_3 \lor x_1 \bar{x}_2 x_3 \lor \bar{x}_1 x_2 x_3 \lor x_1 x_2 x_3
\]

can be computed with 5 gates and 16 wires. For odd \( n \), \( \frac{1}{2}(n-1) \) of these subcircuits are sufficient, altogether \( \frac{5}{2}(n-1) \) gates and \( 8(n-1) \) wires. For even \( n \), we take \( \frac{1}{2}n-1 \) of these subcircuits and one of the former circuits for 2 inputs. Hence, we use \( 5(\frac{1}{2}n-1)+3 = \frac{5}{2}(n-1)+\frac{1}{2} \) gates and \( 16(\frac{1}{2}n-1)+6 = 8(n-1)-2 \) wires. We remark that these upper bounds can be achieved with logarithmic depth.

The next step is to prove the lower bound on the number of gates. Let \( n = 2 \). It is easy to see that no variable can be an input of the output gate. Otherwise, we could make the output constant by fixing this variable. If 2 gates are sufficient, the second gate has only the first gate as input. Then the second gate operates as a negation and this gate could be eliminated in \( U_\alpha \)-circuits. We obtain a one-gate circuit and this gate has variables as inputs. This is a contradiction.

For the induction step \( (n-1 \rightarrow n) \) we first show that the fan-out of each variable \( x_i \) is at least 2. We have already seen that the fan-in of each gate is at least 2. Let us assume that fan-out\((x_i) = 1 \). Let \( G \) be the single successor of \( x_i \) and let \( h \) be some other input of \( G \). \( h \) is not a constant and \( h \) does not depend on \( x_i \). By fixing all variables \( x_j (j \neq i) \) in an appropriate way we can make the output independent of \( x_i \). This is a contradiction.

**Case 1:** \( \exists x_i: \text{fan-out}(x_i) \geq 3 \). Either \( x_i \) is a positive input of at least 2 gates or \( x_i \) is a negative input of at least 2 gates. Either \( x_i = 0 \) or \( x_i = 1 \) eliminates at least 2 gates. We then apply the induction hypothesis.

**Case 2:** \( \forall x_i: \text{fan-out}(x_i) = 2 \). We consider a first gate of the circuit, the inputs are, without loss of generality, \( x_1^{a(1)}, \ldots, x_n^{a(j)} \). If we replace \( x_i \) by \( x_i \), the circuit computes the other parity function. Therefore, without loss of generality \( a(1) = \cdots = a(j) = 1 \).
The situation is shown in Fig. 1. $x_2 = 0$ eliminates $G$. The subfunctions $g_i$ of $g_i$ for $x_2 = 0$ do not depend on $x_1$. We may assume that $g_1, ..., g_r$ are positive inputs of $G'$ since we can shift the negations to the predecessors. Furthermore, $g_i \equiv 1$; otherwise, we can replace the variables $x_m (m \neq 1)$ by constants in such a way that the output is independent of $x_1$. This implies that $x_2$ is a prime implicant of all $g_i$. If $g_i$ is not an input of the circuit then the gate computing it is also eliminated by $x_2 = 0$. Then we can apply the induction hypothesis. Otherwise, $j=2, r=1$ and $g_1 = x_2$; in particular, fan-in($G$) − fan-in($G'$) − 2. $x_2 = 1$ eliminates $G'$ (here 0 is computed) and $G$ (here $x_1$ is computed). Then we can apply the induction hypothesis.

Finally, we prove the lower bounds on the number of wires. We often use the fact that no gate in an optimal circuit has fan-in 1. For $n=2$ we have proved that 3 gates are necessary. This implies that 6 wires are necessary. If we have exactly 6 wires, all 3 gates have fan-in 2. We remark that in this case each variable enters one gate positively and one gate negatively. For the induction hypothesis we assume that the claims are proved for $1, ..., n-1$. We investigate a circuit with a minimal number of wires for $f_n$. If we can eliminate 7 wires by fixing one variable, we have reached a contradiction then since the resulting circuit has by the induction hypothesis $6(n-2)$ wires. Hence, our circuit has at least $6(n-1)+1$ wires and is, by our upper bound, not optimal with respect to the number of wires. If we can eliminate 3 gates with fan-in 2, we can apply the induction hypothesis.

Case 1: $\exists j$: fan-out($x_i$) $\geq 3$. We can assume that $x_i$ enters at least 2 gates, say $G$ and $G'$, positively. $x_i = 0$ eliminates at least 3 wires leaving $x_i$, at least 2 other wires entering $G$ and $G'$ and the wires leaving $G$ and $G'$. These are less than 7 wires only if $G$ and $G'$ have fan-in 2 and fan-out 1 and the only wire leaving $G$ enters $G'$ (or vice versa). Let $g$ be the second input of $G$. Then

$$ \text{res}(G) - (x_i \land g)^a \quad \text{and} \quad \text{res}(G') = (x_i \land (x_i \land g)^b)^c = (x_i \land g^b)^c. $$

$\text{res}(G')$ can be computed directly from $x_i$ and $g$. $G$ is superfluous and the circuit has not the minimal number of wires.

In the following cases, fan-out($x_i$) = 2 for all $i$. We consider a first gate $G$ of the circuit. By renumbering the variables and replacing some $x_i$ by $\bar{x}_i$, we can assume that $x_1, ..., x_j$ are the inputs of $G$. Let $G'$ be the second direct successor of $x_1$ whose inputs are $x_1^t, g_1, ..., g_r$ (see Fig. 1). We have shown above that $\bar{x}_2, ..., \bar{x}_j$ are prime implicants of $g_h$, $1 \leq h \leq r$. 

![Fig. 1](image-url)
Case 2: $j \geq 3$. Then the functions $g_1, \ldots, g_r$ are computed at different gates $G_1, \ldots, G_r$. If $G \neq G_1$, $x_2 = 0$ eliminates $j \geq 3$ input wires of $G$, at least 2 input wires of $G_1$, the wire from $G_1$ to $G'$ and the second output wire of $x_2$. Similar arguments hold for $x_3 = 0$. We eliminate in both situations less than 7 wires only if $\text{res}(G_1) = \tilde{x}_2 \lor \tilde{x}_3$. Since fan-out($x_2$) = 2, the circuit becomes independent of $x_2$ for $x_1 = 0$ and $x_3 = 0$. This is a contradiction.

Hence, we can assume $G = G_1$ and $r = 1$. Then $\text{res}(G') = (x_1 \lor (\tilde{x}_1 \lor \cdots \lor \tilde{x}_j))^b$. In this case, $a = 1$, otherwise $G'$ can be eliminated. $\text{res}(G') = (x_1 \tilde{x}_2 \lor \cdots \lor x_1 \tilde{x}_j)^a$, fan-out($G$) $\geq 2$; otherwise, $x_2 = \cdots = x_j = 1$ makes the circuit independent of $x_1$, $x_2 = 0$ eliminates $j \geq 3$ input wires of $G$, 2 input wires of $G'$, at least one further output wire of $G$ and at least one output wire of $G'$, hence, at least 7 wires.

Case 3: $j = 2$, $r \geq 2$. Since $\tilde{x}_2 \in \Pi(g_h)$ for $1 \leq h \leq r$, we can assume that $g_1, \ldots, g_{r-1}$ are computed at different gates $G_1, \ldots, G_{r-1}$. $x_2 = 0$ eliminates 2 input wires of $G$, $r + 1$ input wires of $G'$ and at least 2($r - 1$) input wires of $G_1, \ldots, G_{r-1}$. These are less than 7 wires only if $r = 2$, $G_1 = G$ and $g_2 = \tilde{x}_2$. Then $\text{res}(G') = (x_1^a \land \tilde{x}_2 \land (x_1 \lor x_2))$ can be computed by a fan-in 2 gate, and the circuit has not the minimal number of wires.

Case 4: $j = 2$, $r = 1$ and no wire leads from $x_2$ to $G'$. If a wire leads from $G$ to $G'$, $\text{res}(G') = (x_1^a \land (x_1 \land x_2)^b)^c$ can be computed by a fan-in 2 gate whose inputs are $x_1$ and $x_2$. This change of the circuit does not increase the number of wires. Afterwards, fan-out($x_2$) = 3 and we can argue as in Case 1. So we can assume that $g_1$ is computed at some gate $G_1 \neq G$. Since $\tilde{x}_2 \in \Pi(g_1)$, $x_2 = 0$ eliminates 2 input wires of $G$, 2 input wires of $G'$, at least 2 input wires of $G_1$, the second output wire of $x_2$, the output wires of $G$ and the output wires of $G_1$. These are less than 7 wires only if fan-in($G_1$) = 2, fan-out($G_1$) = fan-out($G$) = 1, and the inputs of $G_2$ are $x_2$ and $\text{res}(G)$. Then $\text{res}(G_1)$ can be computed directly by a fan-in 2 gate with inputs $x_1$ and $x_2$. $G$ can be eliminated and the circuit has not the minimal number of wires.

Case 5: $j = 2$, $r = 1$ and $x_2^a$ is the second input of $G'$. The inputs of $G'$ are $\tilde{x}_1$ and $\tilde{x}_2$. Otherwise, $x_1 = 0$ ($x_2 = 0$) makes the circuit independent of $x_2$ ($x_1$). If $\text{res}(G)$ enters a direct successor $G''$ positively, $x_2 = 0$ eliminates 2 input wires of $G$, 2 input wires of $G'$ (new output $\tilde{x}_1$), at least 2 input wires of $G''$ and at least one output wire of $G''$; hence, at least 7 wires. We can assume in the sequel that $\text{res}(G)$ and $\text{res}(G')$ enter all direct successors negatively.

Let $t = \text{fan-out}(G)$ and $t' = \text{fan-out}(G')$. $x_2 = 0$ eliminates the 4 input wires of $G$ and $G'$ and the $t$ output wires of $G$. Hence, we are done if $t \geq 3$ or $t' \geq 3$. If $t = t' = 1$, let $G_1$ be the successor of $G'$ and $G_2$, that of $G$. If $G_1 \neq G_2$, we can assume that no path leads from $G_1$ to $G_2$. Hence, we can replace $x_3, \ldots, x_n$ by constants in such a way that $G_2$ is replaced by 0. $x_2 = 1$ makes the circuit independent of $x_1$. This is a contradiction. Hence, $G_1 = G_2$. Also fan-in($G_1$) = 2. Otherwise, there is a replacement of $x_3, \ldots, x_n$ which makes the circuit independent of $x_1$ and $x_2$. $x_3 = 0$ eliminates the fan-in 2 gates $G$, $G'$ and $G_1$. We remark that in this case $x_1$ (and $x_2$) enters one gate positively and one gate negatively.

If $t = 2$ and $t' = 1$, $x_2 = 0$ eliminates the 4 input wires of $G$ and $G'$ and the 2 output wires of $G$. Afterwards, $x_1$ enters only $G_1$, the direct successor of $G'$. By our standard
arguments, $\text{res}(G_1)$ is replaced by $x_1^t$ and also the output wire of $G'$ can be eliminated. Altogether 7 wires can be eliminated. Similar arguments hold for $t=1$ and $t'=2$.

Finally, we consider the situation $t=t'=2$. $x_2=0$ eliminates the 4 input wires of $G$ and $G'$ and the 2 output wires of $G$. Afterwards, fan-out($x_1$) = 2 and $x_1$ enters its direct successors positively. We have eliminated only 6 wires. For the new circuit we apply the same case analysis. Either we can eliminate at least 7 wires then or we reach again Case 5 with $t=t' \in \{1, 2\}$. Then we eliminate only 6 wires but we still have some variable whose fan-out equals 2 and which enters its 2 direct successors positively. Hence, at some step of the process we eliminate 7 wires.

This completes our case analysis. □

5. Circuits of threshold gates of unbounded fan-in

The complexity of threshold circuits has been investigated by Hajnal et al. [2], Parberry and Schnitger [9] and Reif [11]. This model is motivated in various ways. Threshold circuits may simulate the behaviour of the human brain (see [9]). Threshold gates are the most powerful gates of practical use and importance (see also Section 6) and with threshold gates all symmetric and arithmetic functions are available in constant depth and polynomial size (see [1]). It is a hard problem to prove exponential lower bounds for threshold circuits of constant depth and functions in NC (see [2]).

We are interested in unbounded fan-in and depth circuits and the exact complexity of the parity function. Moreover, we prove some results which hold for all symmetric or even all Boolean functions.

Definition 5.1. A threshold gate $T_{\pm k}(T_{\pm k})$ operates on $n$ input wires, say $x_1, \ldots, x_n$, and outputs 1 if and only if $|x| = x_1 + \cdots + x_n \leq k$ ($|x| \geq k$).

We remark that $T_{\pm k}$ is a negative function and $T_{\pm k}$ is a monotone function. We shall see that in threshold circuits it may be useful to have several wires leading from gate $G$ or some input $x_i$ to gate $G'$. This was obviously useless for all circuit models discussed before. Hence, it is possible that the number of wires is exponentially larger than the number of gates and inputs.

Definition 5.2. A circuit is called synchronous if, for each gate all paths from the inputs to this gate have the same length. This length is called the depth of this gate.

It is well known that asynchronous circuits over binary bases, the $U_{\infty}$-basis or the basis of unbounded fan-in NOR gates cannot be much more efficient than synchronous circuits (see e.g. [14]). We shall prove that such an assertion is wrong for threshold circuits. This is a first example that asynchronous circuits can be much more powerful than synchronous circuits.
We consider at first synchronous threshold circuits and prove optimal bounds on the complexity of an arbitrary symmetric Boolean function. A Boolean function \( f \in \mathcal{B}_n \) is called symmetric (\( f \in \mathcal{S}_n \)) if \( f(x) \) depends only on \( |x| \), the number of 1's in the input, and not on their positions. We describe a symmetric function by its value vector \( v(f) = (v_0, \ldots, v_n) \) where \( v_i \) is the value of \( f \) on inputs with exactly \( i \) 1's. The vector \( v(f) \) consists of constant intervals, let \( I(f) \) be the number of maximal constant intervals, e.g. for \( v(f) = (0, 0, 1, 0, 1, 1, 0, 0) \) we have \( I(f) = 5 \).

A chain \( a = (a^0, \ldots, a^n) \), where \( a^i \in \{0, 1\}^n \), is a vector of vectors \( a^i \) such that \( a^i \) contains \( i \) 1's and \( a^i \leq a^{i+1} \) (\( \leq \) is defined componentwise). For a Boolean function \( f \) and a chain \( a \) let \( \text{Ch}(f, a) \) be the number of maximal constant intervals of the vector \( (f(a^0), \ldots, f(a^n)) \) and let \( \text{Ch}(f) \) be the maximum of all \( \text{Ch}(f, a) \) for chains \( a \).

Theorem 5.3. (i) \( \text{Ch}(f) = I(f) \) for all symmetric functions \( f \in \mathcal{S}_n \).

(ii) \( \text{Ch}(f) = 1 \) only for the constant functions. If \( I(f) = 2 \) for some symmetric function \( f \), then \( f \) is a threshold function and can be computed by a threshold circuit with 1 gate and \( n \) wires.

(iii) If \( I(f) \geq 3 \) for \( f \in \mathcal{S}_n \), \( f \) can be computed by a synchronous threshold circuit with depth 2, \( I(f) \) gates and \( (n + 1)(I(f) - 1) \) wires.

(iv) If \( \text{Ch}(f) \geq 3 \), each synchronous threshold circuit for \( f \in \mathcal{B}_n \) contains at least \( \text{Ch}(f) \) gates.

(v) The synchronous threshold complexity of symmetric functions \( f \) is \( I(f) \), if \( I(f) \geq 3 \), and \( I(f) - 1 \), if \( I(f) \leq 2 \). In particular, for \( n \geq 2 \), the parity functions \( f^\oplus_n \) have complexity \( n + 1 \) in synchronous threshold circuits.

Proof. (i) and (ii) are obvious, (v) follows directly from (i)–(iv).

(iii) We improve a construction of Hajnal et al. [2] who proved an upper bound of \( 2n \) for all symmetric functions. Since \( f \) and \( \bar{f} \) have the same complexity in threshold circuits (a negation at the output gate is free of charge), we assume without loss of generality that the first interval of \( v(f) \) consists of 0's. Then \( v(f) \) has \( \lfloor I(f)/2 \rfloor \) intervals consisting of 1's. If \( v_{i-1} = 0, v_i = \cdots = v_j = 1, v_{j+1} = 0, \) we use 2 threshold gates \( T_{\leq i}(x_1, \ldots, x_n) \) and \( T_{\leq j}(x_1, \ldots, x_n) \). These gates yield two 1's as outputs if and only if \( i \leq |x| \leq j \). If \( |x| \) is not in this range then one gate outputs 0 and the other outputs 1. If \( v_1 = \cdots = v_n = 1 \) and \( v_{i+1} = 0, \) we use only the threshold gate \( T_{\leq i}(x_1, \ldots, x_n) \) which computes 1 if and only if \( i \geq |x| \).

If \( I(f) \) is odd, we have \( \frac{1}{2}(I(f) - 1) \) intervals of ones and \( I(f) - 1 \) threshold gates in depth 1. If \( f(x) = 1 \), one pair of threshold gates yields two 1's as outputs and all other pairs yield a 1 and a 0. Hence, if \( g_j \) is the output of the \( j \)th gate on level 1,

\[
f(x) = T_{\geq (I(f) - 1)/2 + 1}^{I(f) - 1} (g_1, \ldots, g_{I(f) - 1}).
\]

If \( I(f) \) is even, we have \( \frac{1}{2}I(f) \) intervals of 1's, the first \( \frac{1}{2}I(f) - 1 \) intervals lead to a pair of threshold gates, altogether \( I(f) - 2 \) gates, and the last interval leads to one further
threshold gate. Hence, we have \( I(f) - 1 \) gates on level 1 computing \( g_1, \ldots, g_{I(f) - 1} \). Again, it is easy to see that

\[
f(x) = T_{I(f) - 1}^{I(f)}(g_1, \ldots, g_{I(f) - 1}).
\]

In both cases we obtain a synchronous circuit with depth 2 and \( I(f) \) gates. The bound on the number of wires follows by counting the wires in our construction.

(iv) We prove the lower bound by induction on \( \text{Ch}(f) \). If \( \text{Ch}(f) = 3 \), \( f \) is neither monotone increasing nor monotone decreasing. The threshold functions are monotone, increasing or decreasing. Hence, one gate is not sufficient. Also, there have to be wires from the first gate to the second gate if 2 gates are sufficient. Then, the second gate is on the second level and cannot be connected (because of synchronicity) directly with the inputs. But this implies that the second gate depends only on the first gate. Such a gate operates like an identity gate or a negation gate or a constant gate. This would imply that \( f \) could be computed already with one threshold gate. This is a contradiction!

Now we assume that \( \text{Ch}(f) = i \) and that the claim is proved for smaller values of \( \text{Ch}(f) \). Without loss of generality (by renumbering) \( a = (a'_0, \ldots, a'_n) \), the chain maximizing \( \text{Ch}(f, a) \), is of such a form that \( a'_j = 1 \) iff \( j \leq i \). Since the complexity of \( f \) and \( \tilde{f} \) are the same, without loss of generality \( f(a_0) = 0 \). Let \( j \) be the smallest index such that \( f(a^j) = 1 \). Since \( f(a^0) \neq f(a^j) \) and since the circuit is synchronous, the information about this fact has to pass through the first level of the circuit. Hence, there is some gate \( G \) on the first level of the circuit where \( \text{res}(G)(a^0) \neq \text{res}(G)(a^j) \). \( G \) is a threshold gate depending only on the inputs. Therefore, there are \( k_1, \ldots, k_n, k \geq 0 \) such that

\[
\text{res}(G)(x) = 1 \text{ iff } W(x) := \sum_{1 \leq i \leq n} k_i x_i \geq k \text{ (or } \leq k). \]

\( W(a^0) = 0 \) and \( W(a^j) = k_1 + \cdots + k_j \). Since \( \text{res}(G)(a^0) \neq \text{res}(G)(a^j) \), \( 0 < k \leq k_1 + \cdots + k_j \) (or \( 0 \leq k < k_1 + \cdots + k_j \)). We replace \( x_1, \ldots, x_j \) by 1's. Then \( G \) is replaced by the constant 1 (or 0). We obtain a threshold circuit for a subfunction \( g \) of \( f \). By the definition of \( g \), \( \text{Ch}(g) = \text{Ch}(f) - 1 \). Furthermore, the resulting circuit is synchronous. \( G \) is replaced by a constant and constant inputs of threshold gates can be eliminated. For 1-inputs the threshold value of the gate has to be changed in the obvious way. By the induction hypothesis, the resulting circuit for \( g \) contains at least \( \text{Ch}(g) = \text{Ch}(f) - 1 \) gates and we have proved the claim. \( \square \)

It has been shown [13] that the minimal sensitive complexity \( l_{\text{min}}(f) \) of a Boolean function \( f \) is an important complexity measure for unbounded fan-in circuits over the basis \{ \&, \lor, \neg \} and even for CRCW-PRAMs. \( l_{\text{min}}(f) \) is the minimum length (number of literals) of all prime implicants and prime clauses of \( f \). It is also the minimal number of variables which have to be replaced by constants in order to obtain a constant subfunction.
For symmetric functions $f \in S_n$, we know a very simple description of $l_{\min}(f)$. If $v_{\max}(f)$ is the maximum length of a constant subvector of $v(f)$, then $l_{\min}(f) = n + 1 - v_{\max}(f)$. For the parity functions, obviously, $v_{\max}(f^e) = 1$ and therefore $l_{\min}(f^e) = n$.

**Theorem 5.4.** (i) The parity functions can be computed in asynchronous threshold circuits with $\lceil \log(n+1) \rceil$ gates, less than $3n \lceil \log(n+1) \rceil$ wires and depth $\lceil \log(n+1) \rceil$.

(ii) Asynchronous threshold circuits for an arbitrary Boolean function $f \in B_n$ have at least $\lceil \log(n+1) - \log(n+1-l_{\min}(f)) \rceil$ gates. For symmetric functions this bound equals $\lceil \log(n+1) - \log(v_{\max}(f)) \rceil$, and for the parity functions this is equal to $\lceil \log(n+1) \rceil$.

**Proof.** (i) We prove the upper bound only for the case $n = 2^k - 1$ since, otherwise, we can pad the input with 0’s. For the design of the circuit we take up ideas from the binary search method. But this simple and powerful method cannot be applied in its pure form. If-tests are not available in circuits. So we make the most of the fact that the value vector of the parity functions again is totally symmetric. For $n = 2^k - 1$ it is a vector of length $2^k$, where all $2^k-1$ blocks of length $2^l$ are equal. Such properties are not necessary for the typical use of binary search. At first we explain the ideas in the special case $n = 15$ (see Fig. 2). A wire from $x$ to some gate means that there is a wire from each $x_i$ to this gate. A wire with label $l$ from some gate to another means that there are $l$ wires connecting these gates. Let $s = \lvert x \rvert = x_1 + \cdots + x_{15}$. Then $s$ can take the values $0, \ldots, 15$ and 4 bits are sufficient to describe $s = (s_3, s_2, s_1, s_0)$. Obviously, $f_{15}^e(x) = s_0$.

We number the gates in inverse order from $G_3$ to $G_0$. Obviously, the first gate $G_3$ computes 1 iff $s_3 = 0$. $\text{res}(G_2) = 1$ iff $s_2 = 0$. The number of 1’s entering $G_2$ is $(8s_3 + 4s_2 + 2s_1 + s_0) + 8s_3$, the first term is the number of 1’s coming from the inputs,
the second one, the number of 1's coming from $G_3$. But $8s_3 + 8\bar{s}_3 = 8$. Hence,

$$\text{res}(G_3) = 1 \iff 4s_2 + 2s_1 + s_0 \leq 3 \iff s_2 = 0.$$ 

$$\text{res}(G_4) = 1 \iff s_1 = 0.$$ 

The number of 1's entering $G_1$ is $8s_3 + 4s_2 + 2s_1 + s_0 + 8\bar{s}_3 + 4\bar{s}_2 = 12 + 2s_1 + s_0$. Hence,

$$\text{res}(G_1) = 1 \iff 2s_1 + s_0 \leq 1 \iff s_1 = 0.$$ 

Finally, the number of 1's entering $G_0$ is $8s_3 + 4s_2 + 2s_1 + s_0 + 8\bar{s}_3 + 4\bar{s}_2 + 2\bar{s}_1 = 14 + s_0$. Hence,

$$\text{res}(G_0) = 1 \iff s_0 = 1 \iff \text{f}_1^*(x_1, \ldots, x_{15}) = 1.$$ 

Now the design for the general case is straightforward. The $k$ gates are ordered in the inverse order $G_{k-1}, \ldots, G_0$. There is one wire from each $x_i$ to each $G_j$. There are exactly $2^j$ wires from $G_j$ to each $G_i$, where $i < j$. $G_j$ computes 1 iff the number of incoming 1's is at most $(2^{k-1} - 1) + 2^{k-2} + \cdots + 2^j$. Obviously, the number of gates and the depth of the circuit are equal to $k = \lceil \log(n + 1) \rceil$. The fan-in of each gate is bounded by $n + (2^{k-1} - 1) + 2^{k-2} + \cdots + 2\leq n + 2^{k-1} = 2n$. Hence, the number of wires is bounded by $2n\lceil \log(n + 1) \rceil$ for $n = 2^{k-1}$. For general $n$, $2^{k-1} \leq n \leq 2^k - 1$, we can estimate the fan-in of each gate also by $n + 2^{k-1}$ which is not larger than $3n$.

The correctness of the circuit is proved by the proof of the following claim. Let $s = (s_{k-1}, \ldots, s_0)$ be the binary representation of $x_1 + \cdots + x_n$. Then we claim that $\text{res}(G_j) = 1 \iff s_j = 0$. For $j = 0$ this implies that $f_n^1$ is computed at $G_0$. We prove the claim by downward induction on $j$. The proof for the induction basis $j = k - 1$ is obvious by the design of the circuit. Let the claim be proved for $j' > j$. We count the number of 1's entering $G_j$. By induction hypothesis this is

$$2^{k-1}s_{k-1} + \cdots + 2^0s_0 + 2^{k-1}\bar{s}_{k-1} + \cdots + 2^j\bar{s}_{j+1}$$

$$= 2^{k-1} + \cdots + 2^j + 2^j s_j + \cdots + 2^0s_0.$$ 

This number is not larger than the threshold of $G_j$ iff

$$2^{k-1} + \cdots + 2^j + 2^j s_j + \cdots + 2^0s_0 \leq (2^{k-1} - 1) + 2^{k-2} + \cdots + 2^j + 2^j$$

$$\iff 2^j s_j + \cdots + 2^0s_0 \leq 2^j - 1 \iff s_j = 0.$$ 

(ii) We consider a first gate $G$ of a threshold circuit for $f$. For this gate we can be sure that all incoming wires are from the variables. Hence, for some $k_1, \ldots, k_n, k \geq 0$, we have

$$\text{res}(G) = 1 \iff k_1 x_1 + \cdots + k_n x_n \geq k \text{ (or } \leq k).$$ 

Let $j$ be the minimal number such that $k_1 + \cdots + k_j \geq k$. Such a $j$ exists, otherwise the gate would compute a constant. Furthermore, $k_j > 0$. If we replace $x_1, \ldots, x_j$ by 1's, $G$ is replaced by the constant 1. If we replace $x_1, \ldots, x_n$ by 0's, $G$ is replaced by the constant 0 since $k_1 + \cdots + k_{j-1} < k$. For a negative threshold gate, a dual argument works. Hence, by replacing $\min\{j, n + 1 - j\} \leq \lceil (n + 1)/2 \rceil$ variables by constants, we can eliminate the first gate of the circuit. The resulting subfunction is defined on at least $n - \lceil (n + 1)/2 \rceil = \lceil (n + 1)/2 \rceil - 1$ variables. We continue in the same way until we
obtain a constant subfunction. After \( k \) iterations the number of variables of the resulting subfunction is at least \( \left[(n+1)/2^k\right]-1 \) (easy induction). We conclude that threshold circuits for \( f \) have at least \( k \) gates for the smallest \( k \), where

\[
\left[(n+1)/2^k\right]-1 \leq n-l_{\text{min}}(f).
\]

This holds also for the smallest \( k \) such that

\[
\frac{n+1}{2^k} - 1 \leq n-l_{\text{min}}(f),
\]

i.e.

\[
\frac{n+1}{n+1-l_{\text{min}}(f)} \leq 2^k.
\]

Hence, \( \left[ \log(n+1) - \log(n+1-l_{\text{min}}(f)) \right] \) is a lower bound on the number of gates in any threshold circuit for \( f \). The special forms of the lower bounds for symmetric functions or the parity functions follow easily. \( \Box \)

6. Practical aspects

We have determined the complexity of parity functions in various circuit models. In this last section we ask whether our results have implications in real-life circuit design. It is an established fact that parity circuits are often used. We cite from the paper of Lai and Muroga [5]: “Although a MOS logic gate can be made to realize a complex negative function, a NOR gate implemented by a MOS logic is widely used in practice due to its compact layout. The same is true with GaAs.” A more detailed discussion can be found in the monograph of Muroga [6].

We have seen that optimal NOR circuits have \( 3n-2 \) gates and \( 8(n-1) \) wires. The fan-in of the gates in the optimal circuits is 2, 3 and 4. Optimal \( U_\omega \)-circuits have also nonnegative gates, the number of gates is at least \( 2n-1 \) and the number of wires is at least \( 6(n-1) \). Furthermore, this small number of wires is not possible for circuits with less than \( 3(n-1) \) gates. These are arguments why \( U_\omega \)-circuits are not better than NOR circuits in practice.

Threshold circuits for the parity functions may have a very small number of gates. This circuit design in its pure form is impractical because the gates are very complex and have a very large fan-in. But we see that we have used only negative gates. In Fig. 3 we see the circuits for \( n=3 \) and \( n=7 \). The circuit for \( n=3 \) has 2 gates, one of fan-in 3 and one of fan-in 5 where the last 2 inputs have always the same value. It is
easy to see that both types of gates can be easily designed in MOS logic. For odd \( n \), \( \frac{1}{2}(n-1) \) of these subcircuits are sufficient to compute a parity function on \( n \) variables. This can be done by a balanced tree of fan-in 3 parity gates (hence, we have logarithmic depth), where each gate is replaced by our threshold circuit. This design is regular and simple, the number of gates is \( n-1 \) for odd \( n \) and \( n \) for even \( n \), the number of wires is \( \frac{3}{2}(n-1) + \frac{2}{2}(n-1) = 4(n-1) \) for odd \( n \) and \( 4(n-1) + 2 \) for even \( n \). The optimal threshold circuit for \( n=7 \) has 3 gates with fan-in 7, 11, 13. If these gates can be designed efficiently, we need only \( 3\left[\frac{1}{2}(n-1)\right] = \frac{3}{2}(n-1) \) gates if \( n \equiv 1 \mod 7 \) and \( (7 + 11 + 13) \frac{1}{2}(n-1) = \frac{3}{2}(n-1) \approx 5.17(n-1) \) wires. But the gates are much more complicated than in the other designs.

In the following table, we compare the optimal NOR circuit and the designs using threshold circuits for the parity of 3 or 7 inputs as subcircuits. All three designs have logarithmic depth. We think that the threshold circuit type 1 uses only simple gates and is the best of the considered circuits for real-life circuit design for the parity functions. It turns out that the investigation of threshold circuits is interesting for theoretical and for practical purposes.

Table 1

<table>
<thead>
<tr>
<th>Type of gates</th>
<th>NOR circuit</th>
<th>Threshold circuit type 1</th>
<th>Threshold circuit type 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of gates</td>
<td>( 3(n-2) )</td>
<td>( T_{\ell,1}^2, T_{\ell,2}^5 )</td>
<td>( T_{\ell,3}^7, T_{\ell,4}^4, T_{\ell,5}^4 )</td>
</tr>
<tr>
<td>Number of wires</td>
<td>( 8(n-1) )</td>
<td>( 4(n-1) )</td>
<td>( \frac{3}{2}(n-1) )</td>
</tr>
</tbody>
</table>

References


