LEAD-PATTERN POTENTIALS AND EXACT VALUES OF MERGING NETWORKS

TEJASVI SINGH TOMAR

ABSTRACT. Let $M(m,n)$ be the least number of comparators in a network that merges sorted lists of lengths m and n. We settle nine of the seventeen values of $M(m,n)$ that were listed as open in 2009, among them $M(6,9)=25$, $M(8,9)=29$ and $M(7,24)=62$. We also prove $M(5,n)=C(5,n)$ for all n and $M(6,8k)=18k+4$ for all $k\geq 1$, where $C(m,n)$ is the size of Batcher's odd-even merge; the second formula is new, and so is the first for $n\equiv 2,3,4,7 \pmod 8$. In all these cases Batcher's odd-even merge is optimal. The lower bounds come from potentials on the monotone Boolean functions computed on the wires of a network, potentials that grow by at most one at each comparator. The best such bound is the optimum of a linear program. For merging networks we round its solutions, and those of a sharper variant, to exact rational certificates, which are checked by short programs. Potentials in closed form, proved feasible by a finite computation, give the formulas and the values for $m=7$. For sorting networks on six channels the sharper variant attains the least size, 12. The values and formulas are also proved in Lean 4, with checks that run as compiled code.

1. INTRODUCTION

Merging networks are the building blocks of Batcher's sorting networks [3]. How few comparators they need is a classical problem [8]. Upper bounds come from explicit networks, whereas a lower bound has to rule out every network with fewer comparators. An (m,n)-merging network merges two sorted sequences of lengths m and n by a fixed sequence of comparators, and $M(m,n)$ denotes the least number of comparators of such a network. Batcher's odd-even merge [3, 8] has $C(m,n)$ comparators, where

$$C(m,n)=\begin{cases} C(\lceil m/2\rceil,\lceil n/2\rceil)+C(\lfloor m/2\rfloor,\lfloor n/2\rfloor)+\lfloor (m+n-1)/2\rfloor & \text{if } mn>1,\\ mn & \text{if } mn\leq 1.\end{cases}$$

Lower bounds that match $C(m,n)$ are known only for some families of pairs (m,n), recalled below, and several small cases have remained open.

Our lower bounds come from potentials. Fix a set P of 0-1 inputs. For merging, P consists of the inputs whose two parts are sorted. Each lead of a network then has a pattern, the set of inputs on which it carries a 1. A comparator turns the patterns f and g of the two leads entering it into $f\cup g$ and $f\cap g$. Suppose that a function w on patterns satisfies $w(f\cup g)+w(f\cap g)-w(f)-w(g)\leq 1$ whenever f and g are incomparable. Then the total potential of the live leads rises by at most one per comparator. Hence the size of the network is at least the potential of the output patterns minus that of the input patterns. Every network that sorts P has the same input and output patterns, so this difference depends only on w. Maximizing it over w is a linear program. We call its optimum the LTP bound, after the lead-pattern potentials it ranges over. On merging

Date: 29 October 2026.

2020 *Mathematics Subject Classification.* Primary 68P10; Secondary 68Q06, 90C05.

Key words and phrases. Merging networks, sorting networks, comparator networks, lower bounds, linear programming, certificates.

networks its solutions can be rounded to exact rational certificates, which we check with two short programs (Section 5). Our main results are the following.

Theorem 1.1. *$M(5,7) = 18$, $M(6,8) = 22$, $M(6,9) = 25$, $M(7,9) = 27$, $M(8,9) = 29$, $M(5,15) = 35$, $M(5,10) = 25$, $M(5,11) = 27$, $M(5,12) = 29$ and $M(6,10) = 27$. In each case Batcher's odd-even merge is optimal.*

Theorem 1.2. *$M(5,n) = C(5,n)$ for every $n \geq 1$, that is, $M(5, 8k + r) = 17k + c_r$ for all $k \geq 0$ and $1 \leq r \leq 8$, where $(c_1, \ldots, c_8) = (5, 8, 10, 12, 13, 16, 18, 20)$. For every $k \geq 1$, $M(6, 8k) = 18k + 4 = C(6, 8k)$. In particular $M(5, 23) = 52$ and $M(6, 24) = 58$.*

Theorem 1.3. *$M(7, 16) = 43$ and $M(7, 24) = 62$. In both cases Batcher's odd-even merge is optimal.*

Each value of Theorem 1.1 rests on a certificate for one pair (m, n). Theorems 1.2 and 1.3 rest on potentials in closed form for $m = 5$, 6 and 7, and a computer check of all configurations (Lemma 3.6) shows that each of them is feasible for all n of its residue class (Section 7).

Earlier work settles $m \leq 4$ and several residue classes for $5 \leq m \leq 9$. Yao and Yao [13] found $M(2, n) = \lceil 3n/2 \rceil$, and Aigner and Schwarzkopf [1] and Amano and Maruoka [2, Thm. 2] found $M(3, n) = \lceil (7n + 3)/4 \rceil$.[1] Iwata [7] proved $M(4, n) = C(4, n)$ for $n \equiv 0, 1, 3 \pmod 4$ and $M(5, n) = C(5, n)$ for $n \equiv 0, 1, 5 \pmod 8$, and found the values $M(6, 8k + 6)$, $M(7, 8k + 7)$ and $M(8, 8k + 8)$ and the linear coefficient $\lim_n M(m, n)/n$. Amano and Maruoka [2] found $M(4, 4k+2) = 8k+6$ (Thm. 7) and sketched a proof of $M(5, 8k+6) = 17k+16$ (Thm. 12), which covers, for example, $M(5, 14)$, and Morohashi and Iwata [10] found $M(6, 8k + 7)$, $M(9, 16k + 9)$ and $M(7, 8) = 24$. Table 2 sets our results on $M(m, n)$ against this record, case by case.

The table of Morohashi and Iwata [10, Table 1], extended by rows for $m \leq 4$ in Morohashi's 2009 thesis [9, Table 5.1], lists seventeen entries as open; Table 2 lists them too, with their bounds. For $M(7, 9)$ and $M(8, 9)$, Morohashi's thesis proves $M(n, n) = M(n-1, n)+1 = M(n-2, n)+3$ under a conjecture on the positions of the leftmost comparators [9, Thm. 4] (see also [10]). Together with $M(9, 9) = 30$, a value of the same table, this would give $M(8, 9) = 29$ and $M(7, 9) = 27$. The pairs $(5, 15)$ and $(5, 23)$ are not covered by Theorem 12 of [2], since $15 \equiv 23 \equiv 7 \pmod 8$. The 2009 table has columns only for $n \leq 9$ and $n = 15, 23, 24, 25$, so it does not cover $M(5, 10)$, $M(5, 11)$, $M(5, 12)$, $M(6, 10)$, $M(6, 16)$ and $M(7, 16)$, and we have not found any of them determined in the literature.

Section 2 fixes the notation. Section 3 introduces the LTP bound and its dual. It refines the bound by the fact that the two leads entering a comparator never carry a common up-step (Lemma 3.3), on which Theorems 1.2 and 1.3 and our certificates for seven of the ten values of Theorem 1.1 rely. It also reduces the checks of potentials that depend only on a few features of a pattern to finitely many cases, with a smaller range for the pairs that Lemma 3.3 allows (Lemmas 3.6 and 3.7). Section 4 shows that the number of comparators that separate two given inputs, or split a given set of inputs, is the same for every network that sorts these inputs, and that LTP is the least fractional number of comparator operations that meets all of these counts. Section 5 explains how the certificates are produced and checked, and describes an exhaustive search that serves as an independent check for all pairs on up to 14 channels and for $(6, 9)$ and $(5, 10)$ on 15. Section 6 proves Theorem 1.1. Section 7 gives closed-form potentials for $m = 2$, for $m = 3$ with $n \geq 8$, for $m = 4$ with n odd and for the linear coefficient; its potentials for $m = 5$ and for $m = 6$ with $n \equiv 0, 6, 7 \pmod 8$ prove Theorem 1.2, and one for $m = 7$ with even

[1] Aigner and Schwarzkopf [1] prove the formula for $n \equiv 0, 1, 3 \pmod 4$ and state the case $n \equiv 2$ without a detailed proof; Amano and Maruoka [2, Thm. 2] prove that case. Our account of [1] and [7] follows [2] and [10, p. 238], and we were unable to consult [1] itself. The 2004 paper [10, p. 238] credits Aigner and Schwarzkopf alone with the formula for $M(3, n)$.

n proves Theorem 1.3. Section 8 turns to general comparator networks, among them sorting networks on six channels, and Section 9 describes the proofs in Lean 4.

2. Preliminaries

Let $P \subseteq \{0,1\}^c$ be a set of 0-1 vectors on c channels, ordered componentwise. A comparator network is a sequence of comparators, and a *lead* is a wire segment between consecutive comparators. Every lead computes a monotone Boolean function of the input, and its *pattern* is the set of vectors of P on which this function is 1. A pattern is an up-set of $(P, \leq)$, and every up-set is the pattern of some monotone function. Let $\mathcal{U}(P)$ be the set of up-sets. A comparator with input patterns f, g has output patterns $f \cup g$ (maximum) and $f \cap g$ (minimum). Input channel i has pattern $X_i = \{p \in P : p_i = 1\}$. If the network sorts P, the output of rank r, counted from $r = 0$ at the bottom, has pattern $T_r = \{p \in P : |p| \geq c - r\}$.

We write $s(P)$ for the least size of a network that sorts P when the outputs may be listed in any order. Allowing generalized comparators as well does not change this value. For sets that are unions of maximal chains of $\{0,1\}^c$, such as merging sets, $s(P)$ can be computed by a version of Harder's exact search [6, 5] (Section 5).

For merging, the channels form two chains A and B of lengths m and n. For $0 \leq i \leq m$ and $0 \leq j \leq n$, the point (i, j) is the vector with ones on the top i channels of A and on the top j channels of B, and P is the set of these points. Since a merging network sorts P, we have $s(P) \leq M(m, n)$. This is the only direction we use. The points $(k, 0), \ldots, (k, n)$ form *row* k. An up-set U of P is determined by its *staircase* $t = (t_0, \ldots, t_m)$, where t_k is the least j with $(k, j) \in U$, and $t_k = n + 1$ if row k misses U. The staircases are exactly the sequences $n + 1 \geq t_0 \geq t_1 \geq \cdots \geq t_m \geq 0$, so there are $\binom{m+n+2}{m+1}$ of them. Union and intersection of up-sets are the componentwise minimum and maximum of staircases. The input channels of A have the staircases $(n + 1, \ldots, n + 1, 0, \ldots, 0)$ with between 1 and m zeros, the input channels of B have the constant staircases $(v, \ldots, v)$ with $1 \leq v \leq n$, and T_r has the entries $t_k = \min(n + 1, \max(0, m + n - r - k))$.

3. Lead-pattern potentials

Definition 3.1. For $w : \mathcal{U}(P) \to \mathbb{R}$ with $w(\emptyset) = w(P) = 0$ put $\mathrm{def}_w(f, g) = w(f \cup g) + w(f \cap g) - w(f) - w(g)$ and $\Phi(w) = \sum_r w(T_r) - \sum_i w(X_i)$. Then $\mathrm{LTP}(P) = \max \Phi(w)$ subject to $\mathrm{def}_w(f, g) \leq 1$ for all incomparable $f, g \in \mathcal{U}(P)$.

Theorem 3.2. *For every P, $s(P) \geq \lceil \mathrm{LTP}(P) \rceil$, and $\mathrm{LTP}(P') \leq \mathrm{LTP}(P)$ for $P' \subseteq P$.*

Proof. Process the comparators in a topological order. The multiset of live patterns starts as $\{X_i\}$ and ends as $\{T_r\}$. This holds for any listing of the outputs, because the outputs of the vectors of P then have nested supports. A comparator on patterns (f, g) changes $\sum w$ over the live leads by $\mathrm{def}_w(f, g)$, which is 0 if f, g are comparable and at most 1 otherwise. Telescoping yields $s(P) \geq \Phi(w)$. For $P' \subseteq P$ and w' feasible on P', the potential $w(f) = w'(f \cap P')$ is feasible on P and has the same Φ. Indeed, restriction commutes with $\cup$ and $\cap$, so $\mathrm{def}_w(f, g) = \mathrm{def}_{w'}(f \cap P', g \cap P')$, which is 0 if $f \cap P'$ and $g \cap P'$ are comparable and at most 1 otherwise. □

An *up-step* of P is a pair $(v, v + e_i)$ with both vectors in P. A lead *carries* it if its function is 0 on v and 1 on $v + e_i$.

Lemma 3.3 (disjoint carried steps)**.** *At every cut of a comparator network, every up-step of P is carried by exactly one live lead, and v, $v + e_i$ agree on all other live leads. In particular the two inputs of a comparator carry disjoint sets of up-steps.*

Proof. At the inputs, v and $v + e_i$ differ exactly on channel i. Assume the claim before a comparator on leads x, y, with carrying lead l. If $l \notin \{x, y\}$, both inputs, and hence both outputs, agree on v and $v + e_i$. Let $l = x$, and let b be the common value of y on v and $v + e_i$. For $b = 0$ the outputs are $(0, 0)$ on v and $(0, 1)$ on $v + e_i$, and for $b = 1$ they are $(0, 1)$ and $(1, 1)$. In both cases exactly one output carries the step. □

By the lemma, the constraints of LTP are needed only for incomparable pairs (f, g) whose sets of carried steps are disjoint. We write $\mathrm{LTP}^{\mathrm{disj}}(P)$ for the optimum of the LP with only these constraints. Then $\mathrm{LTP}(P) \le \mathrm{LTP}^{\mathrm{disj}}(P) \le s(P)$, and the monotonicity of Theorem 3.2 holds for $\mathrm{LTP}^{\mathrm{disj}}$ too, since steps carried disjointly in P are carried disjointly in P'. We call certificates checked on all incomparable pairs *plain*, and those checked only on the pairs with disjoint carried steps *disjoint*.

On merging sets the carried steps can be read off the staircase. Row k carries exactly one B-step, $(k, t_k - 1) \to (k, t_k)$, if $1 \le t_k \le n$, and none otherwise. The A-step $(k, j) \to (k + 1, j)$ is carried if and only if $t_{k+1} \le j < t_k$. For $0 \le k < m$ we say that *kind* k is *active* in t if $t_k > t_{k+1}$, that is, if t carries some A-step between rows k and $k + 1$.

Proposition 3.4 (duality)**.** $\mathrm{LTP}(P)$ *equals the least total weight of a nonnegative combination of comparator operations* $(f, g) \mapsto (f \cup g, f \cap g)$ *that transforms the multiset* $\{X_i\}$ *of input patterns into the multiset* $\{T_r\}$ *of output patterns, counted coordinatewise on* $\mathcal{U}(P) \setminus \{\emptyset, P\}$*. We call such a combination a fractional network. In particular, if a network* N *for* P *contains, on some leads at one cut, a subnetwork* N' *that sorts the image* $\varphi(P)$*, where* $\varphi(p)$ *is the vector of values on those leads for the input* p*, then* $\mathrm{LTP}(P) \le |N| - |N'| + \mathrm{LTP}(\varphi(P))$.

The first statement is LP duality. For the second, we pull back an optimal fractional network for $\varphi(P)$ along φ, which commutes with $\cup$ and $\cap$ and preserves disjointness of carried steps.

Example 3.5. Let $m = n = 2$. The up-sets of P are the 20 staircases (t_0, t_1, t_2) with $3 \ge t_0 \ge t_1 \ge t_2 \ge 0$. Let $w(t)$ be 0, 1 or 3/2 according as none, one or both of the kinds 0 and 1 are active in t. Then $w(\emptyset) = w(P) = 0$, and a check of the 35 incomparable pairs shows $\mathrm{def}_w \le 1$. The inputs have the staircases $(3, 0, 0)$ and $(3, 3, 0)$ on A and $(1, 1, 1)$ and $(2, 2, 2)$ on B, with weights 1, 1, 0 and 0. The outputs $T_0, \dots, T_3$ have the staircases $(3, 3, 2)$, $(3, 2, 1)$, $(2, 1, 0)$ and $(1, 0, 0)$, with weights 1, 3/2, 3/2 and 1. Hence $\Phi(w) = 5 - 2 = 3$, and Theorem 3.2 gives $M(2, 2) \ge 3$. Batcher's network attains this bound. Its first comparator acts on $(3, 3, 0)$ and $(2, 2, 2)$ and produces $(2, 2, 0)$ and $(3, 3, 2)$. The second acts on $(3, 0, 0)$ and $(1, 1, 1)$ and produces $(1, 0, 0)$ and $(3, 1, 1)$, and the third acts on $(2, 2, 0)$ and $(3, 1, 1)$ and produces $(2, 1, 0)$ and $(3, 2, 1)$. Each of the three comparators raises the total weight of the live leads by exactly 1.

The potentials of Section 7 depend only on a few features of a staircase. This makes their checks finite. Call a potential w on the staircases of $M(m, n)$ *typed* if $w(t)$ depends only on the order relations among $t_0, \dots, t_m$, 0 and $n + 1$, and possibly on the residues of $t_0, \dots, t_m$ modulo a fixed integer $Q \ge 2$. These data form the *type* of t. We give a typed potential by a weight for each type and use the same weights for every n. The *configuration* of a pair (f, g) of staircases consists of the order relations among the $2m + 2$ entries of f and g, 0 and $n + 1$, together with the residues of the entries modulo Q if w uses residues.

Lemma 3.6 (finite checks)**.** *Let* w *be a typed potential on the staircases of* $M(m, n)$*.*

(i) The configuration of a pair (f, g) *determines* $\mathrm{def}_w(f, g)$*, whether* f *and* g *are comparable, and whether their sets of carried steps are disjoint. Let the configuration have* s *gaps, as defined in the proof; then* $s \le 2m + 3$*. If* w *ignores residues, a configuration that occurs for some* n *occurs for every* $n' \ge s - 1$*, hence for every* $n' \ge 2m + 2$*. Otherwise it occurs for every* $n' \ge Qs - Q$ *with* $n' \equiv n \pmod{Q}$*, hence for every such* $n' \ge Q(2m + 2)$*.*

(ii) For $n \geq m$, the number of input staircases of each type and the number of output staircases of each type are affine functions of n, on each residue class of n modulo Q if w uses residues. Hence $\Phi(w)$ is affine in n on these ranges.

Proof. (i) The entries of $f \cup g$ and $f \cap g$ are minima and maxima of entries of f and g, so the configuration determines the order relations and residues of the entries of all four staircases, hence their types and $\mathrm{def}_w(f, g)$. Comparability is a matter of order relations, and so is the disjointness of carried steps: f and g share a B-step if and only if $f_k = g_k$ with $1 \leq f_k \leq n$ for some k, and they share an A-step of kind k if and only if $\max(f_{k+1}, g_{k+1}) < \min(f_k, g_k)$. Now let $0 = v_0 < v_1 < \cdots < v_s = n + 1$ be the distinct values among the entries, 0 and $n + 1$. The configuration has the s gaps $v_i - v_{i-1}$, and $s \leq 2m + 3$ because the two staircases have $2m + 2$ entries. Replacing the gaps by other positive integers keeps all order relations, and, since $v_0 = 0$, it keeps all residues modulo Q if each gap keeps its residue. Gaps of 1 give $n' = s - 1$. If $n + 1 > Qs$, some gap is at least $Q + 1$, and narrowing it by Q gives the same configuration at $n - Q$. Repeating this, we reach some $n_0 \equiv n \pmod{Q}$ with $n_0 \leq Qs - 1$. Enlarging one gap by 1, or by Q when residues matter, then reaches every larger n', congruent to n modulo Q in the second case. There the least $n' \geq Qs - Q$ with $n' \equiv n \pmod{Q}$ is the largest integer below Qs that is congruent to n, so it is at least n_0.

(ii) The inputs on A have the same types for all n in one residue class. The inputs on B are the staircases $(v, \ldots, v)$ with $1 \leq v \leq n$, and the type of such a staircase depends only on the residue of v. The output T_r is the staircase with $t_k = \min(n + 1, \max(0, x - k))$, where $x = m + n - r$ runs through $1, \ldots, m + n$. For $m < x \leq n$ its entries satisfy $n \geq t_0 > t_1 > \cdots > t_m \geq 1$, so its type depends only on the residue of x. For $x \leq m$ it is $(x, x - 1, \ldots, 1, 0, \ldots, 0)$, independent of n. For $x = n + 1 + d$ with $0 \leq d < m$ its entries are $n + 1$ for $k \leq d$ and $n + 1 + d - k \geq 1$ otherwise, so its type depends only on d and the residue of n. Counting the values of v and x in each residue class gives affine functions of n on each residue class of n. □

Lemma 3.7 (distinct entries)**.** *If two staircases f and g of $M(m, n)$ have $2m + 2$ distinct entries and disjoint sets of carried steps, then they are comparable. Hence the configuration of an incomparable pair with disjoint carried steps has at most $2m + 2$ gaps, and for such pairs the ranges in Lemma 3.6(i) become $n' \geq 2m + 1$ and $n' \geq Q(2m + 1)$.*

Proof. The staircase f carries the A-steps of kind k at the columns j with $f_{k+1} \leq j < f_k$, and g at those with $g_{k+1} \leq j < g_k$. As the entries are distinct, these two sets of columns are disjoint only if $f_k < g_{k+1}$ or $g_k < f_{k+1}$. Say $g_0 < f_1$; the other case is symmetric. If $g_k < f_{k+1}$ and $k + 1 < m$, then $f_{k+1} < g_{k+2}$ is impossible, since $g_{k+2} < g_k < f_{k+1}$, and so $g_{k+1} < f_{k+2}$. By induction $g_k < f_{k+1} < f_k$ for every $k < m$, and $g_m < g_{m-1} < f_m$. Hence $g < f$ entrywise, and f and g are comparable. The entries of an incomparable pair with disjoint carried steps are therefore not distinct, so together with 0 and $n + 1$ they take at most $2m + 3$ values, and there are at most $2m + 2$ gaps. □

4. Split identities

Theorem 4.1. *Let $p, q \in P$ be incomparable and $d(p, q) = \min(|p|, |q|) - |p \wedge q|$. Every network that sorts P contains exactly $d(p, q)$ comparators whose input patterns f, g satisfy $p \in f \setminus g$ and $q \in g \setminus f$ (or the reverse).*

Proof. Let N_{pq} be the number of live leads whose pattern contains both p and q. A comparator changes N_{pq} by $[\{p, q\} \subseteq f \cup g] + [\{p, q\} \subseteq f \cap g] - [\{p, q\} \subseteq f] - [\{p, q\} \subseteq g]$, which is 1 if it separates p and q as stated and 0 otherwise. It starts at $|p \wedge q|$ and ends at $\min(|p|, |q|)$. □

Theorem 4.2. *For nonempty $T \subseteq P$ let $d(T) = \min_{v \in T} |v| - |\bigwedge T|$. Every network that sorts P contains exactly $d(T)$ comparators whose input patterns f, g satisfy $T \subseteq f \cup g$, $T \cap (f \setminus g) \neq \emptyset$ and $T \cap (g \setminus f) \neq \emptyset$.*

The proof is the same, with N_T the number of live leads whose pattern contains T. A comparator changes N_T by 1 if $T \subseteq f \cup g$ but T lies in neither f nor g, which is the split condition, and by 0 otherwise. Moreover N_T starts at $|\bigwedge T|$ and ends at $\min_{v \in T} |v|$. Writing a potential in Möbius form $w(f) = \sum_{\emptyset \neq T \subseteq f} \mu(T)$ turns Φ into $\sum_T \mu(T) d(T)$ and each constraint into $\sum_T \mu(T) \delta_T(f, g) \leq 1$, where δ_T indicates the split of Theorem 4.2. Hence $\mathrm{LTP}(P)$ is the least fractional number of comparator operations that reproduces every count $d(T)$, whereas every real network reproduces them with integer weights.

Remark 4.3 (degree truncations). Restricting μ to sets of size at most k gives a nondecreasing hierarchy $\mathrm{LTP}_2 \leq \mathrm{LTP}_3 \leq \dots$. It reaches LTP once k is at least the width of P, because every function on $\mathcal{U}(P)$ is a combination of the functions $f \mapsto [T \subseteq f]$ with T an antichain. For $k = 2$, write $\beta(p, q) = \mu(\{p, q\})$ and $\beta(A \times B) = \sum_{p \in A,\, q \in B} \beta(p, q)$. Then the constraint reads $\beta(A \times B) \leq 1$ for every pair $(A, B) = (f \setminus g, g \setminus f)$, that is, for all disjoint convex sets A, B with $A \times B$ incomparable. Every pair of disjoint subsets of an antichain qualifies. For $\beta \geq 0$ on an antichain, the largest $\beta(A \times B)$ is the weight of a maximum cut, so separation for LTP_2 contains MAX-CUT and is NP-hard. The same holds for every constraint family that contains these antichain pairs: adding constraints keeps the bound valid, but dropping them in general does not. The truncation is also strictly weaker in general. On the cube $\{0, 1\}^5$ the values are 7.789 for $k = 2$, 8.057 for $k = 3$ and 8.75 for full LTP, while the least size of a sorting network on 5 channels is 9.

5. Certificates and verification

A certificate for $M(m, n) \geq v$ consists of an integer weight $w(t)$ for every staircase t and a denominator D. To find one, we solve the LP for $\mathrm{LTP}^{\mathrm{disj}}$ or LTP with the solver HiGHS by constraint generation: we start from a subset of the pairs, solve, add the pairs whose constraints the solution violates, and repeat. The LP is invariant under the map $t \mapsto (n{+}1{-}t_m, \dots, n{+}1{-}t_0)$, which complements an up-set and reverses the order of P. Hence it can be solved with one variable per orbit. The weights are LP solutions multiplied by a large integer and rounded. Some come from runs stopped before convergence, and for the disjoint certificates of $M(4, 14)$ and $M(8, 9)$ we rounded the averages of the last four and of the last two solutions. The checker does not rely on any of this, since soundness never depends on optimality. It makes sure that the certificate gives a weight to every staircase, computes $\mathrm{def}_w(f, g)$ in integer arithmetic for every incomparable pair, or for every pair with disjoint carried steps in a disjoint certificate, and puts $D' = \max(D, \max \mathrm{def}_w)$, so that w/D' is feasible even if some defects exceed D. It computes $\Phi(w)$ and D' as integers, so $\lceil \Phi(w)/D' \rceil$ follows by exact integer division. Theorem 3.2, together with Lemma 3.3 for disjoint certificates, then implies $M(m, n) \geq \lceil \Phi(w)/D' \rceil$. In each of our certificates the largest defect equals D, so $D' = D$. The denominator is $2^{24} + 1$, except for $M(6, 8)$, $M(6, 9)$, $M(7, 9)$ and $M(8, 9)$, for which we raised it to the largest defect of the rounded weights. Two checkers, written from the definitions and independently of each other, pass every certificate of Table 1. The certificates are large: the one for $M(8, 9)$ has 92,378 weights. On one core, every check that we re-ran for the supplement took at most about six minutes. The supplement also records longer checks that we did not re-run for it. Among them, one of the two checkers ran the four largest certificates of Table 1 in chunks, which for $M(8, 9)$ took 0.963 CPU hours in total, and the other checked the certificate for $M(8, 9)$ in a single run of about 19 minutes.

Of our certificates, the one for $M(8,9)$ took the longest to find. Its LP has one variable for each of the 92,378 staircases. After the symmetry reduction it has 46,252 orbit variables and 204,825,749 distinct constraints between orbits. Constraint generation took eleven rounds and about 13.6 hours on one core. It stopped at the restricted optimum 29 with eleven violated constraints left, and the rounded average of the last two solutions gives $\Phi(w)/D = 28.200932$ with $D = 17{,}252{,}595$, which suffices for $M(8,9) \geq 29$. Since $\mathrm{LTP}^{\mathrm{disj}}(P) \leq s(P) \leq C(8,9) = 29$, the optimum of this LP lies between 28.200932 and 29.

As a cross-check we used Harder's exact search [5]. The original program handles the cube on up to 11 channels, and we patched it to compute $s(P)$ for given sets, such as merging sets, on up to 15 channels. For each pair, a run with limit $C(m,n)$ proves $s(P) \geq C(m,n)$, and a run with limit $C(m,n)+1$ returns $C(m,n)$. Together the two runs show $s(P) = C(m,n)$. This gives $M(m,n) = C(m,n)$ for all 49 pairs $1 \leq m \leq n$ with $m+n \leq 14$, and for $(6,9)$ and $(5,10)$ on 15 channels. The search does not produce a certificate. As a test of the patch for the 14-channel state store, programs built with and without it give the same values for $M(5,7)$ and $M(4,9)$, on 12 and 13 channels.

6. Exact values

value	certified bound	D	pairs checked	plain	exact search
$M(5,7) = 18$	17.999998	16777217	490,233	–	yes
$M(6,8) = 22$	21.799676	16931387	6,757,741	–	yes
$M(6,9) = 25$	24.994949	16780606	18,721,587	–	yes (15 ch.)
$M(7,9) = 27$	26.099660	17355966	93,693,822	–	–
$M(8,9) = 29$	28.200932	17252595	409,646,733	–	–
$M(5,15) = 35$	34.999998	16777217	203,849,786	–	–
$M(5,10) = 25$	24.666665	16777217	7,222,616	yes	yes (15 ch.)
$M(5,11) = 27$	26.799998	16777217	15,442,183	yes	–
$M(5,12) = 29$	28.499998	16777217	31,337,471	yes	–
$M(6,10) = 27$	26.999998	16777217	47,916,181	–	–
$M(4,10) = 22$	21.888887	16777217	885,754	yes	yes
$M(4,14) = 30$	29.666664	16777217	9,017,353	yes	–
$M(4,18) = 38$	37.585514	16777217	55,822,495	–	–

Table 1. Values proved by certificates. The certified bound is $\Phi(w)/D$ for the disjoint certificate, rounded down, and its ceiling is the value. The fourth column gives the number of incomparable pairs with disjoint carried steps that the checkers test, and the fifth marks the values that also have a plain certificate. Except for $M(6,8)$, $M(6,9)$, $M(7,9)$ and $M(8,9)$, the optimum of the disjoint LP, as computed by HiGHS, exceeds the certified bound by less than $3 \cdot 10^{-6}$.

Proof of Theorem 1.1. The lower bounds follow from the certificates of Table 1, by Theorem 3.2 and, for disjoint certificates, Lemma 3.3. Batcher's networks give the upper bounds, since their sizes $C(m,n)$ are the stated values. □

Table 1 also lists the three cases of $M(4,4k+2)$ of Table 2, and it marks the values that the exact search of Section 5 confirms. That search handles at most 15 channels, so the values on more channels rest only on the certificates, except $M(5,11)$, $M(5,12)$ and $M(5,15)$, which also follow from Theorem 7.6. Table 2 sets these values, and the other results of the paper on $M(m,n)$, against what was known before. For $M(4,10)$, $M(4,14)$, $M(5,10)$ and $M(5,12)$ the

case	before this paper	here	by
$M(5,7)$, $M(6,8)$, $M(6,9)$	open: 17/18, 21/22, 24/25	18, 22, 25	Thm. 1.1
$M(7,9)$, $M(8,9)$, $M(5,15)$	open: 26/27, 28/29, 34/35	27, 29, 35	Thm. 1.1
$M(5,23)$, $M(6,24)$, $M(7,24)$	open: 51/52, 57/58, 61/62	52, 58, 62	Thms. 1.2, 1.3
$M(5,10)$, $M(5,11)$, $M(5,12)$, $M(6,10)$	not in the table	25, 27, 29, 27	Thm. 1.1
$M(6,16)$, $M(7,16)$	not in the table	40, 43	Thms. 1.2, 1.3
$M(5,n)$, $n \equiv 2,3,4,7 \pmod 8$	values for $n \le 4$	new formula	Thm. 7.6
$M(6,8k)$, $k \ge 1$	$M(6,8)$, $M(6,24)$ open	new formula	Thm. 7.7
$M(5,n)$, $n \equiv 6 \pmod 8$	sketch [2, Thm. 12]	complete proof	Thm. 7.6
$M(5,n)$, $n \equiv 0,1,5 \pmod 8$	[7]	new proof	Thm. 7.6
$M(6,8k+6)$, $M(6,8k+7)$	[7], [10, Thm. 1]	new proofs	Thm. 7.7
$M(7,8)$	[10]	new proof	Thm. 7.8
$M(4,10)$, $M(4,14)$, $M(4,18)$	[2, Thm. 7]	new proofs	Table 1
$M(2,n)$	[13]	new proof	Thm. 7.1
$M(3,n)$, $n \ge 8$	[1], [2, Thm. 2]	new proof	Thm. 7.2
$M(4,n)$, odd $n \ge 3$	[7]	new proof	Thm. 7.4
$\lim_n M(m,n)/n$	[7]	new proof	Thm. 7.3
$M(6,25)$, $M(7,25)$	open: 60/61, 64/65	open†	
$M(8,15)$, $M(8,23)$, $M(8,25)$	open: 43/44, 63/64, 68/69	open	
$M(9,15)$, $M(9,23)$, $M(9,24)$	open: 44/47, 65/68, 67/70	open	

TABLE 2. The results of this paper on $M(m,n)$ against what was known before. "Open: a/b" means listed as open, with the bounds a and b, in the table of Morohashi and Iwata [10, Table 1], [9, Table 5.1]. "Not in the table" means that this table has no column for that n; we have not found these values determined in the literature. Before this paper, the values $M(5,n)$ with $n \equiv 2,3,4,7 \pmod 8$ and $n \ge 5$ were open in this table or not in it. "Sketch" means that we know of no complete published proof. $M(5,7)$, $M(5,10)$, $M(5,11)$, $M(5,12)$, $M(5,15)$ and $M(6,8)$ also follow from Theorem 1.2. †These entries stay open; by Remark 7.9, no potential of the parity type settles either of them, whatever its slope, and none that records t_0 and t_6 modulo 4 settles $M(6,25)$.

plain LP has numerically the same optimum as the disjoint one. For $M(5,11)$ the computed plain optimum, 26.79889, is smaller than the disjoint one, 26.8, but it still exceeds 26.

7. Closed-form potentials

The potentials of this section are typed in the sense of Lemma 3.6. Besides the activity of the kinds, some of them record *boundary contacts*: an active kind k touches the bottom if $t_{k+1} = 0$ and the top if $t_k = n+1$. The *parity type* consists of the activity of all kinds, the flags $[t_m \ge 1]$ and $[t_0 \le n]$, and the parities of $t_0, \dots, t_m$, and the *residue type modulo* 4 is defined in the same way with residues modulo 4 in place of parities. By Lemma 3.6, finitely many configurations decide feasibility for every n, and finitely many values of Φ determine Φ for all n. All checks and all values of Φ in the proofs of this section were computed in exact rational arithmetic, and the scripts, the weight tables and the recorded outputs are in the supplement. In the proofs of Theorems 7.4, 7.6, 7.7 and 7.8 and of the odd case of Theorem 7.1 we check only the pairs allowed by Lemma 3.3. These results therefore concern $\mathrm{LTP}^{\mathrm{disj}}$ and depend on that lemma, whereas the other checks cover all pairs.

Table 3 lists the potentials of Theorems 7.4 and 7.6 to 7.8. For Theorems 7.6 to 7.8, two programs written independently list all configurations of the class, which have at most $2m+3$

gaps, and check the weights on every configuration that belongs to an incomparable pair with disjoint carried steps. The table gives the number of these configurations and the number of distinct keys, formed by the types of f, g, $f \cup g$ and $f \cap g$, that they give. The weights of Theorems 7.6 and 7.7 come from LPs over all configurations of the class that fix the slope of Φ at that of $C(m,n)$ and maximize the constant term, solved in floating point and then made exact. By Lemma 3.6(ii), Φ_n is affine on each class for $n \geq m$, so its values at the two sizes in the last column of the table determine it.

Thm.	potential	D	checked	keys	Φ_n	from
7.4	$m=4$, parity, odd n	2	176,698,182*	–	$2n+3/2$	5, 19
7.6	$m=5$, parity, odd n	4740	5,482,874	971,050	$17n/8+19/8$	23, 25
	$m=5$, parity, even n	4	5,482,874	971,050	$17n/8+5/2$	22, 24
	$m=5$, mod 4, $n \equiv 0$	14,615,040	1,799,486,556	271,903,708	$17n/8+\beta_0$	8, 12
	$m=5$, mod 4, $n \equiv 2$	101,050,320	1,799,486,556	271,903,708	$17n/8+\beta_2$	6, 10
	$m=5$, mod 4, $n \equiv 3$	2,812,417,776	1,799,486,556	271,903,708	$17n/8+\beta_3$	7, 11
7.7	$m=6$, parity, odd n	12,976,128	133,401,888	11,834,848	$9n/4+121/36$	7, 9
	$m=6$, parity, even n	655,360	133,401,888	11,834,848	$9n/4+33/10$	6, 8
7.8	$m=7$, parity, even n	10^8	3,316,676,424	140,563,032	$\alpha n+\beta$	8, 10

TABLE 3. The potentials of Theorems 7.4 and 7.6 to 7.8: the denominator D of the weights, the number of configurations of incomparable pairs with disjoint carried steps that were checked, each unordered pair once (*for Theorem 7.4, the number of such pairs at $n=21$), the number of distinct keys they give, Φ_n on the class for $n \geq m$ (β_j as in Theorem 7.6, α and β as in Theorem 7.8), and the two sizes whose values of Φ determine it. The theorems state for which n the ceiling of Φ_n is $C(m,n)$; for $m=7$ these are $n=8$, 16 and 24.

Theorem 7.1 (two rows)**.** *For every n, $\mathrm{LTP}^{\mathrm{disj}}(M(2,n)) = \lceil 3n/2 \rceil = M(2,n)$, and $\mathrm{LTP}(M(2,n)) = 3n/2$ if n is even.*

Proof. Let $w(t)$ be 0, 1 or 3/2 according as none, one or both of the kinds $0,1$ are active in t, as in Example 3.5. Since this potential is typed and ignores residues, only finitely many configurations occur. A check of all of them shows that $\mathrm{def}_w \leq 1$ for every n. Each input on A has one active kind and the inputs on B have none, while T_0 and T_{n+1} have one active kind and the other outputs have both. Hence $\Phi(w) = 2 + 3n/2 - 2 = 3n/2$, which yields the lower bound $M(2,n) \geq \lceil 3n/2 \rceil$ of Yao and Yao [13] for every n. Since $\mathrm{LTP} \leq \mathrm{LTP}^{\mathrm{disj}} \leq s(P) \leq C(2,n) = \lceil 3n/2 \rceil$, the theorem follows for even n.

For odd n we need a finer potential, a disjoint one of the parity type with 40 types and integer weights. By Lemma 3.6(i), every configuration for odd n occurs at $n=13$. The weights pass the check of all pairs with disjoint carried steps for every odd $n \leq 31$. By Lemma 3.6(ii), Φ is affine on odd $n \geq 3$, so its values at $n=3$ and $n=31$ determine $\Phi = (3n+1)/2 = \lceil 3n/2 \rceil$ for all odd $n \geq 3$. At $n=1$ the check gives $\Phi = 2$ directly. □

Theorem 7.2 (three rows)**.** $M(3,n) \geq \lceil (7n+3)/4 \rceil$ *for every $n \geq 8$.*

Proof. The type of a staircase records, for each of the kinds 0, 1 and 2, whether it is active and, if so, whether it touches the bottom and whether it touches the top. Exactly 29 types occur. The weights come from the typed LP for $n=14$ and are rounded to multiples of 1/4. Since the potential ignores residues, Lemma 3.6(i) implies that every configuration occurs at $n=8$. Hence the check of all pairs at $n=8$, repeated at $n=11$ and $n=14$, shows that $\mathrm{def}_w \leq 1$ for

every n. For $n \geq 8$, Lemma 3.6(ii) shows that $\Phi(n)$ is affine in n, so the values $\Phi(8) = 59/4$ and $\Phi(14) = 101/4$ determine $\Phi(n) = (7n+3)/4$. □

Since $C(3,n) = \lceil (7n+3)/4 \rceil$, Theorem 7.2 gives the formula $M(3,n) = \lceil (7n+3)/4 \rceil$ for $n \geq 8$, treating all residues of n at once; Table 2 lists the earlier proofs. For $n < 8$ the values are among those confirmed by the exact search.

Theorem 7.3 (linear coefficient)**.** *For all $m, n \geq 1$, $M(m,n) \geq c_m(n-m+2)-m$, where $c_1 = 1$ and $c_m = (c_{\lceil m/2 \rceil} + c_{\lfloor m/2 \rfloor})/2 + 1/2$.*

Proof. Let $a(t) \in \{0,1\}^m$ record which kinds are active in t, and let $w(t) = W(a(t))$, where $W(0) = 0$, $W(1) = 1$ for vectors of length 1, and

$$W(a) = \tfrac{1}{2}(W(a') + W(a'')) + \tfrac{1}{2} \qquad (a \neq 0),$$

with a' the first $\lceil l/2 \rceil$ entries of a vector a of length $l \geq 2$ and a'' the others. By induction, $W(a) = 1$ if a has exactly one nonzero entry, $W(1,\dots,1) = c_m$, and $W \geq 0$. For $m = 2$ this is the potential of Theorem 7.1.

To show feasibility, split a pair (f,g) of staircases on the rows $0,\dots,m$ into the pairs on the rows $0,\dots,h$ and on the rows $h,\dots,m$, where $h = \lceil m/2 \rceil$. The two halves share row h. The activity of kind k in f, g, $f \cup g$ and $f \cap g$ depends only on rows k and $k+1$, so the defect Δ of the pair satisfies $\Delta = (\Delta' + \Delta'')/2 + E/2$. Here Δ' and Δ'' are the defects of the halves, and $E = e(f \cup g) + e(f \cap g) - e(f) - e(g)$, where $e(t) = 1$ if some kind is active in t and $e(t) = 0$ otherwise. We bound Δ by a table with 22 keys. A key records e for the four staircases and the order relation ($<$, $=$ or $>$) between f and g in the first and in the last row. Every entry of the table is at most 1, every entry is at least the defect of each pair with $m \leq 6$ and that key, and the table is closed under gluing: for two keys that agree on the shared row, $(B' + B'')/2 + E/2$ is at most the entry of the glued key. We checked these properties in exact arithmetic. Strong induction on m then shows $\Delta \leq 1$ for every pair, for all m and n.

Each input on A has exactly one active kind, so these inputs contribute m, and the inputs on B contribute 0. All kinds are active in T_r for $m-1 \leq r \leq n$. These $n-m+2$ outputs have weight c_m, and the other outputs have nonnegative weight. Hence $\Phi(w) \geq c_m(n-m+2) - m$. □

Since $C(m,n) = c_m n + O_m(1)$ by induction on m from Batcher's recursion, Theorem 7.3 implies $\lim_n M(m,n)/n = c_m$. Induction on m also shows $c_m = \lceil \log_2 m \rceil/2 + m/2^{\lceil \log_2 m \rceil}$, so this is Iwata's limit [7].

Theorem 7.4 (four rows, odd n)**.** $\mathrm{LTP}^{\mathrm{disj}}(M(4,n)) \geq 2n + 3/2$ *for every odd $n \geq 3$. Hence $M(4,n) = 2n+2 = C(4,n)$ for odd $n \geq 3$.*

Proof. We use the potential of Table 3 for $m = 4$, a disjoint potential of the parity type with 364 types. By Lemma 3.6(i), every configuration for odd n occurs at $n = 21$, where all incomparable pairs with disjoint carried steps pass the check. By Lemma 3.6(ii), $\Phi_n = 2n + 3/2$ for all odd $n \geq 5$, with $\Phi_5 = 23/2$ and $\Phi_{19} = 79/2$, and the value $\Phi_3 = 15/2$ was computed directly. □

Remark 7.5. For $n \equiv 2 \pmod 4$ we found no closed-form potential with a positive margin over $2n+1$ for all n, although the computed values of $\mathrm{LTP}^{\mathrm{disj}}(M(4,n)) - (2n+1)$ are 1, 8/9, 2/3 and 0.586 at $n = 6$, 10, 14 and 18. This is why Table 1 treats these cases by certificates.

Theorem 7.6 (five rows)**.** $\mathrm{LTP}^{\mathrm{disj}}(M(5,n)) \geq (17n+19)/8$ *for every odd $n \geq 5$, and* $\mathrm{LTP}^{\mathrm{disj}}(M(5,n)) \geq (17n+20)/8$ *for every even $n \geq 6$. Moreover* $\mathrm{LTP}^{\mathrm{disj}}(M(5,n)) \geq 17n/8 + \beta_j$ *for every $n \geq 5$ with $n \equiv j \pmod 4$ and $j = 0, 2, 3$, where $\beta_0 = 55207/20760$, $\beta_2 = 667403/240596$ and $\beta_3 = 65/24$. Hence $M(5,n) = C(5,n)$ for every $n \geq 1$.*

Proof. We use the five potentials of Table 3 for $m = 5$: two of the parity type, for odd and for even n, and three of the residue type modulo 4, for the classes $n \equiv 0$, 2 and 3 (mod 4). Each passes the check of all configurations of its class, so $\mathrm{def}_w \le 1$ on every incomparable pair with disjoint carried steps, for every n of the class. For the two parity potentials, Lemmas 3.6(i) and 3.7 give a second check: every such configuration occurs at $n = 23$ for odd n and at $n = 22$ for even n, and at these sizes the written-out potentials pass on all 9,072,292,799 and 6,042,537,893 such pairs, respectively. For $n = 8k + r$, the values of Φ_n in Table 3 have the ceilings $17k + 3$, $17k + 5$, $17k + 13$, $17k + 16$ and $17k + 18$ for $r = 0$, 1, 5, 6 and 7, from the parity potentials, and $17k + 8$, $17k + 10$ and $17k + 12$ for $r = 2$, 3 and 4, from the potentials modulo 4. These are the values of $C(5, n)$.

For $n \le 4$ the same potentials apply, since the checks cover every configuration at every size, but Lemma 3.6(ii) gives the affine form only from $n = 5$ on. The values $\Phi_1 = 2045/474$, from the potential for odd n, and $\Phi_2 = 421200/60149$, $\Phi_3 = 109/12$ and $\Phi_4 = 231667/20760$, from the potentials of the three classes, all have the ceiling $C(5, n)$; for $n = 2$ the margin over $C(5, 2) - 1 = 7$ is only 157/60149. The exact search of Section 5 confirms these four values, as $M(1, 5)$, $M(2, 5)$, $M(3, 5)$ and $M(4, 5)$. □

The cases $n \le 4$ are classical, since $M(5, n) = M(n, 5)$, and $M(5, 7)$, $M(5, 10)$, $M(5, 11)$, $M(5, 12)$ and $M(5, 15)$ also follow from the certificates of Theorem 1.1.

Theorem 7.7 (six rows)**.** $\mathrm{LTP}^{\mathrm{disj}}(M(6, n)) \ge 9n/4 + 121/36$ *for every odd* $n \ge 7$*, and* $\mathrm{LTP}^{\mathrm{disj}}(M(6, n)) \ge 9n/4 + 33/10$ *for every even* $n \ge 6$*. Hence* $M(6, n) = C(6, n)$ *for every* $n \ge 6$ *with* $n \equiv 0, 6, 7$ (mod 8)*:* $M(6, 8k) = 18k + 4$ *for* $k \ge 1$*, and* $M(6, 8k + 6) = 18k + 17$ *and* $M(6, 8k + 7) = 18k + 20$ *for* $k \ge 0$*.*

Proof. We use the two potentials of Table 3 for $m = 6$, of the parity type, for odd and for even n. Each passes the check of all configurations of its class, and for $n = 8k$, $8k + 6$ and $8k + 7$ the values of Φ_n in the table have the ceilings $18k + 4$, $18k + 17$ and $18k + 20$, the values of $C(6, n)$. □

Theorems 7.6 and 7.7 together prove Theorem 1.2. Theorem 7.7 gives, for example, $M(6, 16) = 40$ and $M(6, 24) = 58$; $M(6, 8)$ also follows from the certificate of Theorem 1.1. We did not use the route through Lemma 3.7 here: it would need $n = 26$ and $n = 27$, where the written-out potentials have 5,379,616 and 6,724,520 staircases, respectively.

Theorem 7.8 (a potential for $m = 7$)**.** $\mathrm{LTP}^{\mathrm{disj}}(M(7, n)) \ge \alpha n + \beta$ *for every even* $n \ge 8$*, where* $\alpha = 236712013/10^8$ *and* $\beta = 424814309/10^8$*. Hence* $M(7, n) = C(7, n)$ *for* $n = 8$*,* 16 *and* 24*, that is,* $M(7, 8) = 24$*,* $M(7, 16) = 43$ *and* $M(7, 24) = 62$*.*

Proof. We use the potential of Table 3 for $m = 7$, of the parity type for even n. Its weights come from the LP that maximizes Φ_{24} over the potentials of this type, with no condition on the slope of Φ and with only the constraints of the configurations that occur at $n = 24$, solved in floating point and then made exact. The check of all configurations of the class gives the largest defect 0.99999901, so the potential is feasible for every even n. At $n = 8$, 16 and 24, $\Phi_n = \alpha n + \beta$ exceeds $C(7, n) - 1 = 23$, 42 and 61 by about 0.185, 0.122 and 0.059; for instance $\Phi_{24} = 6105902621/10^8$. So the ceilings are the values of $C(7, n)$. □

Theorem 7.8 proves Theorem 1.3. Since $\alpha < 19/8$, the slope of $C(7, n)$, its potential falls behind Batcher's networks as n grows, and among even n its ceiling is $C(7, n)$ only at $n = 8$, 16 and 24. By Remark 7.9, every feasible potential of the parity type whose Φ_n has slope 19/8 on even n has a ceiling of at most $C(7, n) - 1$ at every $n \equiv 0$ (mod 8), so a smaller slope is needed for these three values.

Remark 7.9 (limits of the parity type). Fix m and the parity of n. By Lemma 3.6(ii), a potential of the parity type has $\Phi_n = an + b$ for all $n \geq m$ of that parity, where a and b are linear in the weights. If the potential is feasible, then a is at most the slope c_m of $C(m, n)$, defined in Theorem 7.3, since $\Phi_n \leq M(m, n) \leq C(m, n)$; here $c_5 = 17/8$, $c_6 = 9/4$ and $c_7 = 19/8$. For $a = c_m$ an exact dual certificate bounds b. It consists of nonnegative rationals y_k on finitely many keys k and a rational λ such that $b = \sum_k y_k \operatorname{def}_w(k) + \lambda a$ for every choice of the weights, where $\operatorname{def}_w(k)$ is the defect of the pairs with key k. Every feasible potential with $a = c_m$ then has $b \leq \sum_k y_k + \lambda c_m$. Each key of a certificate comes with an explicit pair of staircases that realizes it, and two programs check the certificates in exact arithmetic; Lean checks them too, with the kernel alone (Section 9). We compare the bounds with the values that b must exceed for the ceiling of Φ_n to be $C(m, n)$; these depend only on the residue of n modulo 8.

- For $m = 5$: $b \leq 19/8$ for odd n, while $n \equiv 3$ needs $b > 21/8$; and $b \leq 5/2$ for even n, while $n \equiv 2$ and $n \equiv 4$ need $b > 11/4$ and $b > 5/2$. For odd n the bound also follows from $\Phi_n \leq C(5, n)$ at $n \equiv 5$.
- For $m = 6$: $b \leq 121/36$ for odd n and $b \leq 33/10$ for even n, the values of Theorem 7.7, while $n \equiv 1, 3, 5$ need $b > 15/4$, $17/4$, $15/4$ and $n \equiv 2, 4$ need $b > 7/2$ and $b > 4$. The bound $121/36$ still holds for $n \equiv 1 \pmod 4$ if the type records t_0 and t_6 modulo 4 instead of their parities.
- For $m = 7$: $b \leq 4$ for even n, while $n \equiv 0, 2, 4, 6$ need $b > 4$, $21/4$, $11/2$, $19/4$. For odd n, $\Phi_n \leq C(7, n)$ at $n \equiv 7$ gives $b \leq 35/8$, while $n \equiv 1, 3, 5$ need $b > 37/8$, $39/8$, $41/8$.

So at each of these residues, every feasible potential of the parity type with slope c_m has a ceiling of at most $C(m, n) - 1$, for every $n \geq m$ of the residue. This is why Theorem 7.6 also uses residues modulo 4. A potential with a smaller slope is not bound by these limits and can win at single values of n, as in Theorem 7.8. At a single n no condition on the slope is needed: a certificate of the same kind with $\lambda = 0$, whose keys occur at that n, bounds $\Phi_n = \sum_k y_k \operatorname{def}_w(k) \leq \sum_k y_k$ directly. For $n = 25$ such certificates give $\Phi_{25} \leq 1073/18 < 60$ for $m = 6$ and $\Phi_{25} \leq 2409/38 < 64$ for $m = 7$, so no potential of the parity type proves $M(6, 25) = 61$ or $M(7, 25) = 65$, whatever its slope. For $M(6, 25)$ this stays true if the type records t_0 and t_6 modulo 4.

8. Remarks on general comparator networks

LTP applies to any set P, not only to merging sets. We compared $\lceil \mathrm{LTP}^{\mathrm{disj}}(P) \rceil$ with $s(P)$ on the following sets, and the two agree on every one of them: for $c = 4$ and $c = 5$, all sets reachable from $\{0, 1\}^c$ by comparators, up to symmetry; for $c = 6$, all 1,145 such classes, among them $\{0, 1\}^6$ and its image under one comparator, which we treat below; about 400 further sets, namely random unions of maximal chains on 5 and 6 channels, images of $\{0, 1\}^7$ under random comparator prefixes and unions of two maximal chains on 3 to 9 channels; and sets that arise in exhaustive searches for sorting networks on 8 to 10 channels. On this evidence we state the following conjecture.

Conjecture 8.1. $\lceil \mathrm{LTP}^{\mathrm{disj}}(P) \rceil = s(P)$ *for every set* P *that is a union of maximal chains.*

Write $S(c) = s(\{0, 1\}^c)$ for the least size of a sorting network on c channels. On $\{0, 1\}^6$ the bound is exact: $\mathrm{LTP}^{\mathrm{disj}}(\{0, 1\}^6) = 12 = S(6)$ [8], so a single certificate proves $S(6) \geq 12$. The 7,828,354 up-sets of $\{0, 1\}^6$ fall into 8,282 classes under the permutations of the channels and the duality $f \mapsto \{x : \bar{x} \notin f\}$, where $\bar{x}$ is the complement of x. Both maps preserve the constraints and Φ, so the LP may take one weight per class. The certificate gives nonzero weights to 293 classes, all in $\frac{1}{12}\mathbb{Z}$ with numerators of absolute value at most 22, and $\Phi = 144/12$. Since the weights are invariant, it is enough to check one representative of each class against every up-set: 4,111,909 of these pairs are incomparable with disjoint carried steps, and all of them

satisfy the constraint. The bound is also exact on the image P_1 of $\{0,1\}^6$ under one comparator: $\mathrm{LTP}^{\mathrm{disj}}(P_1) = 11 = s(P_1)$. Here $s(P_1) = S(6) - 1$, since by the symmetry of the channels an optimal sorting network on 6 channels can begin with any comparator. The certificate for P_1 has denominator 334 and nonzero weights on 501 of the 4,729 classes into which a symmetry group of order 48 divides the 160,948 up-sets of P_1, and a second program checks all 7,371,294 incomparable pairs with disjoint carried steps without using the symmetry. The same method gives $\mathrm{LTP}^{\mathrm{disj}}(\{0,1\}^c) = S(c)$ for $c = 3$ and $c = 4$, and $\mathrm{LTP}^{\mathrm{disj}}(\{0,1\}^5) = 8.75$ against $S(5) = 9$.

The obstacle to using LTP for larger sorting problems is size. The number of up-sets explodes. Even the degree-2 truncation has a quadratic number of variables and an NP-hard separation problem (Remark 4.3).

9. Formal verification

The ten values of Theorem 1.1 and the three values of $M(4, 4k+2)$ in Table 1 are also proved in Lean 4 [4], using only its core library, and the development is archived at [11]. In it, a network is a list of comparators acting on vectors of natural numbers, and it merges (a, b) if it sorts every input whose first a entries and whose last b entries are nondecreasing. For each of the thirteen pairs, the main theorem states that the value is the least size of a general merging network, in which a comparator may put the minimum on either of its two channels and the inputs and outputs may be placed on the channels in any order. The proof has three parts. The lower bounds for standard networks come from Theorem 3.2 and Lemma 3.3, formalized for merging sets and their staircases, and from a checker, proved sound, that verifies one certificate for each value: the plain certificate of Table 1 where a value has one, and the disjoint one otherwise. For the upper bounds, Batcher's networks are defined in Lean and shown to merge by a 0-1 principle for merging, which leaves only the $(a+1)(b+1)$ two-chain inputs of zeros and ones to test. Finally, a reduction shows that general and standard merging networks have the same least size.

The development also covers Section 7, as far as its theorems concern $M(m, n)$. It proves versions of Lemmas 3.6 and 3.7 for typed potentials, and Theorems 7.1, 7.2, 7.3, 7.4, 7.6 and 7.7 as lower bounds on the size of merging networks, for all n in their ranges. Batcher's network is defined for all (a, b) and shown to merge with $C(a, b)$ comparators, and $C(m, n)$ is computed in closed form for $m \le 6$ on the residue classes of Section 7. With the reduction above this gives, for general networks, $M(2, n)$ for all n, $M(3, n)$ for $n \ge 8$, $M(4, n)$ for odd $n \ge 3$, $M(5, n)$ for all n and $M(6, n)$ for all n covered by Theorem 7.7. It proves $M(7, 8) = 24$, $M(7, 16) = 43$ and $M(7, 24) = 62$ in the same way, from the potential of Theorem 7.8. For Theorems 7.6 and 7.7 Lean follows the configuration route of their proofs. It shows that every incomparable pair with disjoint carried steps, for any n of the given residue class, is carried onto the canonical pair of its configuration by a relabelling of the entries that keeps their order and their residues, and it then checks the canonical pairs of all configurations. For the parity part of Theorem 7.6 and for Theorem 7.7 there are also kernel-only proofs, in which the kernel evaluates all of these checks itself; the one for Theorem 7.6 took about 32 CPU hours, and the one for Theorem 7.7 about 77. Lean also proves $S(6) = 12$ for standard networks from the certificate of Section 8: every such network that sorts 6 channels has at least 12 comparators, and a network given in Lean has 12.

Table 4 lists what the Lean kernel checks with only the axioms `propext`, `Classical.choice` and `Quot.sound`, and which checks run as compiled code (`native_decide`), each call of which adds one auxiliary axiom. The results that use compiled checks therefore also rely on the Lean compiler.

Nothing else in the paper is formalized. In particular, Lean has Theorem 3.2 only for merging sets and for the cubes $\{0,1\}^c$, not for general P, and it does not formalize Proposition 3.4, the identities of Section 4 or the statements about LTP and $\mathrm{LTP}^{\mathrm{disj}}$ themselves. For Section 7,

checked by the kernel alone	compiled checks (`native_decide`)
the soundness theorems, the 0-1 principle, the upper bounds and the reduction	the certificate checks for the thirteen values
the versions of Lemmas 3.6 and 3.7	the checks for Theorem 7.4
Theorems 7.1, 7.2 and 7.3	the checks of the other proofs of Theorems 7.6 and 7.7, including the part of Theorem 7.6 for residues modulo 4
the merging property of Batcher's networks	the check of the configurations and the three values of Φ for Theorem 7.8
the kernel-only proofs (parity part of Theorem 7.6, Theorem 7.7)	the five checks of the certificate for $\{0,1\}^6$
for $\{0,1\}^6$: the soundness theorem for sorting networks with Lemma 3.3, its reduction to one up-set per class, the 0-1 principle for sorting and the upper bound	
the bounds of Remark 7.9 from its nine certificates and the limits they give for a potential of the parity type with rational weights: if it is feasible at every n of its class and has slope c_m, then $\Phi_n \le C(m,n) - 1$ for all $n \ge m$ with $n \equiv 2, 3, 4 \pmod 8$ if $m = 5$, with $n \equiv 1, 2, 3, 4, 5$ if $m = 6$ (for $n \equiv 1, 5$ also when the type records t_0 and t_6 modulo 4) and with $n \equiv 0, 2, 4, 6$ if $m = 7$; if it is feasible at $n = 25$, then $\Phi_{25} \le 60$ for $m = 6$ (both types) and $\Phi_{25} \le 64$ for $m = 7$, with $C(6, 25) = 61$ and $C(7, 25) = 65$	

TABLE 4. The Lean development of Section 9: what the kernel checks with only the standard axioms, and the checks that run as compiled code.

Lean proves the bounds on the size of networks that the potentials give, for the potential of Theorem 7.8 at $n = 8$, 16 and 24.

10. Open problems

Several questions remain. Besides Conjecture 8.1, it is open whether even $\lceil \mathrm{LTP}(P) \rceil = s(P)$ holds for unions of maximal chains, and whether some fixed degree k has $\lceil \mathrm{LTP}_k \rceil = \lceil \mathrm{LTP} \rceil$. For $M(4, n)$ with $n \equiv 2 \pmod 4$, we do not know whether the margin of $\mathrm{LTP}^{\mathrm{disj}}$ over $2n + 1$ stays positive for all n. A positive answer would give a new proof of the theorem of Amano and Maruoka for all such n. For $m = 6$ the residues $n \equiv 1, \ldots, 5 \pmod 8$ remain open beyond $M(6, 9)$ and $M(6, 10)$, and for $m = 7$ only the residue $n \equiv 7 \pmod 8$ is settled for all n. Remark 7.9 shows that potentials of the parity type with the slope of $C(m, n)$ cannot settle these residues. Of the entries of Table 2 that remain open, $M(6, 25)$ and $M(7, 25)$ have $n \equiv 1 \pmod 8$, and no potential of the parity type proves them (Remark 7.9); the others have $m \ge 8$ and more staircases than any certificate here. The fewest, 2,042,975, are those of $M(8, 15)$, more than twenty times as many as for $M(8, 9)$.

Data availability

The supplement [12], doi:10.5281/zenodo.23756851, contains the certificates, both checkers, the scripts and weight tables for Section 7, and the patches, scripts and logs of the exact search.

It also contains the logs of the LP computations behind Remark 4.3, Table 1 and the margins in Remark 7.5, and of the comparison in Section 8 for $c \leq 6$, and the dual certificates of Remark 7.9 with their witnesses and two checkers. Its README explains how to re-run each check and where the records of the longer computations are. The Lean development of Section 9 is archived at [11], doi:10.5281/zenodo.23756852.

References

1. Martin Aigner and Otfried Schwarzkopf, *Bounds on the size of merging networks*, Discrete Appl. Math. **61** (1995), no. 3, 187–194.
2. Kazuyuki Amano and Akira Maruoka, *On optimal merging networks*, Mathematical Foundations of Computer Science (MFCS 2003), Lecture Notes in Comput. Sci., vol. 2747, Springer, 2003, pp. 152–161.
3. Kenneth E. Batcher, *Sorting networks and their applications*, Proc. AFIPS Spring Joint Computer Conference, vol. 32, 1968, pp. 307–314.
4. Leonardo de Moura and Sebastian Ullrich, *The Lean 4 theorem prover and programming language*, Automated Deduction – CADE 28, Lecture Notes in Comput. Sci., vol. 12699, Springer, 2021, pp. 625–635.
5. Jannis Harder, *Lower size bounds for sorting networks*, source code, `https://github.com/jix/sortnetopt`, commit `0b5d09c`, 2020.
6. ———, *An answer to the Bose–Nelson sorting problem for 11 and 12 channels*, arXiv:2012.04400v3 [cs.DS], 2022.
7. Shigeki Iwata, *Lower bounds for merging networks*, Inform. and Comput. **168** (2001), no. 2, 187–195.
8. Donald E. Knuth, *The art of computer programming, vol. 3: Sorting and searching*, 2nd ed., Addison-Wesley, Reading, MA, 1998.
9. Gembu Morohashi, *Secure multiparty protocol using comparator networks*, Dr. eng. thesis, The University of Electro-Communications, 2009.
10. Gembu Morohashi and Shigeki Iwata, *Some minimum merging networks*, Theoret. Comput. Sci. **329** (2004), 237–250.
11. Tejasvi Singh Tomar, *Lean development for "lead-pattern potentials and exact values of merging networks"*, Zenodo, doi:10.5281/zenodo.23756852, 2026.
12. ———, *Supplement to "lead-pattern potentials and exact values of merging networks"*, Zenodo, doi:10.5281/zenodo.23756851, 2026, Checksum file `SHA256SUMS` with SHA-256 hash `d51d815105c8f82c`....
13. Andrew C. Yao and F. Frances Yao, *Lower bounds on merging networks*, J. Assoc. Comput. Mach. **23** (1976), no. 3, 566–571.

ORCID: `https://orcid.org/0000-0003-4668-3639`