A SUPERLOGARITHMIC LOWER BOUND FOR DETERMINISTIC WORD SEPARATION

WILL HOWE, GRANT HUFFMAN, JENSEN KOHLMEYER, AND LIAM KRUER

Abstract. Let $S(n)$ be the maximum, over distinct binary words of length n, of the least number of states in a complete deterministic finite automaton that accepts exactly one of them. We prove $S(n) \geq (1 - o(1)) \log n \log\log n$. The main step is a common word of length $\exp(O(\sqrt{k}\log k))$ that, after suitable powering of the generators, reaches the sink components of every transformation pair on k states and attains minimum rank on each sink. This transfers the balanced positive permutation identities of Xu and Regan to the full transformation monoid without changing their leading logarithmic length. The conclusion concerns deterministic automata; it makes no assertion about nondeterministic separators.

hexagon:2611.00314v1

1. Statement and conventions

All logarithms are natural. A word acts on states in written order: $q \cdot uv = (q \cdot u) \cdot v$. The same convention is used for products of transition matrices. Thus a transformation matrix T has one entry 1 in each row, and Tv is the indicator of the inverse image of the subset whose indicator is v.

Write T_k for the monoid of all transformations of a k-element set. A binary identity for T_k is a pair of distinct words whose evaluations agree for every choice of the two generators in T_k. An identity is *balanced* if the two words have the same number of occurrences of each letter. In particular, they have the same length.

Theorem 1.1. *For every sufficiently large integer k there are distinct balanced binary words u_k, v_k which form an identity for T_k and satisfy*

$$\log|u_k| = \log|v_k| \leq (1 + o(1))\frac{k}{\log k} \qquad (k \longrightarrow \infty). \tag{1.1}$$

Consequently, for complete deterministic binary automata,

$$S(n) \geq (1 - o(1)) \log n \log\log n. \tag{1.2}$$

In particular $S(n)$ is not $O(\log n)$.

The correspondence between transformation identities and deterministic word separation is standard; see Bulatov, Karpova, Shur, and Startsev [1]. We use the following established input, keeping its permutation hypothesis explicit.

Theorem 1.2 (Xu–Regan, Theorem A.1 of [2])**.** *There are distinct balanced positive binary identities $p_k = q_k$ for the symmetric group on k points such that $\log|p_k| \leq (1 + o(1))k/\log k$.*

The proof below establishes the transformation-monoid extension. It does not infer a lower bound for deterministic automata merely from a lower bound for permutation automata. Nor does it infer any lower bound for nondeterministic automata, whose transitions need not be functions.

Date: November 7, 2026.

Prepared with AI assistance from OpenAI Codex in mathematical exploration, checking, and manuscript preparation.

2. Powering and averaging

Fix $k \geq 4$, a permutation X, and an arbitrary transformation Y on $Q = \{1, \ldots, k\}$. Put

$$L = k \prod_{p \leq \sqrt{k}} p^{\lfloor \log k / \log p \rfloor}, \qquad A = X^L, \quad B = Y^L, \tag{2.1}$$

where the product is over primes. There are at most $\sqrt{k}$ factors, each at most k, so $\log L = O(\sqrt{k} \log k)$.

Lemma 2.1. *Every cycle of A or B has length 1 or a prime exceeding $\sqrt{k}$. There are at most $\sqrt{k}$ nontrivial cycles of either transformation. Moreover $B(Q)$ is precisely the cyclic set of B, and B is a permutation on $B(Q)$.*

Proof. A cycle of a transformation on k points has length $d \leq k$. Every prime-power divisor of d with prime at most $\sqrt{k}$ divides L. There can be at most one prime divisor greater than $\sqrt{k}$, and its exponent is one. The cycles of the Lth power therefore have lengths 1 or that remaining prime. Each nontrivial cycle uses more than $\sqrt{k}$ points. Finally every transient path of Y has length less than $k \leq L$. Thus Y^L maps every point onto a cycle of Y, and its restriction to that cyclic set is a permutation. This is also its own cyclic set. □

The *type* of (A, B) consists of the two multisets of cycle lengths, including fixed points. Only $k^{O(\sqrt{k})}$ types occur: each list of nontrivial cycles has at most $\sqrt{k}$ entries in $\{1, \ldots, k\}$, and each number of fixed points has at most $k + 1$ choices. All random choices below depend only on this type.

For every distinct nontrivial cycle length d of A, choose independently a uniform integer in $\{0, \ldots, d-1\}$, add these integers, and add an independent uniform integer in $\{0, \ldots, k-1\}$. Call the result a. Define b in the same way using the cycle lengths of B, then add 1. All choices for a and b are independent. Since the sum of the distinct cycle lengths is at most k, we have $0 \leq a < 2k$ and $1 \leq b \leq 2k$. The residue of a modulo every A-cycle length is uniform; the same holds for b modulo every B-cycle length.

Lemma 2.2. *There are intervals I, J of k consecutive integers, with $I \subseteq \mathbb{N}$ and $J \subseteq \{1, 2, \ldots\}$, such that*

$$\Pr(a = i) \geq k^{-2} \quad (i \in I), \qquad \Pr(b = j) \geq k^{-2} \quad (j \in J). \tag{2.2}$$

Proof. Before the last uniform summand, either sum is supported on at most k integers. A most probable value has probability at least $1/k$. Adding the last uniform summand supplies the required interval, each point having probability at least $1/k^2$. The additional 1 in b makes its interval positive. □

Let $\overline{A} = \mathbb{E}A^a$ and $\overline{B} = \mathbb{E}B^b$. The first matrix averages uniformly on each A-orbit. The second sends each point uniformly onto the cyclic B-orbit containing its B-image. An independent random block has word and matrix

$$B^b A^a, \qquad P = \mathbb{E}(B^b A^a) = \overline{B}\,\overline{A}. \tag{2.3}$$

A block has at most $4k$ letters.

3. Sink components and stationary denominators

A *sink* is a sink strongly connected component of the directed graph with edges $x \to Ax$ and $x \to Bx$. Sinks are closed under both letters and are unions of A-orbits.

Lemma 3.1. *For every type there is a word of length $k^{O(\sqrt{k})}$ sending every state into a sink, simultaneously for all labeled pairs of that type.*

Proof. After one random block, conditional on the current A-orbit, the point is uniform on that orbit. On these orbits consider the quotient chain that starts with this uniform distribution and applies a block. Each positive transition has probability at least $1/k^2$: choose a point in the initial A-orbit and a point in the relevant cyclic B-orbit. The quotient graph includes every edge induced by B between A-orbits, because the average on a cyclic B-orbit includes the first B-image. Consequently every quotient vertex has a path to a sink.

Every singleton A-orbit reached after a block is a cyclic point of B. Indeed, the last A-rotation cannot enter an A-fixed point from a different point. If that point is B-fixed it is already a singleton sink. Otherwise it lies on a nontrivial B-cycle. Suppose a quotient path enters this singleton and then leaves it. The entering transition and the leaving transition use the same cyclic B-orbit, so the predecessor can reach the successor in one block. The intermediate singleton can be deleted. A shortest path therefore has no intermediate singleton. With at most $\sqrt{k}$ nontrivial A-orbits, it has at most $\lceil\sqrt{k}\rceil + 1$ edges.

It follows that, from any state, at most $H = \lceil\sqrt{k}\rceil + 2$ blocks reach a sink with probability at least $p = k^{-2(\lceil\sqrt{k}\rceil+1)}$. Sinks are absorbing. After t such windows the failure probability is at most $(1-p)^t \le e^{-pt}$. There are at most k^{2k} labeled pairs and k starting states per pair. Choose $t > p^{-1}\log(k^{2k+1})$. A union bound gives a positive probability of success in every case, hence a common word. Its length $4kHt$ is $k^{O(\sqrt{k})}$. □

Fix a sink K. The quotient chain just used is irreducible on its A-orbits, since their graph is the quotient of the strongly connected union graph. Each positive transition into an orbit produces a uniform point of that orbit. Starting from any state, one block first produces such a uniform distribution. These facts show that P is irreducible on the states of K as well.

We recall directly why this gives a unique positive stationary row probability μ. Cesaro averages of any row probability have a convergent subsequence, and a limit is stationary. If any of its coordinates is positive, stationarity and irreducibility propagate positivity to every coordinate. A column satisfying $Pf = f$ attains its maximum on a nonempty set closed under every positive transition; irreducibility forces that set to be all of K. Thus the right kernel of $P - I$ is one-dimensional. Equality of row and column rank gives the same statement for the left kernel, proving uniqueness. Since the last averaging operation is $\overline{A}$, the measure μ is uniform on each A-orbit and $\mu A = \mu$.

Lemma 3.2. *On every sink the coordinates of μ are rational with a common positive denominator $D \le k^{C\sqrt{k}}$, for an absolute constant C.*

Proof. The assertion is immediate for a singleton sink. In a nonsingleton sink write A_i for the A-orbits and B_l for the cyclic B-orbits. Let w_i be the weight of each point of A_i under μ, and let z_l be the weight of each point of B_l after applying $\overline{B}$. Set

$$n_{li} = |B_l \cap A_i|, \qquad m_{il} = |\{x \in A_i : Bx \in B_l\}|.$$

Stationarity and normalization are exactly

$$|A_i| w_i = \sum_l n_{li} z_l, \tag{3.1}$$

$$|B_l| z_l = \sum_i m_{il} w_i, \tag{3.2}$$

$$\sum_i |A_i| w_i = 1. \tag{3.3}$$

An A-fixed point in this sink cannot be transient for B: it would have no incoming B-edge, by Lemma 2.1, and no incoming A-edge other than its loop. It also cannot be B-fixed, since then it would itself be a sink. Hence it lies on a nontrivial B-cycle, and (3.1) identifies its w_i with the

corresponding z_l. If B_l is a singleton, its point is in a nontrivial A-orbit. Furthermore no singleton A-orbit has this B-basin, since all those points lie on nontrivial B-cycles. Equation (3.2) therefore expresses this z_l as an integer combination of the w_i belonging to nontrivial A-orbits.

Eliminate both kinds of singleton variable using these formulas. At most $2\sqrt{k}$ variables remain. All equations have integer coefficients bounded by $O(k^2)$ and right sides 0 or 1. Conversely a solution of the reduced system reconstructs a solution of (3.1)–(3.3). That system has a unique solution, by the uniqueness of μ and the definition of the intermediate measure. Thus a square nonsingular subsystem can be selected. Hadamard's determinant inequality bounds its determinant in absolute value by $k^{C\sqrt{k}}$. Cramer's rule gives this determinant as a common denominator of the remaining variables. The eliminated variables are integer combinations of them, so the same denominator works for every coordinate of μ. □

4. A short common minimum-rank word

Continue on a fixed sink and regard A, B as rational linear operators on columns. Define

$$U_0 = \{v \in \mathbb{Q}^K : \ \mu B^b A^a v = \mu v \text{ for all } a \geq 0,\ b \geq 1\}. \tag{4.1}$$

It is a linear subspace invariant under A and A^{-1}, because $\mu A = \mu$ and A has finite order. Let U_∞ be the largest subspace of U_0 invariant under both A and B. Equivalently, $v \in U_\infty$ if and only if $Tv \in U_0$ for every word T. For $v \in U_\infty$, both letters preserve μv and keep v in U_∞. The assertion for B follows by setting $a = 0, b = 1$ in (4.1).

Lemma 4.1. *It suffices in* (4.1) *to test $a \in I$ and $b \in J$ from Lemma 2.2. The operators A^a, $a \in I$, span all nonnegative powers of A. The operators B^b, $b \in J$, span all positive powers of B.*

Proof. The minimal polynomial of the invertible operator A has nonzero constant term and degree at most $|K| \leq k$. The resulting recurrence expresses every power of A in the span of any k consecutive powers. For B, its action on the linear image $E = B\mathbb{Q}^K$ is invertible: Lemma 2.1 gives $\operatorname{rank} B^2 = \operatorname{rank} B$, and hence $B|_E : E \to E$ is bijective. Its minimal polynomial again has degree at most k and nonzero constant term. Multiplying its recurrence by an initial positive power of B proves the claim about positive powers.

For completeness the subtraction of the constant μv in (4.1) respects these recurrences. The constant column $\mathbf{1}$ is fixed by A and by B and belongs to E. Both relevant minimal polynomials therefore vanish at 1. For fixed a, the sequence $\mu B^b A^a v - \mu v$ satisfies the recurrence for $B|_E$ for $b \geq 1$. Its vanishing on J forces vanishing for all positive b, by extending the recurrence in both directions. For each such b, the recurrence for A extends vanishing from I to all $a \geq 0$. □

Lemma 4.2. *If $v \notin U_\infty$, there is a product of at most $\lceil\sqrt{k}\rceil + 1$ blocks $B^b A^a$, with $a \in I, b \in J$, which sends v outside U_0. The empty product is allowed.*

Proof. Put $W_0 = \operatorname{span}_{\mathbb{Q}}\{A^a v : a \geq 0\}$. Given the A-invariant space W_i, let V_{i+1} be its closure under all nonnegative powers of B, and let W_{i+1} be the closure of V_{i+1} under A. Every V_{i+1} is B-invariant. If $W_{i+1} = W_i$ the construction has stabilized at a space invariant under both letters.

The rational representation of A is semisimple: its minimal polynomial divides $t^d - 1$ for some d, which has no repeated roots in characteristic zero. A cycle of prime length p contributes one trivial factor and one irreducible factor with minimal polynomial $1 + t + \cdots + t^{p-1}$; its irreducibility follows from Eisenstein's criterion after replacing t by $t + 1$. Thus the entire representation has at most $\sqrt{k}$ nontrivial simple factors, counted with multiplicity. If W_{i+1}/W_i contains only trivial factors, A acts as the identity on that quotient. Hence $(A - I)V_{i+1} \subseteq W_i \subseteq V_{i+1}$. This makes V_{i+1} already A-invariant, so $W_{i+1} = V_{i+1}$ and the construction has stabilized. Every other growth step uses a nontrivial factor. There are therefore at most $\lceil\sqrt{k}\rceil + 1$ rounds before stabilization.

The stabilized space is the smallest A, B-invariant space containing v. If it were contained in U_0, then $v \in U_\infty$. Thus some spanning word produced within these rounds sends v outside U_0. Its

outermost A power can be deleted, using the A-invariance of U_0 and its inverse. Delete identity B powers and combine neighboring A powers. The result has at most the stated number of positive B runs. By Lemma 4.1, expand each A power in the powers from I and each positive B power in the powers from J. If every resulting word sent v into U_0, linearity would put the original word there too. At least one resulting product has the required property. □

Lemma 4.3. *For every type there is a word V of length $k^{O(\sqrt{k})}$ such that, on each sink of every pair of that type, every column of V belongs to U_∞.*

Proof. Starting at the indicator v_0 of any subset of the sink, take independent blocks $M_t = B^{b_t}A^{a_t}$ and put $v_{t+1} = M_{t+1}v_t$. All v_t remain indicators. Set $Z_t = \mu v_t$ and $F_t = Z_t^2$. Stationarity gives $\mathbb{E}(Z_{t+1} \mid v_t) = Z_t$ and therefore

$$\mathbb{E}(F_{t+1} - F_t \mid v_t) = \operatorname{Var}(Z_{t+1} \mid v_t) \geq 0. \tag{4.2}$$

If $v_t \notin U_0$, Lemma 4.1 supplies a pair from $I \times J$ for which $Z_{t+1} \neq Z_t$. Its probability is at least k^{-4}, and its difference has absolute value at least $1/D$ by Lemma 3.2. Thus the right side of (4.2) is at least $k^{-4}D^{-2}$.

If $v_t \notin U_\infty$, Lemma 4.2 reaches such a drift point along at most $\lceil\sqrt{k}\rceil + 1$ blocks, each with probability at least k^{-4}. In a horizon $H = \lceil\sqrt{k}\rceil + 2$, the expected gain in F is consequently at least $\eta = k^{-C_1\sqrt{k}}$ for an absolute C_1. Unused steps have nonnegative drift. The subspace U_∞ is absorbing for these operations.

Let q_j be the probability of being outside U_∞ after j horizons. Since $0 \leq F \leq 1$, telescoping the horizon gains gives $\eta \sum_{j=0}^{h-1} q_j \leq 1$. The sequence q_j is nonincreasing, so $q_h \leq 1/(h\eta)$. With $h \geq 2/\eta$ the probability of remaining outside is at most $1/2$, uniformly over the starting indicator. Repeating this experiment s times makes it at most 2^{-s}, by conditioning at the start of each experiment.

There are at most k^{2k} labeled pairs, at most k sinks per pair, and at most 2^k subsets per sink. Choosing $s > \log_2(k^{2k+1}2^k)$ and applying a union bound gives a single sequence that sends every such indicator into its respective U_∞. Its number of letters is $4kHhs = k^{O(\sqrt{k})}$. If the sampled blocks are $M_1, \ldots, M_t$, take the forward word $V = M_t \cdots M_1$. This order is essential: its column action is exactly the successive inverse-image experiment. In particular every singleton indicator, hence every column of V, is stable. □

For a sink K, let r_K denote the minimum rank of any word restricted to K, including the empty word.

Lemma 4.4. *The word of Lemma 4.3 has rank r_K on every sink to which that lemma applies.*

Proof. For a column v of V, stability implies $\mu Tv = \mu v$ for every word T. Since μ is strictly positive and these columns are indicators, Tv is nonzero exactly when v is nonzero. Thus TV and V have the same number of nonzero columns and hence the same transformation rank on K. If a word T had rank smaller than $\operatorname{rank}(V|_K)$, then $\operatorname{rank}((TV)|_K) \leq \operatorname{rank}(T|_K) < \operatorname{rank}(V|_K)$, a contradiction. □

Proposition 4.5. *There are words R, V, depending only on k, of length $k^{O(\sqrt{k})}$ such that, for every powered pair (A, B) in (2.1), R sends all states into sinks and V has minimum rank on every sink. With $W = RV$ and $S = W(Q)$, both AW and BW restrict to permutations of S.*

Proof. Concatenate the words of Lemma 3.1 over all types to obtain R. Once a state has entered a sink, all later letters keep it there. Concatenate the words of Lemma 4.3 over all types to obtain V. For a fixed pair and sink, the factor belonging to its type has rank r_K by Lemma 4.4. Composing on either side by words cannot increase that rank, and cannot decrease it below r_K by its definition. Thus V has the required rank. The number of types is $k^{O(\sqrt{k})}$, so the length bound survives concatenation.

For each sink K put $S_K = V(K)$. Since $R(K) \subseteq K$, $W(K) \subseteq V(K)$; their cardinalities are both r_K, and hence $W(K) = S_K$. Moreover $R(Q)$ is contained in the union of the sinks, so

$$W(Q) = \bigcup_K S_K. \tag{4.3}$$

This equality uses the factorization $W = RV$. Now AW maps each S_K into itself. Its image there is $(WAW)(K)$, whose rank is at least r_K and at most $|S_K| = r_K$. It is therefore a bijection on S_K. The same argument applies to BW. Since the sink images are disjoint, both macros are permutations of all of S. □

5. From permutations to all transformations

Proposition 5.1. *There are distinct balanced words u, v of length $\exp((1 + o(1))k/\log k)$ which agree whenever the first generator is a permutation on k points and the second is an arbitrary transformation.*

Proof. Take the words p_k, q_k of Theorem 1.2. In the powered generators use the macros $0W, 1W$, preceded by the common word W. By Proposition 4.5, the prefix maps into S and the macros act as permutations of S. A permutation identity on k points holds on S by adjoining fixed points if $|S| < k$. Hence

$$Wp_k(0W, 1W) = Wq_k(0W, 1W)$$

in every powered evaluation. The displayed literal words are distinct: the two macros have the same length and different first letters, so their substitution is injective; adjoining a common prefix also is injective. They are balanced because p_k, q_k are balanced and have the same number of substituted copies of W.

Replace each letter by its Lth power. This injective uniform substitution transfers the identity from $A = X^L, B = Y^L$ to X, Y and preserves balance. If $m = |p_k|$, the resulting length is $L(|W| + m(|W| + 1))$. Its logarithm is at most

$$(1 + o(1))\frac{k}{\log k} + O(\sqrt{k}\log k) = (1 + o(1))\frac{k}{\log k}.$$

□

Lemma 5.2 (Cyclic-set encoding)**.** *If $u = v$ is a balanced identity for pairs with the first generator a permutation on at most k points, substitute $0 \mapsto 0^k$, $1 \mapsto 0^k1$ and append 0^k to both words. The resulting words form a distinct balanced identity for T_k. Their length is at most $(k + 1)|u| + k$.*

Proof. Let X, Y be arbitrary transformations on k points. The map X^k sends every point into the cyclic set C of X. On C, the map $A = X^k$ is a permutation and $B = YX^k$ is a transformation of C to itself. If h denotes the stated substitution, associativity gives

$$h(u)(X, Y)X^k = X^k u(A, B), \qquad h(v)(X, Y)X^k = X^k v(A, B).$$

The right sides agree, which proves the identity.

To see injectivity of h, write a word uniquely as $0^{e_0}1\,0^{e_1}1\cdots1\,0^{e_t}$. Its image has zero-run lengths $k(e_0 + 1), \ldots, k(e_{t-1} + 1), ke_t$. These recover the original word; the case of no ones is included. Appending a common suffix preserves distinctness by cancellation in the free monoid. If the input counts are c_0, c_1, the output counts are $k(c_0 + c_1) + k$ zeros and c_1 ones. Thus balance is preserved, as is the claimed length bound. □

Proof of Theorem 1.1. Proposition 5.1 also applies on fewer than k points: extend both generators by fixed points to a k-element set. Lemma 5.2 now proves the identity assertion and (1.1), since its additional logarithmic cost is $O(\log k)$.

An identity for T_k is an identity for all transformations on at most k states, by the same extension argument. Therefore its two words finish in the same state in every complete deterministic automaton

of at most k states, for every starting state and every accepting set. No such automaton separates them.

Fix $0 < \varepsilon < 1$ and put $k = \lfloor (1-\varepsilon) \log n \log\log n \rfloor$. As $n \to \infty$, $k/\log k = (1 - \varepsilon + o(1)) \log n$. Equation (1.1) gives $|u_k| = |v_k| \leq n$ for all sufficiently large n. Append the same number of zeros to both words to reach length exactly n. They remain distinct and form an identity, so $S(n) > k$. Since this holds for every fixed $\varepsilon \in (0, 1)$, it gives (1.2). □

References

[1] A. A. Bulatov, O. Karpova, A. M. Shur, and K. Startsev, *Lower bounds on words separation: Are there short identities in transformation semigroups?*, Electronic Journal of Combinatorics **24** (2017), no. 3, Paper P3.35. doi:10.37236/6450.

[2] C. Xu and K. Regan, *An improved lower bound for separating words by permutation automata*, arXiv:2610.11098v1 (2026), Theorem A.1. `https://arxiv.org/abs/2610.11098`.

Email address: `howew@purdue.edu`

Email address: `huffma97@purdue.edu`

Email address: `jenwin@purdue.edu`

Email address: `kruerl@purdue.edu`