Expander-Based Cryptography Meets Natural Proofs

Igor C. Oliveira

Department of Computer Science, University of Oxford, UK
igor.carboni.oliveira@cs.ox.ac.uk

Rahul Santhanam

Department of Computer Science, University of Oxford, UK
rahul.santhanam@cs.ox.ac.uk

Roei Tell

Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel
roei.tell@weizmann.ac.il

──────── **Abstract** ────────

We introduce new forms of attack on *expander-based cryptography*, and in particular on Goldreich's pseudorandom generator and one-way function. Our attacks exploit *low circuit complexity* of the underlying expander's neighbor function and/or of the local predicate. Our two key conceptual contributions are:

1. We put forward the possibility that the *choice of expander* matters in expander-based cryptography. In particular, using expanders whose neighbour function has low circuit complexity might compromise the security of Goldreich's PRG and OWF in certain settings.

2. We show that the security of Goldreich's PRG and OWF is closely related to two other long-standing problems: Specifically, to the existence of *unbalanced lossless expanders* with low-complexity neighbor function, and to *limitations on circuit lower bounds* (i.e., natural proofs). In particular, our results further motivate the investigation of affine/local unbalanced lossless expanders and of average-case lower bounds against DNF-XOR circuits.

We prove two types of technical results that support the above conceptual messages. First, we *unconditionally break Goldreich's PRG* when instantiated with a specific expander (whose existence we prove), for a class of predicates that match the parameters of the currently-best "hard" candidates, in the regime of quasi-polynomial stretch. Secondly, conditioned on the existence of expanders whose neighbor functions have extremely low circuit complexity, we present attacks on Goldreich's generator in the *regime of polynomial stretch*. As one corollary, conditioned on the existence of the foregoing expanders, we show that either the parameters of natural properties for several constant-depth circuit classes *cannot be improved, even mildly*; or Goldreich's generator is insecure in the regime of a large polynomial stretch, *regardless of the predicate used.*

1   Introduction

Theoretical results provide strong evidence that if secure cryptography is possible, then many fundamental primitives such as one-way functions (OWF) and pseudorandom generators (PRG) can be implemented with a dramatic level of efficiency and parallelism. Specifically, security against efficient adversaries can be achieved by functions where each output bit only depends on a constant number of input bits (see, e.g., [6], and also [2] for a survey of recent results).

A concrete type of such construction is a conjectured form of OWF that is based on any *expander graph* and on a *local predicate*. Specifically, about two decades ago, Goldreich [16, 17] suggested the following candidate $\mathtt{owf} : \{0,1\}^n \to \{0,1\}^n$. Fix any bipartite graph $[n] \times [n]$ of right-degree $\ell \le O(\log(n))$ in which every set $S \subseteq [n]$ of size up to k on the right-hand side has at least (say) $1.01 \cdot |S|$ neighbors, and also fix a predicate $P : \{0,1\}^\ell \to \{0,1\}$. Then, given input $x \in \{0,1\}^n$, each output bit $\mathtt{owf}(x)_i$ is computed by applying P to the bits of x at the ℓ neighbors of $i \in [n]$. The expected running-time of a naive algorithm for inverting $\mathtt{owf}$ is at least $\exp(k)$ (see, e.g., [17, Sec. 3.2] and [2, Sec. 3.1]), and Goldreich conjectured that for an appropriate predicate P, no algorithm can perform significantly better.

In an extensive subsequent line of research (see, e.g., [1, 23, 4, 9, 5, 10, 14, 25, 15, 7, 8], and also see [3] for a related survey), Goldreich's construction was conjectured to yield not only a one-way function, but also a pseudorandom generator $\mathtt{prg} : \{0,1\}^n \to \{0,1\}^m$. In fact, in some settings the two conjectures are essentially equivalent (see [8, Sec. 3]).

The question of whether Goldreich's constructions are secure is a long-standing open problem. Much research has focused on necessary requirements from the *predicate* and from the *parameters* in order for the construction to be secure. Let us, for simplicity of presentation, focus on the PRG. In this case, the locality ℓ cannot be too small: If we want a PRG with super-linear stretch, then we must use $\ell \ge 5$ [23];[1] and if we want stretch $m = n^k$ then ℓ must be at least (roughly) $3k$ (see [25, Thm. II.11]). Also, as shown in [7], the predicate must have *high resilience* (i.e., all of the predicate's Fourier coefficients corresponding to sets of size at most $\Omega(\ell)$ are zero; see [26, Def. 3.4]) and high *rational degree* (this is a generalization of the requirement that the degree of the predicate as a polynomial $\mathbb{F}_2^\ell \to \mathbb{F}_2$ is $\Omega(\ell)$; see [26, Def. 3.7]).

The foregoing properties capture most existing attacks in the PRG setting. Indeed, as mentioned above, all these attacks exploit vulnerabilities of the *predicate* and of the *parameters*, but not of the underlying expander. In fact, prior to our work, the PRG was conjectured to be secure for *any underlying expander* with sufficiently good expansion properties. For reference, let us state such a strong form of conjectured security of the OWF, from a recent work by Applebaum and Raykov [8]. We say that a bipartite graph

---

[1] This impossibility result holds for *any* construction of a pseudorandom generator in $\mathcal{NC}^0$.

$G = ([n], [m], E)$ with right-degree ℓ is a $(k, 0.99)$-expander if for every set $S \subseteq [m]$ on the right-hand side of size at most k, the number of neighbors of S in G is at least $0.99 \cdot \ell \cdot |S|$. [2] Then, the conjecture is the following:

▶ **Assumption 1** (the strong EOWF assumption). *For a family $\mathcal{P} = \{P_\ell : \{0,1\}^\ell \to \{0,1\}\}_{\ell \in \mathbb{N}}$ of predicates, the* **strong** $EOWF(\mathcal{P})$ **assumption** *is the following. For any $(n^{.99}, .99)$-expander $G = ([n], [m], E)$ of right-degree $\ell \le n^{o(1)}$ such that $n \le m \le n^{\alpha \cdot \ell}$, where $\alpha > 0$ is a sufficiently small universal constant, Goldreich's function instantiated with G and P_ℓ cannot be inverted by circuits of size $t \le \exp(\alpha \cdot n^{.99})$ with success probability $1/t$.*

Applebaum and Raykov [8] suggested a suitable candidate predicate, which is the predicate $\mathsf{XOR\text{-}MAJ}(x) = \big(\oplus_{i=1,\ldots,\lfloor \ell/2 \rfloor} x_i\big) \oplus \big(\mathsf{MAJ}(x_{\lfloor \ell/2 \rfloor + 1}, \ldots, x_\ell)\big)$; this predicate indeed has both high resiliency and high rational degree.

1.1   A high-level digest of our contributions

Our main contribution is a *new form of attack* on Goldreich's pseudorandom generator, which exploits *computational complexity* properties (and, in particular, circuit complexity properties) of the expander and/or of the predicate on which the generator is based. In particular, our distinguishers are algorithms associated with *natural properties*, in the sense of Razborov and Rudich [28]. (Recall that a natural property against a circuit class $\mathcal{C}$ is an efficient algorithm that distinguishes a random string, interpreted as a truth table, from truth tables of $\mathcal{C}$-circuits.)[3]

We use our new form of attack to break the generator when it is instantiated with predicates that are sufficiently "strong" to withstand known attacks, but with expanders whose neighbor function has "low" circuit complexity. In high-level, the main conceptual implications of these results are the following:

1. The conjecture that the PRG and OWF are secure with *any expander*, given an appropriate predicate, *might be too naive*. In particular, the security of the constructions might crucially hinge on a choice of expander whose neighbor function has sufficiently high circuit complexity. Alternatively, if the latter is not true (i.e., if the PRG and OWF can be secure given any expander), then the predicate must have sufficiently high circuit complexity for the constructions to be secure in some settings (i.e., when the stretch is quasi-polynomial).

   Note that a random graph will (with high probability) not only be an expander, but also have a neighbor function with high circuit complexity. Therefore, our results do not put into question the security of the PRG and OWF when instantiated with a random graph.

2. There are significant interdependencies between *the security of Goldreich's PRG and OWF*, the existence of *unbalanced lossless expanders* with low-complexity neighbor function, and *limitations on circuit lower bounds* (i.e., natural proofs). Moreover (as further explained below), the questions motivated by our results are closely related both to existing results and to long-standing open problems in each area.

---

[2] We stress that lossless expansion (i.e., expansion to $\alpha \cdot \ell \cdot |S|$ vertices for $\alpha > 1/2$) is crucial in the PRG setting. To see this, note that one can duplicate a right-vertex in a $(k, 0.99)$-expander: This will produce a graph that, on the one hand, has good (but not lossless!) expansion properties, and on the other hand yields a corresponding PRG that is clearly insecure, regardless of the predicate.

[3] Natural properties are typically used to break *pseudorandom functions*, but the idea of using natural properties to break pseudorandom generators goes back to [28, Thm. 4.2]. Nevertheless, implementing this idea in our setting presents specific new challenges; for further discussion see Section 2.4.

Being more specific, we unconditionally break Goldreich's generator in the setting of quasi-polynomial stretch when it is instantiated with predicates with *high resilience and rational degree*, but with an expander whose neighbor function can be computed by $\mathcal{AC}^0[\oplus]$ *circuits of (small) subexponential size*. In fact, our predicates are variations on the specific XOR-MAJ predicate mentioned above. Using a known reduction of PRGs to OWFs (by [8]), it follows that Assumption 1 *does not* hold for some predicates with high resilience and rational degree. To prove this result we actually prove the *existence* of expanders with neighbor function as above; the latter proof, which uses certain *unconditional* PRGs that can be computed in a *strongly explicit* fashion, might be of independent interest. (See Section 1.2.)

In the regime of polynomial stretch, we put forward two assumptions about plausible extensions of known expander constructions in which the neighbor functions have even lower circuit complexity (compared to the expander mentioned above). Conditioned on *any* of the two assumptions, we show that exactly one of two options holds: Either the parameters of natural properties for certain restricted constant-depth circuit classes *cannot be improved, even mildly*; or Goldreich's generator is insecure in the regime of a large polynomial stretch, *regardless of the predicate used.* (See Section 1.3.)

Some important cryptographic applications crucially rely on the security of expander-based PRGs with polynomial, or even linear, stretch (see, e.g., [3, Sec. 4, "The Stretch"] and the references therein). We stress that our results for the setting of polynomial stretch are conditional on the existence of suitable expanders, and only break the PRG and OWF if there are natural properties for constant-depth circuit classes beyond what is currently known. Thus, further investigation is needed to determine whether our results have implications on the security of the aforementioned applications.

1.2   Unconditional results for quasi-polynomial stretch

Our main result for the setting of quasi-polynomial stretch is an attack that *unconditionally breaks* Goldreich's PRG when it is instantiated with a *specific expander that has optimal expansion properties*, and with a class of predicates that have both high resilience and high rational degree. Specifically:

▶ **Theorem 2** (unconditional attack on Goldreich's PRG with quasi-polynomial stretch; informal)**.** *For every $d \in \mathbb{N}$ and sufficiently large $k, c \in \mathbb{N}$ there exists a deterministic polynomial-time algorithm A that satisfies the following. Let $n \in \mathbb{N}$ be sufficiently large, let $m = n^{\log^k(n)}$, and let $\ell = c \cdot \log^k(n)$. Then, there exists an $(n^{0.99}, 0.99)$-expander $G = ([n], [m], E)$ of right-degree ℓ such that for any predicate $P : \{0,1\}^\ell \to \{0,1\}$ that can be computed by an $\mathcal{AC}^0[\oplus]$ circuit of depth d and sufficiently small sub-exponential size, when Goldreich's generator is instantiated with the expander G and the predicate P, the algorithm A distinguishes the m-bit output of the generator from a uniform m-bit string (with gap $> 1/2$).*

In fact, we actually prove a more general theorem, which exhibits a trade-off between the locality ℓ and the size of the $\mathcal{AC}^0[\oplus]$ circuit for the predicate P (for a precise statement see [26, Thm. 4.6]). That is, we are able to break the generator even with much larger locality (e.g., $\ell = n^{.01}$), at the expense of using a more restricted predicate family, namely that of $\mathcal{AC}^0[\oplus]$ circuits of smaller size (e.g., polynomial size). We stress that even the latter predicate family is rich enough to contain predicates that have both high resilience and high rational degree (see below).

Recall that the property of the expander $[n] \times [m]$ that we exploit in our attack is that its *neighbor functions* (i.e., the functions $\Gamma_i : [m] \to [n]$ for $i \in [\ell]$) have *low circuit complexity*. The expander in Theorem 2 in particular has neighbor functions that can be computed by $\mathcal{AC}^0[\oplus]$ circuits of small sub-exponential size, and we prove its existence in [26, Sec. 4.1] (see Section 2.2 for a high-level description).

Combining Theorem 2 with Applebaum and Raykov's reduction of expander-based PRGs to expander-based OWFs [8, Thm. 3.1] (i.e., they prove that if an arbitrary instance of Goldreich's OWF is secure, then a closely-related instance of Goldreich's PRG is also secure), our attack also breaks Goldreich's OWF. Specifically, we say that a predicate $P : \{0,1\}^\ell \to \{0,1\}$ is *sensitive* if it is "fully sensitive" to one of its coordinates (i.e., if for all $x \in \{0,1\}^\ell$ it holds that $P(x) = x_i \oplus P'(x)$, for some $i \in [\ell]$ and P' that does not depend on x_i). Then:

▶ **Corollary 3** (unconditional attack on Goldreich's OWF with quasi-polynomial stretch; informal)**.** *There exists a probabilistic polynomial-time algorithm A' that satisfies the following. Let $n \in \mathbb{N}$ be sufficiently large, let $m' = n^{k'=\mathrm{poly}\log(n)}$, and let $\ell = O(k')$. Then, there exists an $(n^{0.99}, 0.99)$-expander $G = ([n], [m'], E)$ of right-degree ℓ such that for any sensitive predicate $P : \{0,1\}^\ell \to \{0,1\}$ that can be computed by an $\mathcal{AC}^0[\oplus]$ circuit of sufficiently small subexponential size, when Goldreich's one-way function is instantiated with the expander G and the predicate P, the algorithm A inverts the function with success probability $\Omega(1/m'n)$.*

As immediate corollaries of Theorem 2 and of Corollary 3, we deduce that Assumption 1 does not hold for any sensitive predicate family that can be computed by $\mathcal{AC}^0[\oplus]$ circuits of sufficiently small sub-exponential size; and similarly, that the "PRG analogue" of Assumption 1, denoted $EPRG(\mathcal{P})$ in [8], does not hold for any predicate family that can be computed by $\mathcal{AC}^0[\oplus]$ circuits of sufficiently small sub-exponential size.

Recall that Applebaum and Raykov suggested the candidate predicate XOR-MAJ; we prove that when replacing majority by *approximate majority* (see [26, Def. 4.9]), the resulting predicate XOR-APPROX-MAJ still has both high resilience and high rational degree, and can also be computed by a polynomial-sized $\mathcal{AC}^0[\oplus]$ circuit (see [26, Sec. 4.3.2]). Thus, the predicate families in Theorem 2 and Corollary 3 contain predicates with high resilience and high rational degree, and even predicates that are variations on the "hard" candidate XOR-MAJ. [4]

Moreover, the predicate XOR-APPROX-MAJ does not even use the "full power" of the predicate family for which Theorem 2 allows us to break Goldreich's generator – the predicate XOR-APPROX-MAJ is computable by a circuit of polynomial size, whereas we can break the generator when the predicate can be computed by a circuit of sub-exponential size. We use this to our advantage by relying on the more general version of Theorem 2 (i.e., [26, Thm. 4.6]), which exhibits a trade-off between locality and the predicate class. Specifically, we obtain the following theorem, which breaks the generator even when the locality ℓ is large (e.g., $\ell = n^{\Omega(1)}$) and the predicate has high resilience and rational degree:

▶ **Theorem 4** (breaking Goldreich's generator with XOR-APPROX-MAJ and high locality)**.** *There exists $s > 1$ such that the following holds. Let $n \in \mathbb{N}$, let $m = n^{k=(\log(n))^s}$, and let $c \cdot k \leq \ell \leq n^{1/c}$, where c is a sufficiently large constant. Then, there exists an $(n^{0.99}, 0.99)$-expander $G = ([n], [m], E)$ of right-degree ℓ and a predicate $P : \{0,1\}^\ell \to \{0,1\}$ with resilience $\Omega(\ell)$ and rational degree $\Omega(\ell)$ (i.e., the predicate XOR-APPROX-MAJ) such that the following holds: When Goldreich's generator is instantiated with the expander G and the predicate P, the output of the generator can be distinguished from a uniform string (with gap $> 1/2$) by a deterministic $\mathrm{poly}(m)$-time algorithm.*

---

[4] Indeed, the main difference between XOR-MAJ and XOR-APPROX-MAJ seems to be in their *circuit complexity*, which corresponds to our main point that circuit complexity considerations are crucial for the security of Goldreich's PRG and OWF.

1.3   Conditional results for large polynomial stretch

Recall that the conjectured "hardness" of Goldreich's PRG (i.e., Assumption 1) refers both to the regime of polynomial stretch and to the regime of quasi-polynomial stretch (as long as the locality is sufficiently large to support the corresponding stretch). Could it be that complexity-based attacks separate these two parameter regimes? That is, could the reason that our attacks from Section 1.2 work be that the stretch of the generator is super-polynomial?

As mentioned in Section 1.1 (and will be explained in Section 2), the underlying technical components in our complexity-based attacks are *unbalanced lossless expanders* $[n] \times [m]$ whose neighbor functions have low circuit complexity, and *natural properties* against weak circuit classes. Our main results for the polynomial-stretch regime are of the following form: If lossless expanders $[n] \times [n^{O(1)}]$ with constant degree and (specific) "very simple" neighbor functions exist, then exactly one of two cases holds:

1. Either the parameters of natural properties for certain well-studied weak circuit classes *cannot be improved*, even mildly; or

2. For a sufficiently large polynomial stretch, Goldreich's generator is insecure when instantiated with a specific expander, *regardless of the predicate used*.

We now present two plausible assumptions on existence of suitable expanders, which are essentially improvements or extensions of existing explicit constructions. Conditioned on each assumption, we will contrast the security of Goldreich's PRG with the possibility of extending natural proofs for some well-studied circuit class.

1.3.1   Affine expanders and DNF-XOR circuits

As motivation for our first assumption, let us recall two well-known *explicit* constructions of unbalanced lossless expanders, which were given by Ta-Shma, Umans, and Zuckerman [30], and later on by Guruswami, Umans, and Vadhan [19]. We note that these two constructions are inherently different (the relevant construction from [30] is combinatorial, whereas the construction of [19] is algebraic), and yet in both constructions the neighbor function of the expander can be computed by *single layer of parity gates* (see [26, Sec. 5.1] for further details); we will call expanders with such a neighbor function *affine expanders*.

In the two foregoing affine expanders, the right-degree ℓ is polylogarithmic, and it is an open problem to improve the degree to be constant, which matches the degree of a random construction. However, a random construction is not necessarily affine. Our first assumption is that there indeed exists an *affine expander* with *constant degree*:

▶ **Assumption 5** (expanders with an affine neighbor function; informal, see [26, Ass. 5.4]). *There exists $\beta > 3$ such that for every constant $k \in \mathbb{N}$ and sufficiently large $n \in \mathbb{N}$, there exists an $(n^{.99}, 0.99)$-expander $G = ([n], [m = n^k], E)$ with right-degree $\ell = \beta \cdot k$ whose neighbor function $\Gamma_G : [m] \to ([n])^\ell$ can be computed by a single layer of parity gates.*

An unconditional proof of Assumption 5 will contrast the security of Goldreich's PRG with the possibility of extending the known natural properties for DNF-XOR *circuits of exponential size.* [5] Specifically, known lower bounds for DNF-XOR circuits yield natural

---

[5] Recall that DNF-XOR circuits are depth-3 circuits that consist of a top OR gate, a middle layer of AND gates, and a bottom layer of parities above the inputs.

properties useful against such circuits of size up to $2^{(1-o(1))\cdot n}$ (see [26, Sec. 5.1.2]).[6] Can these natural properties be extended to functions that are *approximated*, in the average-case sense, by DNF-XOR circuits of size $2^{\epsilon \cdot n}$, for some $\epsilon > 0$? This is the natural property that we contrast with the security of Goldreich's PRG:

▶ **Theorem 6** (is Goldreich's generator insecure, or are natural properties for DNF-XOR circuits "non-extendable"?; informal statement)**.** *Suppose that Assumption 5 holds. Then, exactly one of the following two options holds:*
1. *For all $\epsilon > 0$, there does not exist a natural property for the class of functions that can be approximated with success $1/2 + o(1)$ by* DNF-XOR *circuits of size $2^{\epsilon \cdot n}$.*
2. *For a sufficiently large $k \in \mathbb{N}$, Goldreich's generator is insecure with stretch $m = n^k$ and locality $\ell = \beta \cdot k$, for some expander and regardless of the local predicate used.*

We stress that for any value of $\beta > 3$ such that Assumption 5 holds, Theorem 6 follows with that value of β. Also note that Cohen and Shinkar [13] specifically conjectured that strong average-case lower bounds for DNF-XOR circuits of size $2^{\Omega(n)}$ hold, and proved a similar statement for the related-yet-weaker model of parity decision trees. (Their proof for parity decision trees indeed yields a natural property; see [26, Prop. 5.13].)

1.3.2 $\mathcal{NC}^0$ expanders and weak $\mathcal{AC}^0_4$ circuits

To motivate our next assumption, recall the recent explicit construction of lossless expanders by Viola and Wigderson [33, Thm. 4] (which builds on the well-known construction of Capalbo *et al.* [11]). In this construction the neighbor function can be computed by an $\mathcal{NC}^0$ circuit, but this construction is only for *balanced* expanders, rather than unbalanced ones. The following assumption is that such a construction is possible also for unbalanced expanders:

▶ **Assumption 7** (expanders with $\mathcal{NC}^0$ neighbor functions; informal, see [26, Ass. 5.19])**.** *There exists $\beta > 3$ such that for every constant $k \in \mathbb{N}$ and sufficiently large $n \in \mathbb{N}$, there exists an $(n^{.99}, 0.99)$-expander $G = ([n], [m = n^k], E)$ with right-degree $\ell = \beta \cdot k$ such that the neighbor function $\Gamma_G : [m] \to ([n])^\ell$ can be computed by an $\mathcal{NC}^0$ circuit.*

An unconditional proof of Assumption 7 will immediately break Goldreich's PRG in the polynomial-stretch regime by a complexity-based attack, when instantiated with a weak (but non-trivial) predicate class; see [26, Prop. 5.25]. But more importantly, such a proof will contrast the security of Goldreich's PRG with the possibility of extending the known natural properties for the class of exponential-sized $\mathcal{AC}^0$ *circuits of depth four with constant bottom fan-in and top fan-in*.

Since the precise trade-off between the parameters is a bit subtle, let us present the theorem in a simplified form (for a discussion of the more general setting, see [26, Sec. 5.2], and in particular [26, Sec. 5.2.3]). To do so, consider the (optimistic) possibility that in Assumption 7, there exists a single t such for any $k \in \mathbb{N}$ the arity of the $\mathcal{NC}^0$ circuit is t (i.e., each output bit of the circuit is a function of at most t input bits, where t does not depend on k); as far as we are aware of, such a hypothesis is possible even with $t = 1$. Relying on Håstad's switching lemma [21], for any $c = O(1)$ there exists a natural property against depth-four circuits with top fan-in c, bottom fan-in t, and size $2^{\epsilon \cdot (n/\log(c))}$ for a tiny universal

---

[6] Some of these natural properties actually run in slightly super-polynomial time, rather than in strictly polynomial time, but this issue is not crucial for our purpose of breaking Goldreich's PRG.

$\epsilon > 0$ (see [26, Cor. 5.24]). In the following theorem, the security of Goldreich's PRG is contrasted with the possibility of extending these natural properties to work against such circuits of size $2^{\beta \cdot (n/\log(c))}$ where $\beta > 3$.

▶ **Theorem 8** (is Goldreich's generator insecure, or are natural properties for very restricted $\mathcal{AC}^0$ circuits "non-extendable"?; informal statement)**.** *Suppose that Assumption 7 holds and that for any $k \in \mathbb{N}$, the arity of the $\mathcal{NC}^0$ circuit equals $t = O(1)$. Then, exactly one of the following two options holds:*

1. *For any $c \in \mathbb{N}$, there does not exist a natural property for depth-four $\mathcal{AC}^0$ circuits with top fan-in c and bottom fan-in t and size $O\left(2^{\beta \cdot (n/\log(c))}\right)$.*
2. *For a sufficiently large $k \in \mathbb{N}$, Goldreich's generator is insecure with stretch $m = n^k$ and predicate locality $\ell = \beta \cdot k$, for some expander and regardless of the predicate used.*

Recall that Assumption 7 is parametrized by β and by the arity of the $\mathcal{NC}^0$ circuit; we stress that for *any* values of β and t such that Assumption 7 holds, we get a corresponding "win-win" theorem such as Theorem 8 (for further details see [26, Sec. 5.2]). We also stress that both the natural properties that we can unconditionally prove and the natural properties referred to in Theorem 8 are for circuits of exponential size $2^{\Theta(n/\log(c))}$, and the difference is in the universal constant hidden in the Θ-notation.

As mentioned in Section 1.1, the *explicit* construction of highly unbalanced lossless expanders is a long-standing open problem, regardless of the circuit complexity of their neighbor function (see, e.g., [11], [32, Prob. 5.36 & 6.35], and [34, Chap. 8.7]). Assumptions 5 and 7, however, *do not concern explicit constructions* of expanders, but only assume their *existence*; in particular, the circuit family for the neighbor function of the graph may be *non-uniform*. (This is indeed the case for our construction of expanders in the quasi-polynomial stretch regime.)

2   Overviews of the proofs

2.1   The general form of attack

A natural property for a class $\mathcal{F}$ of functions is a deterministic polynomial-time algorithm that rejects all truth-tables of functions from $\mathcal{F}$, but accepts the truth-tables of almost all functions.[7] Indeed, a natural property for $\mathcal{F}$ exists only if almost all functions are *not* in $\mathcal{F}$. We will show how to use natural properties to break Goldreich's pseudorandom generator.

The key step in our proofs is to show, for every fixed $x \in \{0,1\}^n$, that $\mathtt{prg}(x)$ is the truth-table of a function from some class $\mathcal{F}$ of "simple" functions (e.g., $\mathtt{prg}(x)$ is the truth-table of a small constant-depth circuit). When we are able to show this, it follows that a natural property for $\mathcal{F}$ can distinguish the outputs of the PRG from uniformly-chosen random strings: This is because the natural property rejects any string in the output-set of the PRG (which is the truth-table of a function in $\mathcal{F}$), but accepts a random string, with high probability. (The general idea of using natural properties to break PRGs in this manner goes back to the original work of [28].)

Recall that Goldreich's PRG (i.e., the function $\mathtt{prg}$) is *always* a very "simple" function, since each output bit depends on a few (i.e., $\ell \ll n$) input bits. However, in order for our idea to work, we need that a *different* function (i.e., not the function $\mathtt{prg}$) will be simple:

---

[7] Throughout the paper, we identify a natural property with the "constructive" algorithm that recognizes the property (see [26, Def. 3.8].

Specifically, for every *fixed* input x, we want that the function $g_x : \{0,1\}^{\log(m)} \to \{0,1\}$ such that $g_x(i) = \text{prg}(x)_i$ will be "simple". That is, for a *fixed* "seed" x for the PRG, the function g_x gets as input an index i of an output bit, and computes the ith output bit of $\text{prg}(x)$ *as a function of i*. Intuitively, given $i \in [m]$, the function g_x needs to compute three different objects, successively:

- The neighbors $\Gamma_G(i)$ of the vertex $i \in [m]$ in G.
- The projections of the (fixed) string x on locations $\Gamma_G(i)$.
- The output of the predicate P on $x\restriction_{\Gamma_G(i)}$.

The proofs of our main theorems consist of showing instantiations of Goldreich's generator (i.e., choices for an expander and a predicate) such that g_x is a function from a class against which we can construct natural properties.

An alternative view of the construction of g_x above is as giving rise to a collection of *pseudorandom functions* (PRFs) $\{g_x : \{0,1\}^{\log(m)} \to \{0,1\}\}_{x \in \{0,1\}^n}$ that are based on (an instantiation of) Goldreich's PRG. In fact, the construction of g_x is technically reminiscent of constructions of PRFs that are based on Goldreich's PRG by Applebaum and Raykov [8]. However, the crucial point is that our transformation of Goldreich's PRG to a PRF incurs very little complexity overhead; in particular, the circuit complexity of g_x is essentially determined by the circuit complexity of the expander's neighbor function and of the predicate. For further discussion see Section 2.4.

2.2   The setting of quasi-polynomial stretch

The proof of Theorem 2 consists of showing that for a suitable expander G, and for any predicate P computable by an $\mathcal{AC}^0[\oplus]$ circuit of sufficiently small sub-exponential size, the function g_x can be computed by an $\mathcal{AC}^0[\oplus]$ circuit of sufficiently small sub-exponential size. Natural properties for such circuits, based on the lower bounds by Razborov and Smolensky [27, 29], are well-known (see, e.g., [28, 12]).

To describe the instantiations and the construction of an $\mathcal{AC}^0[\oplus]$ circuit for g_x, let $n \in \mathbb{N}$, and let $m = 2^{(\log(n))^k}$, for a sufficiently large k. The first technical component that we need is an expander graph G such that the function $i \mapsto \Gamma_G(i)$ can be computed by a sub-exponential sized $\mathcal{AC}^0[\oplus]$ circuit. We show that there exists such a graph, with essentially optimal parameters:

▶ **Theorem 9** (strongly-explicit lossless expander in $\mathcal{AC}^0[p]$; see [26], Thm. 4.5). *There exists a universal constant $d_G \in \mathbb{N}$ such that the following holds. For any $k \in \mathbb{N}$ and sufficiently large n and $m = 2^{(\log(n))^k}$, there exists a $(n^{0.99}, 0.99)$-expander $G = ([n], [m], E)$ of right-degree $\ell = O(\log(m)/\log(n))$, and an $\mathcal{AC}^0[\oplus]$ circuit $C_G : \{0,1\}^{\log(m)} \to \{0,1\}^{\ell \cdot \log(n)}$ of depth d_G and size $\text{poly}(n)$ such that for every $i \in [m]$ it holds that $C_G(i)$ outputs the list of ℓ neighbors of i in G.*

We stress that the depth d_G of the circuit in Theorem 9 does not depend on the relation between m and n, which is what will allow us to have a natural property for the circuit C_G. Specifically, recall that we have natural properties against $\mathcal{AC}^0[\oplus]$ circuits of depth d_G over $\ell_m = \log(m)$ input bits of sub-exponential size $2^{\Omega(\ell_m^{1/2d_G})}$. The size of C_G is $\text{poly}(n)$, and thus if we take $m = 2^{(\log(n))^k}$, for a sufficiently large k, then the size of C_G is a sufficiently small sub-exponent in its input length $\log(m)$.

In high-level, our construction of the expander in Theorem 9 is as follows. Our starting point is the well-known fact that a random graph is, with high probability, a good lossless bipartite expander (see, e.g., [26, Thm. 3.2]). The first step is to construct an *efficient*

test that gets as input a string $G \in \{0,1\}^{m'}$, where $m' = m \cdot \ell \cdot \log(n)$, considers G as the incidence-list of a graph, and decides whether or not G is an $(n^{.99}, .99)$-expander. We show that such a test can be implemented by a CNF of size 2^n (see [26, Clm. 4.2]). Hence, a pseudorandom generator for CNFs of size 2^n outputs, with high probability, a good expander. Specifically, we will use the pseudorandom generator of Nisan [24], which has seed length $\text{poly}(n)$. Thus, for some fixed "good" seed s, the output $NW(s) \in \{0,1\}^{m'}$ of the generator on s is an $(n^{.99}, .99)$-expander.

Our next step is to show that the expander represented by $NW(s)$ has neighbor functions that can be computed by an $\mathcal{AC}^0[\oplus]$ circuit. In fact, we will show that there exists a circuit that gets as input the index $i \in \{0,1\}^{\log(m')}$ of a bit in $NW(s)$ and outputs $NW(s)_i$. To do so we can rely, for instance, on the recent work of Carmosino *et al.* [12] , who showed that Nisan's generator can be made "strongly-explicit": That is, there exists an $\mathcal{AC}^0[\oplus]$ circuit of polynomial size that gets as input a seed z and an index i of an output bit, and computes the ith output bit of the generator on seed z. [8] By "hard-wiring" a "good" seed s into the latter circuit, we obtain an $\mathcal{AC}^0[\oplus]$ circuit of size $\text{poly}(n)$ that computes the output bits of the expander $NW(s)$. Indeed, a crucial point is that we did not algorithmically look for a good seed s, but rather non-uniformly fixed a "good" seed and "hard-wired" it into the circuit.

Given this expander construction, g_x can compute $i \mapsto \Gamma_G(i)$ in sub-exponential size, and we now need g_x to compute the projections of x on locations $\Gamma_G(i)$. To do so we simply "hard-wire" the entire string x into g_x. Specifically, after computing the function $i \mapsto \Gamma_G(i)$, the circuit now has the $\ell \cdot \log(n)$ bits of $\Gamma_G(i)$; it then uses ℓ depth-two formulas, each over $\log(n)$ bits and of size n, to compute the mapping $\Gamma_G(i) \mapsto x\restriction_{\Gamma_G(i)}$ by brute-force. This increases the size of the circuit for g_x by $\ell \cdot n < n^2$ gates, which is minor compared to the size $\text{poly}(n)$ of C_G from Theorem 9.

Finally, the circuit g_x has now computed the ℓ bits corresponding to $x\restriction_{\Gamma_G(i)}$, and needs to compute the predicate $P : \{0,1\}^{\ell} \to \{0,1\}$ on these bits. To get the circuit to be of sufficiently small sub-exponential size, we require that the predicate can be computed by a sufficiently small sub-exponential sized $\mathcal{AC}^0[\oplus]$ circuit. Specifically, we want that for some d_P, the predicate P can be computed by an $\mathcal{AC}^0[\oplus]$ circuit of depth d_P and size $2^{\ell^{\epsilon}}$, for a sufficiently small $\epsilon < 1/2(d_G + d_P + 2)$. We thus obtain a circuit for g_x of depth $d = d_G + d_P + 2$ and of size $O\left(2^{\ell^{\epsilon}}\right) < 2^{\log(m)^{1/2d}}$, [9] which is sufficiently small such that we have natural properties against it (for a formal statement of the parameters of this well-known natural property, proved by [28, 12], see e.g. [26, Thm. 3.9]).

2.3   The setting of large polynomial stretch

Why are the results in Section 2.2 applicable only to the setting of quasi-polynomial stretch? The main bottleneck is the expander construction in Theorem 9, which is an $\mathcal{AC}^0[\oplus]$ circuit. Specifically, since we only know of natural properties against $\mathcal{AC}^0[\oplus]$ circuits of at most sub-exponential size, and since the circuit that we obtain is of size at least n (because we hard-wire $x \in \{0,1\}^n$ to the circuit), we were forced to take $m = n^{\text{poly} \log(n)}$ such that n will be a small sub-exponential function of $\log(m)$.

In this section we circumvent this obstacle by using the hypothesized existence of expanders whose neighbor functions have "extremely simple" circuits. For simplicity, in the current high-level overview we present the attacks that are based on the existence of an expander

---

[8] A similar observation has appeared in other works, such as in [28, Thm. 4.2].

[9] For this calculation we assumed that $2^{\ell^{\epsilon}}$ dominates the size of the circuit (since the size of C_G is already sufficiently small); and we used the fact that $\ell = O(\log(m)/\log(n)) < \log(m)$, and that $\epsilon < 1/2d$ is sufficiently small).

as in Assumption 5; that is, a lossless expander $G = ([n], [m = n^k], E)$ of right-degree $\ell = O(k)$ whose neighbor function is an *affine function* (i.e., each output bit is a parity of input bits). The ideas that underlie the attacks that are based on expanders whose neighbor function is an $\mathcal{NC}^0$ circuit (as in Assumption 7) are similar, yet require a slightly more subtle parametrization (see [26, Sec. 5.2]).

Consider an instantiation of Goldreich's predicate with expander G as above and with a predicate $P : \{0,1\}^\ell \to \{0,1\}$ that can be computed by a CNF of size $2^{\delta \cdot \ell}$, where δ can be an arbitrarily large constant compared to k (or even $\delta = 1$, which allows for *any* predicate). In this case, for any $x \in \{0,1\}^n$, the output $\texttt{prg}(x)$ of the generator on x is a truth-table of a function g_x over an input $i \in \{0,1\}^{\log(m)}$ that can be computed as follows. One layer of *parity gates* maps $i \in [m]$ to $\Gamma_G(i) \in \{0,1\}^{\ell \cdot \log(n)}$ (this uses our assumption about the expander). Then, ℓ copies of a DNF over $\log(n)$ bits and of size n map the names of the ℓ vertices to $x{\upharpoonright}_{\Gamma_G(i)} \in \{0,1\}^\ell$, i.e., we project the bits of x that feed the predicate P (this DNF is essentially a "hard-wiring" of x into g_x). Finally, the CNF that computes P of size $2^{\delta \cdot \ell}$ maps $x{\upharpoonright}_{\Gamma_G(i)}$ to the value $P(x{\upharpoonright}_{\Gamma_G(i)})$. After collapsing a layer that connects the top CNF and the DNFs, we obtain an AND-OR-AND-XOR circuit g_x over $\ell_m = \log(m)$ input bits of size $O\big(\ell \cdot \log(n) + \ell \cdot n + 2^{\ell \cdot \delta}\big) = O\big(2^{\ell_m/k}\big)$ with top fan-in $2^{\delta \cdot \ell} = 2^{O(\delta \cdot k)}$.

When $\delta > 0$ is sufficiently small, we are able to unconditionally construct a natural property against circuits as above. However, the main point (i.e., Theorem 6) comes when considering the case $\delta = 1$; that is, *any* predicate $P : \{0,1\}^\ell \to \{0,1\}$. In this case, we first use the discriminator lemma of [20] to deduce that g_x can be $(1/2 + 1/2^{O(k)})$-approximated by a DNF-XOR circuit of size $O\big(2^{\ell_m/k}\big)$. Now (still under Assumption 5), exactly one of two options holds. The first option is that there exists a natural property for functions on ℓ_m input bits that can be $(1/2 + o(1))$-approximated by DNF-XOR circuits of size $2^{\Omega(\ell_m)}$; in this case, by taking k sufficiently large so that $2^{\ell_m/k}$ is sufficiently small, the natural property breaks the generator. The other option is that no such natural property exists, despite the fact that natural properties exist both for functions computed (in the worst-case) by DNF-XOR circuits of size $2^{(1-o(1)) \cdot \ell_m}$, and for functions approximated (even weakly) by parity decision trees of such size. This completes the sketch of the proof of Theorem 6.

2.4   The connection to expander-based pseudorandom functions

As mentioned in Section 2.1, our construction of the function $g_x : \{0,1\}^{\log(m)} \to \{0,1\}$ (i.e., $g_x(i) = P(x{\upharpoonright}_{\Gamma_G(i)})$) can be viewed as a construction of a collection of *pseudorandom functions* (PRFs) $\big\{g_x : \{0,1\}^{\log(m)} \to \{0,1\}\big\}_{x \in \{0,1\}^n}$ based on (an instantiation of) Goldreich's PRG. The crucial point in our transformation of Goldreich's PRG to a PRF is that the resulting PRF can have very low circuit complexity, depending essentially only on the complexity of the expander's neighbor function and of the predicate. In contrast, previously-known transformations of Goldreich's PRG to a PRF incur a significant overhead. Specifically, the transformation of Goldreich, Goldwasser, and Micali [18] yields a circuit with super-constant depth; whereas the constructions of Applebaum and Raykov [8] either yield only a *weak* PRF (which is not broken by natural properties, in general) or require complicated computations, which they implement using majority gates (i.e., the resulting function is in the class $\mathcal{TC}^0$, for which natural properties are neither known nor conjectured to exist).

Nevertheless, as pointed out by Applebaum,[10] a transformation of Goldreich's PRG to a *weak* PRF from [8] can be used to break the PRG when it is intantiated with a *random graph* and with a predicate with sufficiently low circuit complexity; this attack uses algorithms for

---

[10] Personal communication.

learning from random examples (instead of natural properties). Specifically, assume that Goldreich's PRG is secure when instantiated with a random graph $[n] \times [m]$ of right-degree ℓ and a predicate $P : \{0,1\}^\ell \to \{0,1\}$. Using the argument that appears in [8, Sec. 1.2.1] it follows that the function $g_x : \{0,1\}^{\ell \cdot \log(n)} \to \{0,1\}$ that considers its input as a set S of ℓ vertices in $[n]$, and outputs $g_x(S) = P(x\restriction_S)$, is a weak PRF against adversaries that make m (uniformly-chosen) queries. The complexity of g_x is essentially determined by the complexity of the predicate P.[11] Thus, if the latter is sufficiently small such that there exists an algorithm for learning g_x from $m - 1$ random examples, then g_x cannot be a weak PRF for adversaries that make m queries (since such an adversary can use the learning algorithm to predict the mth evaluation of the function at a random point, using the first $m - 1$ evaluations at random points). This contradicts the hypothesis that Goldreich's PRG is secure when instantiated with the predicate P and a random graph $[n] \times [m]$.

Loosely speaking, the argument above implies that Goldreich's PRG is not secure when the stretch is quasipolynomial (and the locality is polylogarithmic and sufficiently large), the graph is random, and the predicate is computable by an $\mathcal{AC}^0$ circuit of sufficiently small sub-exponential size; this relies on the learning algorithm of Linial, Mansour, and Nisan [22].[12] However, the latter class of predicates is much weaker than the class of predicates to which our main unconditional result applies (i.e., than the class of $\mathcal{AC}^0[\oplus]$ circuits of sufficiently small sub-exponential size, from Theorem 2). For example, such predicates have "low" resilience $o(\ell)$, because the Fourier weight of depth-d $\mathcal{AC}^0$ circuits over ℓ bits of size 2^{ℓ^ϵ} is .01-concentrated on sets of size at most $O(\ell^{\epsilon \cdot (d-1)}) = o(\ell)$ (see [22, 31]); therefore, such predicates do not withstand the attacks from [7]. Finally, recall that it is currently an open problem to understand the learnability of $\mathcal{AC}^0[\oplus]$ circuits from random examples.

References

1   Michael Alekhnovich. More on average case vs approximation complexity. *Computational Complexity*, 20(4):755–786, 2011.

2   Benny Applebaum. *Cryptography in Constant Parallel Time*. Information Security and Cryptography. Springer, 2014.

3   Benny Applebaum. Cryptographic Hardness of Random Local Functions. *Computational Complexity*, 25(3):667–722, 2016.

4   Benny Applebaum, Boaz Barak, and Avi Wigderson. Public-key cryptography from different assumptions. In *Proc. 42nd Annual ACM Symposium on Theory of Computing (STOC)*, pages 171–180. ACM, 2010.

5   Benny Applebaum, Andrej Bogdanov, and Alon Rosen. A dichotomy for local small-bias generators. *Journal of Cryptology*, 29(3):577–596, 2016.

6   Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. Cryptography in NC^0. *SIAM Journal of Computing*, 36(4):845–888, 2006.

7   Benny Applebaum and Shachar Lovett. Algebraic attacks against random local functions and their countermeasures. *SIAM Journal of Computing*, 47:52–79, 2018.

---

[11] More specifically, the circuit g_x can be implemented by $2 \cdot \ell$ depth-two formulas of size $O(n)$ to compute the mapping $S \mapsto x\restriction_S$, and then a circuit for P to compute $P(x\restriction_S)$.

[12] Specifically, let $n \in \mathbb{N}$, and let $\ell = \log^k(n)$ for some $k \in \mathbb{N}$. Assume that the predicate $P : \{0,1\}^\ell \to \{0,1\}$ is computable by an $\mathcal{AC}^0$ circuit of depth $d \in \mathbb{N}$ and size $s = 2^{\ell^\epsilon}$, where $\epsilon \leq 1/(d+1)$. Then, g_x can be implemented by a circuit of size $s' = O(\ell \cdot n + s)$ and depth $d + 1$. The algorithm of [22] learns g_x with error $1/s'$ from $m = n^{O(\log(s'))^d} = o(n^\ell)$ random examples in time poly(m), where the last bound on m is since $\epsilon \leq 1/(d+1)$. Therefore, Goldreich's PRG is not secure when the locality is $\ell = \log^k(n)$, the stretch is $m = o(n^\ell)$, and the ℓ-bit predicate is an $\mathcal{AC}^0$ circuit of depth d and size 2^{ℓ^ϵ}.

8   Benny Applebaum and Pavel Raykov. Fast pseudorandom functions based on expander graphs. In *Theory of cryptography. Part I*, volume 9985 of *Lecture Notes in Comput. Sci.*, pages 27–56. Springer, Berlin, 2016.

9   Andrej Bogdanov and Youming Qiao. On the security of Goldreich's one-way function. *Computational Complexity*, 21(1):83–127, 2012.

10 Andrej Bogdanov and Alon Rosen. Input locality and hardness amplification. *Journal of Cryptology*, 26(1):144–171, 2013.

11 Michael Capalbo, Omer Reingold, Salil Vadhan, and Avi Wigderson. Randomness Conductors and Constant-degree Lossless Expanders. In *Proc. 34th Annual ACM Symposium on Theory of Computing (STOC)*, pages 659–668, 2002.

12 Marco L. Carmosino, Russell Impagliazzo, Valentine Kabanets, and Antonina Kolokolova. Learning algorithms from natural proofs. In *Proc. 31st Annual IEEE Conference on Computational Complexity (CCC)*, page 10 (24), 2016.

13 Gil Cohen and Igor Shinkar. The complexity of DNF of parities. In *Proc. 7th Annual Innovations in Theoretical Computer Science Conference (ITCS)*, pages 47–58. ACM, 2016.

14 James Cook, Omid Etesami, Rachel Miller, and Luca Trevisan. On the one-way function candidate proposed by Goldreich. *ACM Transactions of Computation Theory*, 6(3):Art. 14, 35, 2014.

15 Vitaly Feldman, Will Perkins, and Santosh Vempala. On the Complexity of Random Satisfiability Problems with Planted Solutions. In *Proc. 47th Annual ACM Symposium on Theory of Computing (STOC)*, pages 77–86, 2015.

16 Oded Goldreich. Candidate One-Way Functions Based on Expander Graphs. *Electronic Colloquium on Computational Complexity: ECCC*, 7:90, 2000.

17 Oded Goldreich. Candidate one-way functions based on expander graphs. In *Studies in complexity and cryptography*, volume 6650 of *Lecture Notes in Computer Science*, pages 76–87. Springer, Heidelberg, 2011.

18 Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986.

19 Venkatesan Guruswami, Christopher Umans, and Salil Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *Journal of the ACM*, 56(4):Art. 20, 34, 2009.

20 András Hajnal, Wolfgang Maass, Pavel Pudlák, Márió Szegedy, and György Turán. Threshold circuits of bounded depth. *Journal of Computer and System Sciences*, 46(2):129–154, 1993.

21 Johan Håstad. *Computational Limitations of Small-depth Circuits*. MIT Press, 1987.

22 Nathan Linial, Yishay Mansour, and Noam Nisan. Constant depth circuits, Fourier transform, and learnability. *Journal of the Association for Computing Machinery*, 40(3):607–620, 1993.

23 Elchanan Mossel, Amir Shpilka, and Luca Trevisan. On ϵ-biased generators in NC^0. *Random Structures & Algorithms*, 29(1):56–81, 2006.

24 Noam Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, 11(1):63–70, 1991.

25 Ryan O'Donnell and David Witmer. Goldreich's PRG: evidence for near-optimal polynomial stretch. In *Proc. 29th Annual IEEE Conference on Computational Complexity (CCC)*, pages 1–12. IEEE, 2014.

26 Igor Carboni Oliveira, Rahul Santhanam, and Roei Tell. Expander-Based Cryptography Meets Natural Proofs. *Electronic Colloquium on Computational Complexity: ECCC*, 25:159, 2018. URL: https://eccc.weizmann.ac.il/report/2018/159/.

27   Alexander A. Razborov. Lower bounds on the size of constant-depth networks over a complete basis with logical addition. *Mathematical Notes of the Academy of Science of the USSR*, 41(4):333–338, 1987.

28   Alexander A. Razborov and Steven Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55(1, part 1):24–35, 1997.

29   Roman Smolensky. Algebraic Methods in the Theory of Lower Bounds for Boolean Circuit Complexity. In *Proc. 19th Annual ACM Symposium on Theory of Computing (STOC)*, pages 77–82, 1987.

30   Amnon Ta-Shma, Christopher Umans, and David Zuckerman. Lossless condensers, unbalanced expanders, and extractors. *Combinatorica*, 27(2):213–240, 2007.

31   Avishay Tal. Tight Bounds on the Fourier Spectrum of AC0. In *Proc. 32nd Annual IEEE Conference on Computational Complexity (CCC)*, pages 15:1–15:31, 2017.

32   Salil P. Vadhan. *Pseudorandomness*. Foundations and Trends in Theoretical Computer Science. Now Publishers, 2012.

33   Emanuele Viola and Avi Wigderson. Local Expanders. *Computational Complexity*, 2017.

34   Avi Wigderson. *Mathematics and Computation (book draft)*, August 26, 2018. Accessed at `https://www.math.ias.edu/avi/book`, August 26, 2018.