Electronic Colloquium on Computational Complexity, Report No. 186 (2018)

Lower bounds for data structures with space close to maximum imply circuit lower bounds

Emanuele Viola*

October 31, 2018

Abstract

Let $f : \{0,1\}^n \to \{0,1\}^m$ be a function computable by a circuit with unbounded fan-in, arbitrary gates, w wires and depth d. With a very simple argument we show that the m-query problem corresponding to f has data structures with space $s = n + r$ and time $(w/r)^d$, for any r. As a consequence, in the setting where s is close to m a slight improvement on the state of existing data-structure lower bounds would solve long-standing problems in circuit complexity. We also use this connection to obtain a data structure for error-correcting codes which nearly matches the 2007 lower bound by Gal and Miltersen. This data structure can also be made dynamic. Finally we give a problem that requires at least 3 bit probes for $m = n^{O(1)}$ and even $s = m/2 - 1$.

Proving data-structure lower bounds is a fundamental research agenda to which many papers have been devoted, see for example [Pat11] and the 29 references there. A *static data structure* for a function $f : \{0,1\}^n \to \{0,1\}^m$ is specified by an arbitrary map mapping an input $x \in \{0,1\}^n$ into s memory bits, and m query algorithms running in time t. Here the i query algorithm answers query i which is the i output bit of f. The state of time lower bounds for a given space s can be summarized with the following expression:

$$\log(m/n)/\log(s/n). \tag{1}$$

Specifically, no explicit function for which a bound better than (1) is known, for any setting of parameters. This is true even if time is measured in terms of *bit* probes (that is, the word size is 1), and the probes are non-adaptive. Note that in such a data structure a query is simply answered by reading t bits from the s memory bits at fixed locations that depend only on the query but not on the data. All the data structures in this paper will be of this simple form, making our results stronger.

On the other hand, for several settings of parameters we can prove lower bounds that either match or are close to (1) for explicit functions. Specifically, for *succinct* data structures using space $s = n + r$ when $r = o(n)$, the expression (1) becomes $(n/r)\log(m/n)$. Gal and Miltersen [GM07], Theorem 4, have proved lower bounds of the form $\Omega(n/r)$.

*Supported by NSF CCF award 1813930. Work partially done while visiting and supported by the Simons institute.

ISSN 1433-8092

When $s = n(1 + \Omega(1))$, (1) is at best logarithmic. Such logarithmic lower bounds where obtained for $m = n^{1+\Omega(1)}$ by Siegel [Sie04], Theorem 3.1, for computing hash functions. For several settings of parameters [Sie04] also shows that the bound is tight. The lower bound was rediscovered in [Lar12]. Their bounds are stated for non-binary, adaptive queries. For a streamlined exposition of this lower bound and matching upper bound, in the case of non-adaptive, binary queries see Lecture 18 in [Vio17]. Remarkably, if $s = n(1 + \Omega(1))$ and $m = O(s)$, or if $s = n^{1+\Omega(1)}$ no lower bound is known. Counting arguments (Theorem 8 in [Mil93]) show the existence of functions requiring polynomial time even for space $s = m - 1$.

In this paper we show that when m is close to s, say $m = O(s)$ or $m = s \cdot \operatorname{poly}\log s$ even a slight improvement over the state of data structure lower bounds implies new circuit lower bounds. Note that several well-studied problems do indeed have a number m of queries that is close to n (and so in particular m is close to s). They include representing (1) dense sets with membership queries, (2) arrays supporting rank/select, (3) well-bracketed expressions supporting matching brackets, (4) permutations supporting evaluations, (5) texts supporting accessing symbols and occurrences (access/select), (6) polynomials supporting evaluation, when the field size is close to the degree, or more generally retrieving symbols in an error-correcting code. See for example [Păt08] for (1)-(3), [Gol09], for (4)-(5), [GM07] for (6).

For problems when m is much larger than n, the question that is most relevant to this work is whether a data structure exists with space s close to m, say $s = m/\operatorname{poly}\log(m)$. When $m = s^{1+\epsilon}$ for a small enough ϵ our connection still applies, but one would need to prove polynomial lower bounds to obtain new circuit lower bounds. When say $m = s^2$ we do not obtain anything. It is an interesting open question to link that setting to circuit lower bounds.

Circuits with arbitrary gates. A *circuit* $C : \{0,1\}^n \to \{0,1\}^m$ *with arbitrary* gates is a circuit made of gates with unbounded fan-in, computing arbitrary functions. The complexity measures of interest here are the number w of wires, and the depth d. These circuits have been extensively studied, see for example Chapter 13 in the book [Juk12], titled "Circuits with arbitrary gates." The best-available lower bounds are proved in [Pud94, Che08b, Che08a]. In the case of depth 2 they are polynomial, but for higher depths they are barely super-linear.

Definition 1. The function $\lambda_d : \mathbb{N} \to \mathbb{N}$ is defined as $\lambda_1(n) := \lfloor \sqrt{n} \rfloor$, $\lambda_2(n) := \lceil \log_2 n \rceil$ and for $d \geq 3$ $\lambda_d(n) := \lambda^{\star}_{d-2}(n)$, where $f^{\star}(n)$ is the least number of times we need to iterate the function f on input n to reach a value ≤ 1. Note $\lambda_3(n) = O(\log \log n)$ and $\lambda_4(n) = O(\log^{\star} n)$.

With this notation in hand we can express the best-available lower bounds from [Pud94, Che08b, Che08a]. They show explicit functions $f : \{0,1\}^n \to \{0,1\}^m$ for which any depth-d circuit with w wires satisfies

$$w \geq \Omega_d(m \cdot \lambda_{d-1}(n)). \tag{2}$$

Those papers only consider the setting $m = n$, but we note that no lower bound better than (2) is available for $m > n$, because such a lower bound would immediately imply a bound better than $\Omega_d(n \cdot \lambda_{d-1}(n))$ for some subset of n output bits. (Write $f : \{0,1\}^n \to \{0,1\}^m$ as $f = (f_1, f_2, \ldots, f_{m/n})$ where each $f_i : \{0,1\}^n \to \{0,1\}^n$. If every f_i is computable in depth d with w wires then f can be computed in depth d with $(m/n)w$ wires.)

Problem 2. Exhibit an explicit function $f : \{0,1\}^n \to \{0,1\}^m$ that cannot be computed by circuits of depth d with $O(m\lambda_{d-1}(n))$ wires, with unbounded fan-in arbitrary gates, for some d.

We show how to simulate circuits with data structures.

Theorem 3. *Suppose the function $f : \{0,1\}^n \to \{0,1\}^m$ has a circuit of depth d with w wires, consisting of unbounded fan-in, arbitrary gates. Then f has a data structure with space $s = n + r$ and time $(w/r)^d$, for any r.*

Proof. Let R be a set of r gates in the circuit with largest fan-in. Note R may include some of the output gates, but does not include any of the input. Note that any other gate has fan-in $\leq w/r$, for else there are r gates with fan-in $> w/r$, for a total of $> w$ wires. The data structure simply stores in memory the input and the values of the gates in R. This takes space $s = n + r$. It remains to show how to answer queries efficiently.

Group the gates of the circuit in $d + 1$ levels where level 0 contains the n input gates and level d is the output. We prove by induction on i that for every $i = 0, 1, \ldots, d$, a gate at level i can be computed by reading $(w/r)^i$ bits of the data structure. For $i = d$ this gives the desired bound.

The base case $i = 0$ holds as every input gate is stored in the data structure and thus can be computed by reading $(w/r)^0 = 1$ bit.

Fix $i > 0$ and a gate g. If $g \in R$ then again it can be computed by reading 1 bit. Otherwise $g \notin R$. Then g has fan-in $\leq w/r$. Then we can compute g if we know the values of its w/r children. By induction each child can be computed by reading $(w/r)^{i-1}$ bits. Hence we can compute g by reading $(w/r)^i$ bits. □

This theorem shows that if for an explicit function $f : \{0,1\}^n \to \{0,1\}^m$ we have a data-structure lower bound showing that for space $s = n + r$ the time t must be

$$t \geq (\omega(m\lambda_{d-1}(n))/r)^d, \tag{3}$$

for some d, then we have new circuit lower bounds and Problem 2 is solved. We illustrate this via several settings of parameters.

Setting $s = 1.01n$ and $m = 100n$. As mentioned earlier in this setting no data structure lower bound is available: (1) gives nothing. We obtain that even proving, say, a $t \geq \log^{\star\star\star}(n)$ lower bound would solve Problem 2. Indeed, pick $d = 100$ and $r = 0.01n$. By Inequality (3) to solve Problem 2 it suffices to prove a lower bound of $t \geq \omega(\lambda_{99}(n))^{100}$, which is implied by $t \geq \log^{\star\star\star}(n)$.

The succinct setting $s = n+r$ with $r = o(n)$, $m = O(n)$. In this setting the best available lower bound is $t \geq \Omega(n/r)$, see [GM07], Theorem 4. For say $d = 4$ and $r \leq n/\log^{\star} n$, the right-hand side of (3) is within a polynomial of n/r. Hence for any setting of r the lower bound in [GM07] is within a polynomial of the best possible that one can obtain without solving Problem 2. In particular, for polylogarithmic redundancy $r = n/\log^c(n)$, we have lower bounds $\Omega(\log^c n)$, and proving $\log^{5c}(n)$ would solve Problem 2. We note that moreover the data-structure given by Theorem 3 is *systematic*: the input is copied in n of the $n + r$ memory bits. Thus the connection to Problem 2 holds even for lower bounds for systematic data structures.

The setting $m = n^{1+\epsilon}$ and $s = n(1 + \Theta(1))$. As mentioned earlier the best lower bound is $\Omega(\log m)$. We obtain that proving a data-structure lower bound of the form $t \geq n^{3\epsilon} \log^4 n$ would solve Problem 2. (Pick $r = n$ and $d = 3$.)

The setting $s = n^{1+\Omega(1)}$ and $m = s^{1+\epsilon}$. Here no data-structure lower bounds are known. We get that a lower bound of $t \geq s^{3\epsilon} \log^4 n$ would solve Problem 2.

Bounded fan-in circuits. We also get a connection with bounded fan-in circuits (over the usual basis And, Or, Not). Recall that it is not known if every explicit function $f : \{0,1\}^n \to \{0,1\}^m$ has circuits of size $O(m)$ and depth $O(\log m)$. Using Valiant's well-known connection [Val77] (see [Vio09], Chapter 3, for an exposition) we obtain the following.

Theorem 4. *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a function computable by bounded fan-in circuits with $O(m)$ wires and depth $O(\log m)$. Suppose $m = O(n)$. Then f has a data structure with space $n + o(n)$ and time $n^{o(1)}$.*

Proof. Suppose the circuit has $w = cm$ wires and depth $d = c \log m$. It is known [Val77] (see Lemma 28 in [Vio09]) that we can halve the depth by removing $cm/\log d$ wires. Repeating this process say $\log\log\log n$ times the depth becomes $O(\log n)/\log\log n = o(\log n)$, and we have removed $o(m)$ wires. Let R be the set of wires we removed. The data structure consists of the input and the values of R. Thus the redundancy is $|R| = o(n)$.

It remains to see how to answer queries fast. Because the depth is $o(\log n)$, the value at every output gate depends on at most $n^{o(1)}$ wires that were removed, and at most $n^{o(1)}$ input bits. Thus reading the corresponding bits we know the value of the output gate. □

In the other uses of Valiant's result, for depth-3 circuits and matrix rigidity, it is not important that each gate depends on few bits of R. However it is essential for us. For this reason it is not clear if the corresponding depth-reduction for Valiant's series-parallel circuits [Cal08] yields data structures.

For completeness we discuss briefly lower bounds for *dynamic* data structures. Here the best lower bounds are $\Omega(\log^{1.5} n)$ [LWY17]. We note that for an important class of problems, known as *decomposable* problems, it is known since [Ben79] how to turn a static data structure with query time t into a data structure that supports queries in time $O(t \log n)$ as well as insertions in time $O(\log n)$, see Theorem 7.3.2.5 in the book [Ove83]. Hence a strong lower bound for such "half-dynamic" data structures would imply a lower bound for static data structures, and one can apply the above theorems to get a consequence for circuits.

Data structures for error-correcting codes. We can use Theorem 3 to obtain new data structures for any problem which has efficient circuits. Let $f : \{0,1\}^n \to \{0,1\}^m$ be the encoding map of a binary error-correcting code which is *asymptotically good*, that is $m = O(n)$ and the minimum distance is $\Omega(m)$. Gal and Miltersen show [GM07], Theorem 4, that any data structure for this problem requires time $\geq \Omega(n/r)$ if the space is $s = n + r$. Combining a slight extension of Theorem 3 together with a circuit construction in [GHK+13] we obtain data structures with time $O(n/r) \log^3 n$.

Theorem 5. *There exists an asymptotically good, binary code whose encoding map $f : \{0,1\}^n \to \{0,1\}^m$ has data structures with space $n + r$ and time $O(n/r) \log^3 n$, for every r.*

Proof. First note that if in Theorem (3) we start with a circuit where the output gates have fan-in k, then we can have a data structure with time $k(w/r)^{d-1}$. The proof is the same as before, using the bound of k instead of w/r for the output gates. In [GHK+13], Section 6, it was shown the existence of an asymptotically good code whose encoding map is computable by depth-2 circuits made of Xor gates and with $w = O(n \log^2 n)$ wires. Moreover, the fan-in of the output gates is $k = O(\log n)$. The result follows. □

We also obtain a dynamic data structure for the encoding map.

Theorem 6. *There exists an asymptotically good, binary code whose encoding map $f : \{0,1\}^n \to \{0,1\}^m$ has dynamic data structure with space $O(n \log n)$ supporting updating an input bit in time $O(\log^2 n)$, and computing one bit of the codeword in time $O(\log n)$.*

Proof. Suppose f has a depth-2 circuit where the output gates have fan-in k and the input gates have fan-out ℓ. Then this gives a data structure where the memory consists of the middle layer of gates. To compute one bit of the codeword we simply read the k corresponding bits in the data structure, and to update one message bit we simply update the ℓ corresponding bits. Essentially this observation already appears in [BL15], except they do not parameterize it by the fan-in and fan-out, and so do not get a worst-case data structure.

An inspection of the encoding circuits [GHK+13] mentioned in the proof of Theorem (5) reveals that they also have a good bound on the fan-out ℓ of the input gates: $\ell = O(\log^2 m)$. This follows because the gates in the middle layer are grouped in $O(\log m)$ *range detectors*. And each range detector is constructed with a unique-neighbor expander where the degree in the input nodes is $O(\log m)$. □

In both data structures, the query algorithms are explicit, but the preprocessing and updates are not (because the corresponding layer in the circuits in [GHK+13] is not explicit).

A lower bound for large s. As remarked earlier we have no lower bounds when s is much larger than n. Next we prove a lower bound of $t \geq 3$ for any $m = n^{O(1)}$ even for $s = m/2 - 1$. The lower bound is established for a *small-bias generator* [NN93]. A function $f : \{0,1\}^n \to \{0,1\}^m$ is an ϵ-biased generator if the xor of any subset of the output bits is equal to one with probability p such that $|p - 1/2| \leq \epsilon$, over a uniform input. There are explicit constructions with $n = O(\log n/\epsilon)$ [NN93, AGHP92].

Theorem 7. *Let $f : \{0,1\}^n \to \{0,1\}^m$ be a $o(1)$-biased generator. Suppose f has a data structure with time $t = 2$. Then $s \geq m/2$.*

Proof. Suppose by contradiction that $s = m/2 - 1$. By inspection, any function g on 2 bits is either *affine*, or else is *biased*, that is either $g^{-1}(1)$ or $g^{-1}(0)$ contains only one input.

Suppose $\geq m/2$ of the queries are answered with affine functions. Then because $s < m/2$ some linear combination of these affine queries is fixed. This is a contradiction.

Otherwise $\geq m/2$ of the queries are answered with biased functions. We claim that there exists one biased query whose (set of two) probes are covered by the probes of other two biased queries. To show this we can keep collecting biased queries whose probes are not covered. We must stop eventually, for $s < m/2$. Hence assume that the probes of f_3 are covered by those of f_1 and f_2. By the small-bias property, the distribution of $(f_1, f_2, f_3) \in$

$\{0,1\}^3$ should be close to uniform. But this is not the case, because for some setting of (f_1, f_2) the value of f_3 is determined. □

Problem 8. Exhibit an explicit function $f : \{0,1\}^n \to \{0,1\}^m$ that does not have a data structure with space $s = n + m/10$, and time $t = 3$.

Acknowledgment. I am grateful to Omri Weinstein for stimulating discussions during his visit at Northeastern University and at the Simons institute.

References

[AGHP92] Noga Alon, Oded Goldreich, Johan Håstad, and René Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures & Algorithms*, 3(3):289–304, 1992.

[Ben79] Jon Louis Bentley. Decomposable searching problems. *Inf. Process. Lett.*, 8(5):244–251, 1979.

[BL15] Joshua Brody and Kasper Green Larsen. Adapt or die: Polynomial lower bounds for non-adaptive dynamic data structures. *Theory of Computing*, 11:471–489, 2015.

[Cal08] Chris Calabro. A lower bound on the size of series-parallel graphs dense in long paths. *Electronic Colloquium on Computational Complexity (ECCC)*, 15(110), 2008.

[Che08a] Dmitriy Yu. Cherukhin. Lower bounds for boolean circuits with finite depth and arbitrary gates. *Electronic Colloquium on Computational Complexity (ECCC)*, 15(032), 2008.

[Che08b] Dmitriy Yu. Cherukhin. Lower bounds for depth-2 and depth-3 boolean circuits with arbitrary gates. In *Computer Science - Theory and Applications, Third International Computer Science Symposium in Russia, CSR 2008, Moscow, Russia, June 7-12, 2008, Proceedings*, pages 122–133, 2008.

[GHK+13] Anna Gál, Kristoffer Arnsfelt Hansen, Michal Koucký, Pavel Pudlák, and Emanuele Viola. Tight bounds on computing error-correcting codes by bounded-depth circuits with arbitrary gates. *IEEE Transactions on Information Theory*, 59(10):6611–6627, 2013.

[GM07] Anna Gál and Peter Bro Miltersen. The cell probe complexity of succinct data structures. *Theoretical Computer Science*, 379(3):405–417, 2007.

[Gol09] Alexander Golynski. Cell probe lower bounds for succinct data structures. In *20th ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pages 625–634, 2009.

[Juk12] Stasys Jukna. *Boolean Function Complexity: Advances and Frontiers*. Springer, 2012.

[Lar12] Kasper Green Larsen. The cell probe complexity of dynamic range counting. In *ACM Symp. on the Theory of Computing (STOC)*, pages 85–94, 2012.

[LWY17] Kasper Green Larsen, Omri Weinstein, and Huacheng Yu. Crossing the logarithmic barrier for dynamic boolean data structure lower bounds. *CoRR*, abs/1703.03575, 2017.

[Mil93] Peter Bro Miltersen. The bit probe complexity measure revisited. In *Symp. on Theoretical Aspects of Computer Science (STACS)*, pages 662–671, 1993.

[NN93] Joseph Naor and Moni Naor. Small-bias probability spaces: efficient constructions and applications. *SIAM J. on Computing*, 22(4):838–856, 1993.

[Ove83] Mark H. Overmars. *The Design of Dynamic Data Structures*, volume 156 of *Lecture Notes in Computer Science*. Springer, 1983.

[Păt08] Mihai Pătraşcu. Succincter. In *49th IEEE Symp. on Foundations of Computer Science (FOCS)*. IEEE, 2008.

[Pat11] Mihai Patrascu. Unifying the landscape of cell-probe lower bounds. *SIAM J. Comput.*, 40(3):827–847, 2011.

[Pud94] Pavel Pudlák. Communication in bounded depth circuits. *Combinatorica*, 14(2):203–216, 1994.

[Sie04] Alan Siegel. On universal classes of extremely random constant-time hash functions. *SIAM J. on Computing*, 33(3):505–543, 2004.

[Val77] Leslie G. Valiant. Graph-theoretic arguments in low-level complexity. In *6th Symposium on Mathematical Foundations of Computer Science*, volume 53 of *Lecture Notes in Computer Science*, pages 162–176. Springer, 1977.

[Vio09] Emanuele Viola. On the power of small-depth computation. *Foundations and Trends in Theoretical Computer Science*, 5(1):1–72, 2009.

[Vio17] Emanuele Viola. Special topics in complexity theory. Lecture notes of the class taught at Northeastern University. Available at http://www.ccs.neu.edu/home/viola/classes/spepf17.html, 2017.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il