Resilient functions: Optimized, simplified, and generalized

Peter Ivanov[*] Emanuele Viola[*]

June 27, 2024

Abstract

An n-bit boolean function is resilient to coalitions of size q if any fixed set of q bits is unlikely to influence the function when the other $n - q$ bits are chosen uniformly. We give explicit constructions of depth-3 circuits that are resilient to coalitions of size $cn/\log^2 n$ with bias n^{-c}. Previous explicit constructions with the same resilience had constant bias. Our construction is simpler and we generalize it to biased product distributions.

Our proof builds on previous work; the main differences are the use of a tail bound for expander walks in combination with a refined analysis based on Janson's inequality.

1 Introduction

A resilient function, informally speaking, is a function for which a malicious adversary that controls a small coalition of the input bits can not change the output with high probability. Resilient functions have a wide range of applications. They were initially introduced for *coin flipping protocols* [BL85, AL93, RZ98]. They have also been used to construct *randomness extractors* [KZ07, GVW15, CZ16, Mek17, CL16, HIV22] and more recently, to show *correlation bounds* against low-degree $\mathbb{F}_2$ polynomials [CHH+20].

Our main contribution is an improved and simplified construction that generalizes to product distributions. Before we present our results we introduce some definitions.

Definition 1. Fix a function $f : \{0,1\}^n \to \{0,1\}$, a distribution D over $\{0,1\}^n$, and a coalition $Q \subseteq [n]$. Define $I_{Q,D}(f)$ to be the probability that f is not fixed after the bits indexed by $\overline{Q}$ are sampled according to D. When D is the uniform distribution we write $I_Q(f)$.

We say f is *ρ-tradeoff resilient under D* if for any $Q \subseteq [n], I_{Q,D}(f) \le |Q|\rho$. We simply say f is *ρ-tradeoff resilient* when D is the uniform distribution.

[*]Partially supported by NSF grant CCF-2114116.

In this paper, every occurrence of "c" denotes a possibly different positive real number. Replacing "c" with $O(1)$ everywhere is consistent with one common interpretation of the big-Oh notation.

First we provide non-explicit tradeoff resilient circuits.

Theorem 2. *For infinitely many n there exist monotone depth 3, size n^c circuits $C : \{0,1\}^n \to \{0,1\}$ which are $\left(\frac{c \log^2 n}{n}\right)$-tradeoff resilient with bias $n^{-1+o(1)}$.*

This result is considered folklore, but we are not aware of any proofs in the literature. Related works [BL85, AL93, RZ98, CZ16, Mek17, Wel20] either do not prove a full tradeoff, are not as balanced, or have worse resilience.

The construction in Theorem 2 is due to Ajtai and Linial [AL93]. In their seminal work, they proved their construction is resilient to coalitions of size $cn/\log^2 n$ which is close to the theoretical best $cn/\log n$ implied by the KKL Theorem [KKL88]. However, Ajtai and Linial did not prove any tradeoff resilience. Russell and Zuckerman [RZ98] then showed the Ajtai-Linial construction has tradeoff resilience for coalitions of size $n/\log^c n$, but not for smaller coalitions. There is a more recent exposition [Wel20] on the topic; however, it proves a tradeoff that is weaker. In particular, for coalitions of constant size the resulting influence will be $c \log n/\sqrt{n}$ instead of $c \log^2 n/n$.

Next we state our main result, which is an explicit tradeoff resilient function that generalizes to product distributions, improves the bias to essentially match the non-explicit construction, and has a simplified proof.

Definition 3. B_σ denotes the distribution over $\{0,1\}^n$ where each bit is independently set to 1 with probability σ.

Theorem 4. *Fix integers $w \le v \le n$ where v is prime and $\sigma \in (0, 1/2]$ s.t. $n = vw$ and $\sigma^{-w} = \frac{Cv}{\log v}$ for a fixed constant C. Then there are explicit monotone depth 3, size n^c circuits $C : \{0,1\}^n \to \{0,1\}$ which are $\left(\frac{c\sigma^{-2}}{\log(\sigma^{-1})} \cdot \frac{\log^2 n}{n}\right)$-tradeoff resilient under B_σ with bias $\sigma^{-2}/n^{1-o(1)}$.*

Let us provide some background on existing explicit resilient functions. It is folklore that Majority is $c/\sqrt{n}$-tradeoff resilient. Building on this, Ben-Or and Linial showed that Recursive-Majority-3 is $n^{-0.63\ldots}$-tradeoff resilient [BL85].

More recently, Chattopadhyay and Zuckerman gave an explicit $n^{-0.99}$-tradeoff resilient function with bias n^{-c} [CZ16]. Moreover, they derandomized the original Ajtai-Linial construction so their function is computable by a small circuit. This was a key part of their two-source extractor breakthrough.

Meka [Mek17] then improved the derandomization and achieved $c \log^2 n/n$-tradeoff resilience, but with constant bias. [IMV23] gave a generic way to compose tradeoff resilient circuits and this allowed for nearly optimal size circuits with tradeoff resilience $\log^c n/n$. And using this composition result, one can xor $c \log n$ copies of Meka's construction to achieve circuits with tradeoff resilience $c \log^3 /n$ and bias n^{-c}.

We remark all of the results stated above are over the uniform distribution. A natural question is to consider resilience over non-uniform distributions like product distributions. Such distributions arise naturally; for instance, in a voting scenario one might consider the votes being cast independently but not uniformly.

The recent work of [FHH+19] investigates this question by studying how resilient *any function* can be under arbitrary product distributions. They show that in this setting, the KKL theorem essentially still holds. Specifically, they prove a function can not be resilient to coalitions of size $> cn \log\log n/\log n$ under any product distribution.

We complement their result by extending the Ajtai-Linial construction to product distributions of the form B_σ, though with some loss in resilience depending on σ. Its not clear whether this dependence is necessary. Besides complementing [FHH+19], our work might be useful for further improved resilient constructions; see Section 1.2 for additional discussion.

Next we provide a table with known resilient circuit constructions under $B_{1/2}$.

Explicit:	Resilience:	Tradeoff:	Bias:	Monotone:	Depth:	Size:	Citation
Yes	$cn^{-1/2}$	Yes	0	Yes	$c\log n$	n^c	Folklore
Yes	$n^{-0.63...}$	Yes	0	Yes	$c\log n$	cn	[BL85]
No	$c\log^2 n/n$	No	n^{-c}	No	3	cn^2	[AL93]
No	$c\log^2 n/n$	Partial	n^{-c}	No	3	cn^2	[RZ98]
No	$c\log^2 n/n$	Partial	n^{-c}	No	3	cn^2	[Wel20]
No	$c\log^2 n/n$	Yes	n^{-c}	Yes	3	n^c	Theorem 2
Yes	$n^{-0.99}$	Yes	n^{-c}	Yes	4	n^c	[CZ16]
Yes	$c\log^2 n/n$	Yes	c	Yes	3	n^c	[Mek17]
Yes	$\log^c n/n$	Yes	n^{-c}	No	c	$n^{1.01}$	[IMV23]
Yes	$c\log^3 n/n$	Yes	n^{-c}	No	5	n^c	[IMV23]
Yes	$c\log^2 n/n$	Yes	n^{-c}	Yes	3	n^c	Theorem 4

Our next contribution is an explicit circuit that matches the KKL Theorem up to constant factors and is exactly balanced under $B_{1/2}$. As far as we know, only nearly balanced circuits were known prior to this work.

Theorem 5. *For infinitely many n, there is an explicit circuit $C : \{0,1\}^n \to \{0,1\}$ such that $I_Q(C) \leq c\log n/n$ for any $Q \subseteq [n] : |Q| = 1$ and $\mathbb{E}[C] = 1/2$.*

To prove this we use a result by Ajtai and Linial which gives a generic way to turn a nearly balanced circuit into an exactly balanced one, without hurting the resilience too much. However, it comes at a cost to the depth and monotonicity of the original circuit.

1.1 Proof of Theorem 4

The final construction is an Ajtai-Linial style AND of TRIBES circuit, which will be defined through a generator G. The bulk of the proof is showing that the resulting circuit will be 1) resilient and 2) nearly balanced whenever G is a sampler and a design. 1) follows from the sampler property, while both properties are needed to prove 2). Our starting point is an expander walk which is a sampler by known tail bounds. However, an expander walk does not form a good design since two different walks can differ in just one node. Thus we pad the expander walk with a short Reed-Solomon code which has good design properties. This construction achieves a polynomial size domain which results in a polynomial size circuit.

Constructing a circuit through G First we set up notation. We identify n with a $v \times w$ matrix and for any $y \in [v]^w$ we associate a subset of $[n]$ of size w with one element per column in the natural way: the kth element where $k \in [w]$ is in column k and row $y[k]$. We let $S(y)$ denote this subset.

From $S(y)$ we obtain other disjoint sets by increasing the row indices by $j \bmod v$. We let $S(y, j)$ denote this set. Note that for any $y \in [v]^w$ the sets $S(y, 0), \ldots, S(y, v-1)$ form a partition of $[n]$ into v sets of size w each.

We now define C_G.

Definition 6. For any $G : [u] \to [v]^w$ and $i \in [u]$ we define

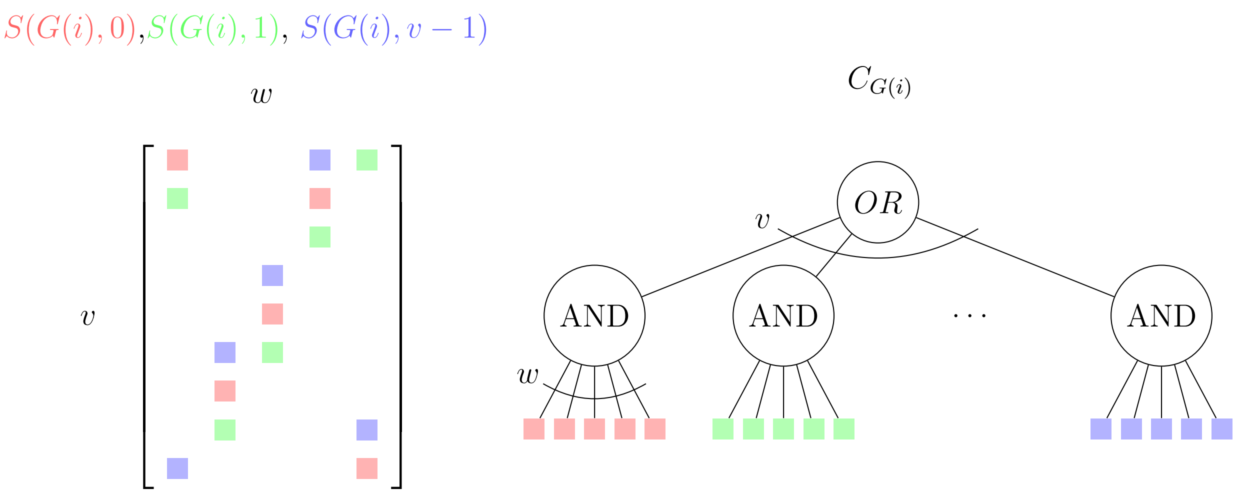
$$C_{G(i)}(x) := \vee_{j \in [v]} \wedge_{k \in S(G(i),j)} x_k$$

and we define

$$C_G(x) := \wedge_{i \in [u]} C_{G(i)}(x).$$

Note C_G is an AND_u-OR_v-AND_w circuit and $C_{G(i)}$ is a read-once OR_v-AND_w circuit, where AND_w denotes a layer of AND gates of fan-in w, etc. For intuition see the following illustration.

$G(i)$ defines a read-once OR_v-AND_w subcircuit:



We next define some relevant quantities.

Definition 7. For integers $1 \leq w \leq v \leq u$ and $0 < \sigma < 1$ we define

$$p := (1 - \sigma^w)^v, \quad bias(u, v, w, \sigma) := (1 - p)^u.$$

Since the $C_{G(i)}(x)$ are read-once, we have $\mathbb{P}[C_{G(i)}(B_\sigma) = 0] = p$. And if we supposed that C_G was read-once (on uvw bits), then we would have $\mathbb{P}[C_G(B_\sigma) = 1] = bias(u, v, w, \sigma)$. Jumping ahead, we will show that when G is a sampler, C_G on vw bits behaves similarly. So by setting the parameters appropriately and the following fact, C_G will be nearly balanced.

Fact 8. *Fix $1 \le w \le v \le u$ and $0 < \sigma < 1$ so that $\sigma^{-w} \ln(u/\ln 2) \le v \le \sigma^{-w} \ln(u/\ln 2) + 1$. Then $|bias(u, v, w, \sigma) - 1/2| \le c\sigma^w$.*

For the sake of flow, we defer the proof of Fact 8 and some of the other technical claims below to the appendix.

The sampler property

Definition 9. $G : [u] \to [v]^w$ is a (α, β)-*sampler* if for any $f_1, \dots, f_w : [v] \to \{0, 1\}$ s.t. $\mu := \mathbb{E}_{y\in[v]^w}[F(y)] \le \frac{1}{\alpha\beta \ln u}$ where $F := \sum_{k\in[w]} f_k$, we have

$$\mathop{\mathbb{E}}_{i\in[u]}[\alpha^{F(G(i))}] \le e^{c\beta\alpha\mu}.$$

When $\beta = c$ we say G is an α-sampler, and when $\alpha = 2, \beta = c$ we say G is a sampler.

The $1/\ln u$ factor is present in the definition for technical reasons. We will also need a second version of the definition given next.

Claim 10. *The statement in Definition 9 is equivalent to the following:*

$$\mathop{\mathbb{E}}_{i\in[u]}[\alpha^{F(G(i))}\mathbf{1}_{F(G(i))\neq 0}] \le c\beta\alpha\mu.$$

Next we show the identity function is a sampler.

Fact 11. *The identity function $I : [v]^w \to [v]^w$ is a sampler.*

This directly follows by the proceeding.

Fact 12. *Let $X_1, \dots, X_w$ be independent $\{0, 1\}$-valued r.v. s.t. $\mu := \mathbb{E}[X] < 1$ where $X := \sum_{k\in[w]} X_k$. Fix $\alpha > 1$ s.t. $\alpha\mu \le 1$. Then $\mathbb{E}[\alpha^X] \le e^{\alpha\mu}, \mathbb{E}[\alpha^X \mathbf{1}_{X\neq 0}] \le 2\alpha\mu$.*

However, the identity function would not result in an efficient construction since the resulting circuit would have size $\ge u = v^w = n^{c \log n}$. Thus we are interested in samplers with a polynomial size domain $u = v^c$. The existence of such samplers follows by the probabilistic method (see Lemma 19). For an explicit construction, we can take G to be a random walk over a (v, d, λ) expander, which is a regular graph with v nodes, degree d, and spectral expansion λ. Tail bounds on expander walks [RR17] imply that G is indeed a good sampler.

Theorem 13 ([RR17])**.** *Let $G : [vd^w] \to [v]^w$ output walks of length w on a (v, d, λ) expander for $\lambda < 1/3$. Then G is an α-sampler for any $1 < \alpha < 1/2\lambda$.*

We remark that tail bounds from earlier works [Lez98, Wag08], appropriately extended, would also suffice for our main result.

The design property

Definition 14. We say G is a d-design if $|S(G(i),j) \cap S(G(i'),j')| \leq w-d$ for any $i,i' \in [u], j,j' \in [v]$ s.t. $(i,j) \neq (i',j')$.

In other words, any two sets differ in at least d elements. Note $|S(G(i),j) \cap S(G(i),j')| = 0$ for any $j \neq j'$ by definition.

We will require the design properties of the Reed-Solomon code:

Fact 15. *Fix some prime v and integers $\ell \leq w \leq v$. The degree ℓ Reed-Solomon code $RS : [v]^\ell \to [v]^w$ is ℓ-wise independent and a $w-\ell$ design.*

The final construction The final generator is the concatenation of two different codes, as is done in [Mek17]. We replace the complicated extractor in [Mek17] with a standard expander walk, which grants the sampler property by Theorem 13.

The second code will be a constant-degree Reed-Solomon code of length approximately $c \log\log n$. The final generator will then possess the desired design property, albeit with a small loss in the sampler property.

Lemma 16. *Fix integers $w \leq v$ where v is prime and $\sigma \in (0, 1/2]$ s.t. $\sigma^{-w} = \frac{Cv}{\log v}$ for a fixed constant C. Then there is an explicit $G : [u] \to [v]^w$ that is a $(\sigma^{-1}, \sigma^{-1})$-sampler and $4 \log\log u / \log(\sigma^{-1})$-design, where $u = \mathrm{poly}(v)$.*

Proving resilience and small bias The remainder of the proof consists in showing that circuits obtained from G are 1) resilient and 2) nearly balanced. 1) was known for $\sigma = 1/2$, and it is straightforward to generalize to $\sigma \neq 1/2$.

Lemma 17. *Fix integers $w \leq v \leq u$ and $\sigma \in (0, 1/2]$ so that $\sigma^{-w} = v/\ln(u/\ln 2)$ and suppose $G : [u] \to [v]^w$ is a (σ^{-1}, β)-sampler. Then for any $Q \subseteq [n]$ s.t. $|Q| \leq c\sigma^{-w+1}/\beta$,*

$$I_{Q,B_\sigma}(C_G) \leq |Q| \cdot c\beta\sigma^{w-1}.$$

For 2), we follow an approach similar to that of [CZ16, Mek17], which proved small bias by combining Janson's inequality with the requirement that G is a good design. However, we consider a *slightly tighter version* of Janson's inequality; see Proposition 24 and the discussion there. This crucially allows us to apply the sampler property of G which in turn allows us to simplify the design requirements on G and improve the final bias to essentially match the nonexplicit construction.

Lemma 18. *Suppose $G : [u] \to [v]^w$ is a (σ^{-1}, β)-sampler and d-design. Then*

$$|\mathbb{E}[C_G(B_\sigma)] - bias(u,v,w,\sigma)| \leq e^{\sigma^d \log^4 u} \frac{\beta\sigma^{-1}}{n^{1-o(1)}}.$$

We are now ready to prove Theorem 4.

Proof of Theorem 4. Take G from Lemma 16. By Lemma 17,

$$I_{Q,B_\sigma}(C_G) \le |Q| \cdot c\sigma^{-2}\sigma^w = |Q| \cdot \frac{c\sigma^{-2}}{\log(\sigma^{-1})} \cdot \frac{\log^2 n}{n}.$$

The last inequality follows since $\sigma^{-w} = cv/\log v$ thus $w = c \log v/\log(\sigma^{-1})$ and $v = n/w$ so $\log v = c \log n$.

By Lemma 18, $|\mathbb{E}[C_G(B_\sigma)] - bias(u,v,w,\sigma)| \le \sigma^{-2}/n^{1-o(1)}$. We conclude by Fact 8. $\square$

1.2 Future Directions

A long-standing open problem is to improve the $cn/\log^2 n$ resilience achieved by Ajtai and Linial. In this direction, we pose the following question: Is there a function $f : \{0,1\}^n \to \{0,1\}$ such that 1) $\mathbb{P}[f = 0] = 1/n$ and 2) the influence of each bit is $c \log n/n^2$? In other words, are there biased functions matching the KKL theorem?

It is well-known there are balanced functions which match KKL, namely TRIBES. However, when the parameters are set so that $\mathbb{P}[\text{TRIBES} = 0] = 1/n$, the influence of each bit becomes $c \log^2 n/n^2$. The Ajtai-Linial construction is an AND over such biased TRIBES.

Thus any progress on the question above can be viewed as a first step towards beating $cn/\log^2 n$ resilience. The works of [EG20, EKLM22] provide some information on the structure of functions which match the KKL Theorem that may be helpful.

Another problem is to obtain alternative constructions that improve on [BL85]. One possible approach follows from Theorem 4 by setting w constant (and a suitable σ) which allows one to reach influence $n^{-0.99}$; alternative derandomizations of the Ajtai-Linial construction in this setting could be of interest.

1.3 Organization

In Section 2 we prove Theorem 2. We prove Lemmas 16, 17, 18 in Sections 3, 4, 5 respectively. In Section 6 we prove Theorem 5.

2 Nonexplicit tradeoff resilient circuits

Here we prove the existence of good samplers and designs over the uniform distribution.

Lemma 19. *For large enough integers $w \le v$ there is a $G : [v^2 2^{2w} \ln v] \to [v]^w$ that is a sampler and $\lfloor w/2 \rfloor$-design.*

Combining this with Lemmas 17 and 18 we can prove Theorem 2.

Proof of Theorem 2. Fix w and set $v = \lceil 2^w \ln(u/\ln 2) \rceil$ where $u := (vw)^4$ and set $n = vw$. Note $u \ge v^2 2^{2w} \ln v$. Take G from Lemma 19. By Lemma 17,

$$I_Q(C_G) \le c|Q| \cdot 2^{-w+1} \le c|Q| \cdot \frac{\log^2 n}{n}.$$

The last inequality follows since $v = c2^w \log n$ so $n = c2^w w \log n$ which implies that $2^w = cn/\log^2 n$. And by Lemma 18 and Fact 8, $|\mathbb{E}[C_G] - 1/2| \le n^{-1+o(1)}$. $\square$

Let us add a couple of remarks. First, one can improve the final circuit size to cn^2 through a different proof which avoids the sampler definition and argues directly about each subcircuit. However, we choose to present the current proof as it is simpler and more consistent with the explicit construction. Second, one can replace Lemma 18, the proof of which is somewhat involved, with a simpler argument due to [Wel20], at the cost of the monotonicity of the final nonexplicit circuit.

2.1 Proof of Lemma 19

For any $G : [u] \to [v]^w$ and $F = \sum_{k \in [w]} f_k$, where $f_1, \dots, f_w : [v] \to \{0, 1\}$, let $S_F(G) := \sum_{i \in [u]} 2^{F(G(i))} \mathbf{1}_{F(G(i)) \neq 0}$. By Fact 12, over a uniformly sampled $G : [u] \to [v]^w$ and any fixed F with mean $\mathbb{E}_{y \in [v]^w}[F(y)] = \mu < 1/2$ we have

$$\mathop{\mathbb{E}}_G [S_F(G)] \le u \cdot 4\mu.$$

By the above and Hoeffding's inequality, for any fixed F with mean $\mu = t/v$ we have

$$\mathbb{P}_G [S_F(G) - 4u\mu > 2u\mu] < exp\left(-\frac{2(2u\mu)^2}{u2^{2w}}\right) < exp\left(-\frac{8ut^2}{v^2 2^{2w}}\right) < v^{-8t^2}.$$

The last $<$ follows for $u \ge v^2 2^{2w} \ln v$. Now we union bound the probability of some bad F with mean t/v:

$$\mathbb{P}_G[\exists F : \mathbb{E}[F] = t/v \wedge S_F(G) > 6u\mu] < |\{F : \mathbb{E}[F] = t/v\}| \cdot v^{-8t^2} \le v^{-6t}.$$

The last $\le$ follows by the Vandermonde identity, which says there are $\sum_{\ell_1 + \cdots + \ell_w = t} \binom{v}{\ell_1} \dots \binom{v}{\ell_w} = \binom{vw}{t} \le (vw)^t$ functions F with mean t/v.

After a union bound over all possible $1 \le t \le v$, the probability of some bad F with mean ≤ 1 is at most $\sum_{t=1}^{\infty} v^{-6t} < 2v^{-6} < 1/2$.

Now we bound the probability that G is a $w/2$ design. For a fixed $z \in [v]^w$ and a uniformly sampled $y \sim [v]^w$, the probability y intersects z in more than $w/2$ elements is $\le (c/v)^{w/2}$. Thus by a union bound,

$$\mathbb{P}_G[\exists i' \neq i \in [u] \wedge j', j \in [v] : |S(G(i'), j') \cap S(G(i), j)| \ge w/2] \le (uv)^2 (c/v)^{w/2} < 1/2.$$

The last $<$ holds for w a large enough constant since $u = (vw)^4, w \le v$. Hence there is a $G : [u] \to [v]^w$ that is a sampler and $(w/2)$-design for $u \ge v^2 2^{2w} \ln v$. $\square$

3 Explicit tradeoff resilient circuits

In this section we we prove Lemma 16, restated below, which provides an explicit σ^{-1}-sampler and design. The bulk of the output of $G : [u] \to [v]^w$ will come from an expander walk, but a small subset of the output of size roughly $\log w$ will come from a constant-degree Reed-Solomon code.

To analyze the sampler property of G (Proposition 20) we apply Cauchy-Schwarz and use the known sampler properties of expander walks (Theorem 13) and Reed-Solomon codes (Proposition 22). However, there is a σ^{-1} factor loss from applying Cauchy-Schwarz.

G will be approximately a $c \log w$-design (Proposition 21) which simply follows from the design properties of the Reed-Solomon code.

Lemma. *Fix $w \le v$ where v is prime and $\sigma \in (0, 1/2]$ s.t. $\sigma^{-w} = \frac{Cv}{\log v}$ for a fixed constant C. Then there is an explicit $G : [u] \to [v]^w$ that is a $(\sigma^{-1}, \sigma^{-1})$-sampler and $4 \log\log u/\log(\sigma^{-1})$-design, where $u = \mathrm{poly}(v)$.*

3.1 Proof of Lemma 16

Fix $w \le v$ where v is prime and $\sigma \in (0, 1/2]$ so that $\sigma^{-w} = v/\ln(u/\ln 2)$ for u which we specify below.

It is well known there are explicit (v, d, λ) expanders with $d \le \lambda^{-c}$ for any explicit λ. For instance, one can take powers of constant degree expanders with constant expansion. Let W output walks of length $w_1 \le w$ on such an expander with $\lambda = \sigma^2/4$ for some w_1 we specify later. By Theorem 13, $W : [vd^{w_1}] \to [v]^w$ is a σ^{-2}-sampler. Note $vd^{w_1} = v^c$ since $d = \sigma^{-c}$ and $\sigma^{-w} \le v$.

Let $RS : [v]^{c_1} \to [v]^{w_2}$ denote the code from Fact 15 where c_1 is a constant large enough so that $v^{c_1} \ge vd^{w_1}$ and $w_2 := (c_1/3)\max(\lfloor \log \ln u/\log(\sigma^{-1})\rfloor, 4)$. Note $w_2 < w$ since $\sigma^{-w} = v/\ln(u/\ln 2)$ and $c_1 < w_2$.

Finally, we set $w_1 := w - w_2$ and $u := vd^{w_1}$ which implies $v/\ln(u/\ln 2) = (1 + o(1))Cv/\log v$ for some fixed constant C. We define $G : [u] \to [v]^w$ as follows:

$$\begin{cases} G(i)_k = W(i)_k & \text{if } 1 \le k \le w_1 \\ G(i)_k = RS(i)_{k-w_1} & \text{if } w_1 < k \le w. \end{cases}$$

Proposition 20. *G is a $(\sigma^{-1}, \sigma^{-1})$-sampler.*

Proof. Fix $f_1, \dots, f_w : [v] \to \{0, 1\}$ so that $\mu = \mathbb{E}[F] \le 1/(c\sigma^{-2} \ln u)$ where $F = \sum_{k\in[w]} f_k$. Let $F_1 = f_1 + \cdots + f_{w_1}$, $F_2 = f_{w_1+1} + \cdots + f_w$, $\mu_1 = \mathbb{E}[F_1], \mu_2 = \mathbb{E}[F_2]$ (so $\mu_1 + \mu_2 = \mu$). Then

$$\begin{aligned} \mathop{\mathbb{E}}_{i\in[u]}[\sigma^{-F(G(i))}] &= \mathop{\mathbb{E}}_{i\in[u]}[\sigma^{-F_1(W(i))}\sigma^{-F_2(RS(i))}] \\ &\le \mathop{\mathbb{E}}_{i\in[u]}[\sigma^{-2F_1(W(i))}]^{1/2} \mathop{\mathbb{E}}_{i'\in[u]}[\sigma^{-2F_2(RS(i'))}]^{1/2} \\ &\le e^{c\sigma^{-2}\mu_1} \cdot (e^{c\sigma^{-2}\mu_2} + \sigma^{-2w_2}\mu_2^{c_1})^{1/2}. \end{aligned}$$

The second $\leq$ follows by Cauchy-Schwarz. The last $\leq$ follows since W is a σ^{-2} sampler and by Proposition 22, stated at the end. To conclude it suffices to show

$$(\sigma^{-2w_2}\mu_2^{c_1})^{1/2} \leq \mu_2.$$

This follows as $\sigma^{-2w_2} \leq (\ln u)^{(2c_1/3)}$ and $\mu_2^{c_1} \leq \mu^{(2c_1/3)}\mu_2^{(c_1/3)} \leq (\ln u)^{-(2c_1/3)}\mu_2^{(c_1/3)}$. □

Proposition 21. *G is a $4\log\log u/\log(\sigma^{-1})$-design.*

Proof. Its clear that G is a $(w_2 - c_1)$-design, and note $w_2 - c_1 \geq (c_1/6)\cdot(\log\ln u/\log(\sigma^{-1})) \geq 4\log\log u/\log(\sigma^{-1})$ for c_1 large enough. □

3.2 Remaining proof

The following is a sampler like property of Reed-Solomon codes.

Proposition 22. *Let D be a ℓ-wise uniform distribution on $[v]^w$. Then for any $f_1, \ldots, f_w : [v] \to \{0,1\}$ s.t. $\mu := \mathbb{E}_{y\in[v]^w}[F(y)] \leq 1/2\alpha$ where $F = \sum_{k\in[w]} f_k$,*

$$\mathbb{E}[\alpha^{F(D)}] \leq e^{c\alpha\mu} + \alpha^w\mu^\ell.$$

Proof. Define the random variables $Y_1 = f_1(y_1), \ldots Y_w = f_w(y_w)$ where y is sampled from D and let $Y = \sum_{k\in[w]} Y_k$. Then

$$\mathbb{P}[Y \geq \ell] \leq \sum_{S\subseteq[w],|S|=\ell} \mathbb{P}\left[\prod_{i\in S} Y_i = 1\right] = \sum_{S\subseteq[w],|S|=\ell}\prod_{i\in S}\mathbb{P}[Y_i = 1] \leq \binom{w}{\ell}\left(\frac{\mu}{w}\right)^\ell \leq \mu^\ell.$$

The $=$ follows as D is ℓ-wise uniform. The next $\leq$ follows by Maclaurin's inequality. Since the above holds for any $k \leq \ell$, we have

$$\begin{aligned}
\mathbb{E}[\alpha^Y] &\leq \mathbb{E}[\alpha^Y|Y=0] + \sum_{k=1}^{\ell-1}\mathbb{E}[\alpha^Y|Y=k]\mathbb{P}[Y=k] + \mathbb{E}[\alpha^Y|Y\geq\ell]\mathbb{P}[Y\geq\ell] \\
&\leq 1 + \sum_{k=1}^{\ell-1}\alpha^k\mu^k + \alpha^w\mu^\ell \\
&\leq 1 + 2\alpha\mu + \alpha^w\mu^\ell.
\end{aligned}$$

The last $\leq$ follows since $\alpha\mu < 1/2$. We can now conclude since $1 + x \leq e^x$. □

4 Sampler to resilience

In this section we prove Lemma 17 which says that when G is a sampler, then the resulting circuit C_G will be resilient. To do so we bound the probability that each read-once subcircuit $C_{G(i)}$ will be fixed and then apply a union bound. Each subcircuit $C_{G(i)}$ is unlikely to be fixed since the coalition size is less than the number of independent AND_w terms in $C_{G(i)}$.

Lemma. *Fix integers $w \le v \le u$ and $\sigma \in (0, 1/2]$ so that $\sigma^{-w} = v/\ln(u/\ln 2)$ and suppose $G : [u] \to [v]^w$ is a (σ^{-1}, β)-sampler. Then for any $Q \subseteq [n]$ s.t. $|Q| \le c\sigma^{-w+1}/\beta$,*

$$I_{Q,B_\sigma}(C_G) \le |Q| \cdot \beta\sigma^{w-1}.$$

Proof. Fix a coalition $Q \subseteq [n]$ of size q. After sampling from B_σ the bits indexed by $\overline{Q}$, $C_{G(i)}$ is not fixed iff $E_i \wedge F_i = 1$ where

$$\begin{cases} E_i = 1 & \text{if } \forall j : S(G(i), j) \cap Q = \emptyset, A_{i,j}(x) = 0, \\ F_i = 1 & \text{if } \exists j : S(G(i), j) \cap Q \neq \emptyset, A_{i,j}(x) = ? \end{cases}$$

where $A_{i,j}(x) := \wedge_{k \in S(G(i),j)} x_k$. By $A_{i,j}(x) = ?$ we denote that the bits indexed by $S(G(i), j) \cap \overline{Q}$ are set to 1.

First we bound $\mathbb{P}[E_i]$. Since there are v AND_w terms in $C_{G(i)}$ and Q can intersect with $\le q$ of them we have

$$\mathbb{P}[E_i] \le (1 - \sigma^w)^{v-q} \le p \cdot e^{q\sigma^w} \le c/u.$$

since $v = c\sigma^{-w} \ln u$ and $q \le c\sigma^{-w}$.

Next we bound $\mathbb{P}[F_i]$ by union bounding over all intersecting j:

$$\mathbb{P}[F_i] \le \sum_{j \in [v]: S(G(i),j) \cap Q \neq 0} \sigma^{(w - |S(G(i),j) \cap Q|)} = \sigma^w \sum_{j \in [v]} \sigma^{-|S(G(i),j) \cap Q|} \mathbf{1}_{|S(G(i),j) \cap Q| \neq 0}.$$

Combining the bounds above we have

$$\begin{aligned} \sum_{i \in [u]} I_Q(C_{P_i}) &\le \sum_{i \in [u]} \mathbb{P}[E_i]\mathbb{P}[F_i] \\ &\le \frac{c}{u} \sigma^w \sum_{i \in [u]} \sum_{j \in [v]} \sigma^{-|S(G(i),j) \cap Q|} \mathbf{1}_{|S(G(i),j) \cap Q| \neq 0} \\ &= c\sigma^w \sum_{j \in [v]} \mathop{\mathbb{E}}_{i \in [u]} \sigma^{-|S(G(i),j) \cap Q|} \mathbf{1}_{|S(G(i),j) \cap Q| \neq 0}. \end{aligned}$$

To conclude we claim that for any fixed $j \in [v]$,

$$\mathop{\mathbb{E}}_{i \in [u]} \sigma^{-|S(G(i),j) \cap Q|} \mathbf{1}_{|S(G(i),j) \cap Q| \neq 0} \le \beta\sigma^{-1} q/v.$$

To see this, for each $k \in [w]$ define $f_k : [v] \to \{0, 1\}$ as

$$\begin{cases} f_k(y) = 1 & \text{if } \{((k-1)v + y + j) \bmod v\} \in Q; \\ f_k(y) = 0 & \text{if } \{((k-1)v + y + j) \bmod v\} \notin Q. \end{cases}$$

Note $|S(G(i), j) \cap Q| = F(G(i))$ and $\mathbb{E}_{y \in [v]^w}[F(y))] = q/v \le c\sigma^{-w+1}/(v\beta) \le 1/(\sigma^{-1}\beta \ln u)$ where $F = \sum_{k \in [w]} f_k$. The claim now follows since G is a (σ^{-1}, β) sampler. $\square$

5 Sampler and design to small bias

Here we prove Lemma 18, restated below.

Lemma. *Suppose $G : [u] \to [v]^w$ is a (σ^{-1}, β)-sampler and a d-design. Then*

$$|\mathbb{E}[C_G(B_\sigma)] - bias(u, v, w, \sigma)| \le e^{\sigma^d \cdot \log^4 u} \frac{\beta\sigma^{-1}}{n^{1-o(1)}}.$$

For this we will need two different approximations of the OR of boolean circuits. The first is the Bonferroni inequality.

Proposition 23. *For any boolean random variables $Z_1, \dots, Z_n$ and odd K, letting $Z := \vee_{i\in[n]} Z_i$ we have*

$$0 \le \mathbb{P}[Z] - \sum_{k\in[K-1]} (-1)^{k-1} S_k(Z_1, \dots, Z_n) \le S_K(Z_1, \dots, Z_n)$$

where $S_k(Z_1, \dots, Z_n) := \sum_{S\subseteq[n]:|S|=k} \mathbb{P}[\wedge_{i\in S} Z_i]$.

We also need the following slight tightening of Janson's inequality [Jan90]. The below version is implicit in the proof presented by [AS92] (c.f. [LSS+21]). We provide a justification in the appendix.

Proposition 24. *Let $C_1, \dots, C_n$ be arbitrary monotone boolean circuits such that $\mathbb{P}[C_i = 0] = p \ge 1/2$ $\forall i$ over some product distribution D. Then letting $C := \vee_{i\in[n]} C_i$ we have*

$$\prod_{i\in[n]} \mathbb{P}[C_i = 0] \le \mathbb{P}[C = 0] \le \prod_{i\in[n]} \mathbb{P}[C_i = 0] \cdot \left(1 + \sum_{\ell=1}^{n} \frac{2^\ell}{\ell!} \Delta(C)^\ell\right)$$

where the probabilities are over D and

$$\Delta(C) := \sum_{i\in[n]} L(C, i), \quad L(C, i) := \sum_{\substack{i'\in[n]:\\ i'<i,\\ i'\sim i}} \mathbb{P}[C_{i'} \wedge C_i]$$

where $i' \sim i$ denotes that $C_{i'}$ and C_i are not on disjoint variables.

The upper bound is usually stated as $\prod_{i\in[n]} \mathbb{P}[C_i = 0] \cdot e^{2\Delta(C)}$. If one used this bound, then in the course of proving Lemma 18 one needs to bound the quantity $\mathbb{E}_{T\subseteq[u]:|T|=k}\, e^{\Delta(C_{G(T)})} - 1$ for k not too large, where $C_{G(T)} := \vee_{i\in T} C_{G(i)}$. [CZ16, Mek17] do so by requiring design properties of G. If G is a d-design, then $\mathbb{E}_{T\subseteq[u]:|T|=k}\, e^{\Delta(C_{G(T)})} \le e^{\log^c u/2^d}$ (see Lemma 26), resulting in a final bias of approximately 2^{-d}. To achieve polynomial bias, one would need a Reed-Solomon code of length $c \log n$, which would ruin the sampler property.

Instead if one uses the above version of Janson's inequality, one needs to bound $\mathbb{E}_{T\subseteq[u]:|T|=k}\, \Delta(C_{G(T)})^\ell$ for $1 \le \ell \le n$. Through the sampler property of G, we prove $\mathbb{E}_{T\subseteq[u]:|T|=k}\, \Delta(C_{G(T)}) = n^{-1+o(1)}$ (Lemma 25). We then use Lemma 26 to bound the remaining terms $\mathbb{E} \sum \Delta(C_{G(T)})^\ell$. This analysis results in a final bias of $e^{\log^c u/2^d} n^{-1+o(1)} = n^{-1+o(1)}$ for d roughly $c \log\log n$.

Lemma 25. *Suppose $G : [u] \to [v]^w$ is a (σ^{-1}, β)-sampler. For any $1 \le k \le \log u$,*

$$\mathop{\mathbb{E}}_{\substack{T \subseteq [u]: \\ |T| = k}} \Delta(C_{G(T)}) \le \frac{\beta \sigma^{-1}}{v^{1-o(1)}}.$$

Lemma 26. *Suppose $G : [u] \to [v]^w$ is a d-design. For any $1 \le k \le \log u$,*

$$\max_{\substack{T \subseteq [u]: \\ |T| = k}} \Delta(C_{G(T)}) \le \log^4 u \cdot \sigma^d.$$

Assuming Lemmas 25 and 26 we can prove Lemma 18.

Proof of Lemma 18 . We can write $\neg C_G = \vee_{i \in [u]} Z_i$ where $Z_i := \neg C_{G(i)}$. We can also write $1 - bias(u, v, w, \sigma) = 1 - (1-p)^u$ where recall $p = (1 - \sigma^w)^v$. By Bonferroni's inequality, for any odd K which we set later we have

$$\left| \mathbb{E}[\neg C_G] - \sum_{k \in [K-1]} (-1)^{k-1} \mathbb{E}[S_k(Z_1, \dots, Z_u)] \right| \le |\mathbb{E}[S_K(Z_1, \dots, Z_u)|,$$

$$\left| (1 - bias(u, v, w, \sigma)) - \sum_{k \in [K-1]} (-1)^{k-1} \binom{u}{k} p^k \right| \le \binom{u}{K} p^K$$

where the expectations are over B_σ. Note that $\mathbb{E}[S_k(Z_1, \dots, Z_u)] = \sum_{T \subseteq [u]: |T| = k} \mathbb{P}[C_{G(T)} = 0]$, where $C_{G(T)} = \vee_{i \in T} C_{G(i)} = \vee_{i \in T} \vee_{j \in [v]} A_{i,j}$, and $A_{i,j} = \wedge_{k \in S(G(i),j)} x_k$. Thus we view $C_{G(T)}$ as an OR_{kv}-AND_w circuit. First note that by Lemmas 25, 26 we have

$$\mathop{\mathbb{E}}_{\substack{T \subseteq [u]: \\ |T| = k}} \Delta(C_{G(T)})^\ell \le \max_{\substack{T \subseteq [u]: \\ |T| = k}} \Delta(C_{G(T)})^{\ell - 1} \mathop{\mathbb{E}}_{\substack{T \subseteq [u]: \\ |T| = k}} \Delta(C_{G(T)}) \le (\log^4 u \cdot \sigma^d)^{\ell-1} \binom{u}{k} \frac{\beta \sigma^{-1}}{v^{1-o(1)}}.$$

Combining this with Proposition 24 we have

$$\begin{aligned}
\binom{u}{k} p^k \le \mathbb{E}[S_k(Z_1, \dots, Z_u)] &\le p^k \sum_{T \subseteq [u]: |T| = k} (1 + \sum_{\ell=1}^{kv} \frac{2^\ell}{\ell!} \Delta(C_{G(T)})^\ell) \\
&\le \binom{u}{k} p^k (1 + \frac{\beta \sigma^{-1}}{v^{1-o(1)}} \sum_{\ell=1}^{kv} \frac{2^\ell}{\ell!} (\log^4 u \cdot \sigma^d)^{\ell-1}) \\
&\le \binom{u}{k} p^k (1 + \frac{\beta \sigma^{-1}}{v^{1-o(1)}} e^{\log^4 u \cdot \sigma^d}).
\end{aligned}$$

The last inequality follows since $\sum_{\ell=0}^\infty x^\ell / \ell! = e^x$. If the $Z_1, \dots, Z_u$ were independent then of course $\mathbb{E}[S_k(Z_1, \dots, Z_u)] = \binom{u}{k} p^k$. So the above is saying that when G is a sampler, the resulting Z_i behave as if they were independent up to a small multiplicative error.

After repeated applications of the triangle inequality, letting $\delta = \frac{\beta\sigma^{-1}}{v^{1-o(1)}} e^{\log^4 u \cdot \sigma^d}$, we have

$$
\begin{aligned}
|\mathbb{E}[C_G] - bias(u, v, w, \sigma)| &\le \delta \sum_{k=1}^{K-1} \binom{u}{k} p^k + (2+\delta)\binom{u}{K} p^K \\
&\le \delta(1+p)^u + (c/K)^K \\
&\le c\delta.
\end{aligned}
$$

The last inequality follows since $p = c/u$ and by setting $K = c \log v / \log\log v$. $\square$

5.1 Proof of Lemmas 25, 26

Fix any $T \subseteq [u] : |T| = k$ and define $Y(i', j', i, j) := \sigma^{-|S(G(i'),j') \cap S(G(i),j)|} \mathbf{1}_{|S(G(i'),j') \cap S(G(i),j)| \neq 0}$. By definition we have

$$
\begin{aligned}
\Delta(C_{G(T)}) &= \sum_{(i,j) \in T \times [v]} L(C_{G(T)}, (i, j)) \\
&= \sum_{(i,j) \in T \times [v]} \sum_{\substack{(i',j') \in T \times [v]: \\ (i',j') < (i,j), \\ (i',j') \sim (i,j)}} \mathbb{P}[A_{i',j'} \wedge A_{i,j}] \\
&= \sigma^{2w} \sum_{(i,j) \in T \times [v]} \sum_{\substack{(i',j') \in T \times [v]: \\ (i',j') < (i,j)}} Y(i', j', i, j)
\end{aligned}
$$

The last equality follows as $\mathbb{P}[A_{i',j'} \wedge A_{i,j}] = \sigma^{2w - |S(G(i'),j') \cap S(G(i),j)|}$ and $\mathbf{1}_{(i',j') \sim (i,j)} = \mathbf{1}_{|S(G(i'),j') \cap S(G(i),j)| \neq 0}$. One can think of (i, j) as a number, with i as the most significant bit.

To prove Lemma 26, since G is a d-design, for any fixed $i \neq i' \in T$ and $j \in [v]$ we have

$$
\sum_{\substack{j' \in [v]: \\ (i',j') < (i,j)}} Y(i', j', i, j) \le w\sigma^{-(w-d)}.
$$

Thus $\Delta(C_{G(T)}) \le \sigma^{2w} \cdot k^2 v \cdot w\sigma^{-(w-d)} \le \sigma^d \cdot k^2 \ln u \cdot w \le \sigma^d \ln^4 u$. The second inequality follows since $v = c\sigma^{-w} \ln u$.

Now we prove Lemma 25. We need the following result.

Proposition 27. *Suppose $G : [u] \to [v]^w$ is a (σ^{-1}, β)-sampler. For any $1 \le k \le u$ and $j', j \in [v]$,*

$$
\mathop{\mathbb{E}}_{\substack{T \subseteq [u]: \\ |T| = k}} \sum_{\substack{i', i \in T: \\ i' < i}} Y(i', j', i, j) \le \binom{u}{k} k^2 \frac{\beta\sigma^{-1}}{v^{1-o(1)}}.
$$

Assuming Proposition 27, we can prove Lemma 25.

$$\begin{aligned}
\mathop{\mathbb{E}}_{\substack{T\subseteq[u]:\\|T|=k}} \Delta(C_{G(T)}) &\leq \sigma^{2w} \mathop{\mathbb{E}}_{\substack{T\subseteq[u]:\\|T|=k}} \sum_{(i,j)\in T\times[v]} \sum_{\substack{(i',j')\in T\times[v]:\\(i',j')<(i,j)}} Y(i',j',i,j) \\
&= (\frac{c\ln u}{v})^2 \sum_{j',j\in[v]} \mathop{\mathbb{E}}_{\substack{T\subseteq[u]:\\|T|=k}} \sum_{\substack{i',i\in T:\\i'<i}} Y(i',j',i,j) \\
&\leq (\frac{c\ln u}{v})^2 \cdot v^2 k^2 \frac{\beta\sigma^{-1}}{v^{1-o(1)}} \\
&\leq \frac{\beta\sigma^{-1}}{v^{1-o(1)}}.
\end{aligned}$$

5.2 Proof of Proposition 27

Proposition 27 directly follows from the next two results.

Proposition 28. *For any $j',j\in[v]$, $i\in[u]$. $\mathbb{E}_{i'\in[u]} Y(i',j',i,j) \leq c\beta\sigma^{-1}\frac{w}{v}$.*

Proof. We can write

$$Y(i',j',i,j) = \sigma^{-F(G(i))}\mathbf{1}_{F(G(i))\neq 0}$$

where $F = \sum_{k\in[w]} f_k$ and for each $k\in[w]$, $f_k : [v] \to \{0,1\}$ is defined as follows:

$$\begin{cases} f_k(y) = 1 & \text{if } y + j = G(i')_k + j' \bmod v; \\ f_k(y) = 0 & \text{otherwise.} \end{cases}$$

Note $\mathbb{E}[F] = w/v$. We can conclude since G is a (σ^{-1},β) sampler. □

Proposition 29. *Fix $1\leq k\leq u$ and non-negative $X : [u]\times[u]\to\mathbb{R}$ s.t. for any $i\in[u]$, $\mathbb{E}_{i'\in[u]} X(i',i)\leq\mu$. Then*

$$\mathop{\mathbb{E}}_{\substack{T\subseteq[u]:\\|T|=k}} \sum_{\substack{i',i\in T:\\i'<i}} X(i',i) \leq ck^2\mu\cdot$$

Proof. We have

$$\mathop{\mathbb{E}}_{\substack{T\subseteq[u]:\\|T|=k}} \sum_{\substack{i',i\in T:\\i'<i}} X(i',i) = \binom{u}{k}^{-1}\binom{u-2}{k-2} \sum_{\substack{i',i\in[u]:\\i'<i}} X(i',i) \leq \binom{u}{k}^{-1}\binom{u-2}{k-2} u^2\mu \leq ck^2\mu.$$

□

Remark 30. *The condition $i'<i$ is necessary. Suppose $X(i',i) = u\mu$ for $i'=i$ and 0 otherwise. Then*

$$\mathop{\mathbb{E}}_{\substack{T\subseteq[u]:\\|T|=k}} \sum_{i',i\in T} X(i',i) = ku\mu\cdot$$

6 Balanced circuits matching KKL

In this section we prove Theorem 5. We need the following result due to Ajtai and Linial [AL93], the proof of which we give at the end.

Lemma 31. *Let $C_1, C_2 : \{0,1\}^n \to \{0,1\}$ be depth d circuits such that $|\mathbb{E}[C_1] - 1/2| < \epsilon_1$, $\mathbb{E}[C_2] < (1 - 2\epsilon_1)$. Then there is a depth $d+2$ circuit $C' : \{0,1\}^{2n} \to \{0,1\}$ such that $\mathbb{E}[C'] = 1/2$ and $I_Q(C') \leq I_Q(C_1) + I_Q(C_2) + \mathbb{P}[C_2 = 0]$ for any $Q \subseteq [2n]$. Moreover, if C_1, C_2 are explicit then C' is explicit.*

Proof of Theorem 5. Let C_1, C_2 be read-once OR_v-AND_w, $OR_{v'}$-$AND_{w'}$ circuits where $vw, v'w' = cn$. First we set w, v so that $v = \lceil 2^w \ln 2 \rceil$. Thus by the inequality $e^{-x/(1-x)} \leq 1 - x \leq e^{-x}$,

$$|\mathbb{E}[C_1] - 1/2| \leq \frac{c_1 \log n}{n}$$

for some fixed c_1. Similarly, we set w', v' so that $v' = \lceil 2^{w'} \ln \left(\frac{n}{3c_1 \log n}\right) \rceil, w'$ which implies

$$\left| \mathbb{E}[C_2] - \left(1 - \frac{3c_1 \log n}{n}\right) \right| \leq \frac{c \log^3}{n^2}.$$

Now for any $Q_1, Q_2 \subseteq [n] : |Q_1| = |Q_2| = 1$ we have

$$I_{Q_1}(C_1) \leq \frac{c \log n}{n},$$

$$I_{Q_2}(C_2) = (1 - 2^{-w'})^{v'-1} 2^{-(w'-1)} \leq \frac{c \log n}{n} \cdot \frac{\log^2 n}{n} = \frac{c \log^3 n}{n^2}.$$

We conclude by Lemma 31. $\square$

6.1 Proof of Lemma 31

Let $\delta = \mathbb{E}[C_1] - 1/2$ and define μ so that $\mathbb{E}[C_2] = 1 - \mu$. We define

$$C'(x, y) := (C_1(x) \wedge C_2(y)) \vee (D(x) \wedge \neg C_2(y))$$

where $D(x) : \{0,1\}^n \to \{0,1\}$ is an explicit DNF with $\mathbb{E}[D] = \frac{1}{2} + \delta - \frac{\delta}{\mu} \in [0,1]$. The $\in$ follows since $\mu > 2|\delta|$ by hypothesis. We justify such a D in the end. Now,

$$\mathbb{E}[C'(x, y)] = (1/2 + \delta)(1 - \mu) + \mathbb{E}[D(x)] \cdot \mu = 1/2.$$

For any $Q \subseteq [2n]$, letting Q_1, Q_2 denote the sets in x, y respectively, by a union bound we have $I_Q(C') \leq I_{Q_1}(C_1) + I_{Q_2}(C_2) + \mathbb{P}[C_2 = 0]$.

To conclude, it remains to construct an explicit DNF D such that $\mathbb{E}[D] = 2^{-n} \cdot k$ for any $k \in [2^n]$. Let us write the binary representation of k as $\alpha_1 2^{n-1} + \cdots + \alpha_n 2^0$ where $\alpha_i \in \{0,1\}$. We construct f by adding the term $\neg x_1 \ldots \neg x_{i-1} x_i$ if $\alpha_i = 1$. The term $\neg x_1 \ldots \neg x_{i-1} x_i$ has 2^{n-i} inputs in its support. Furthermore, each term will be disjoint. Hence f attains the desired bias. $\square$

Acknowledgments We are grateful to Raghu Meka for helpful discussions, providing clarifications on [Mek17], and suggesting the use of tail bounds for expander walks.

References

[AL93] Miklos Ajtai and Nathan Linial. The influence of large coalitions. *Combinatorica*, 13:129–145, 1993.

[AS92] Noga Alon and Joel H. Spencer. *The Probabilistic Method*. Wiley-Interscience Series in Discrete Mathematics and Optimization. John Wiley and Sons, Inc., 1992.

[BL85] Michael Ben-Or and Nathan Linial. Collective coin flipping, robust voting schemes and minima of Banzhaf values. In *26th Symposium on Foundations of Computer Science*, pages 408–416, Portland, Oregon, 21–23 October 1985. IEEE.

[CHH+20] Eshan Chattopadhyay, Pooya Hatami, Kaave Hosseini, Shachar Lovett, and David Zuckerman. XOR lemmas for resilient functions against polynomials. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *ACM Symp. on the Theory of Computing (STOC)*, pages 234–246. ACM, 2020.

[CL16] Kuan Cheng and Xin Li. Randomness extraction in AC0 and with small locality. *CoRR*, abs/1602.01530, 2016.

[CZ16] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. In *ACM Symp. on the Theory of Computing (STOC)*, pages 670–683, 2016.

[EG20] Ronen Eldan and Renan Gross. Concentration on the boolean hypercube via pathwise stochastic analysis. In Konstantin Makarychev, Yury Makarychev, Madhur Tulsiani, Gautam Kamath, and Julia Chuzhoy, editors, *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2020, Chicago, IL, USA, June 22-26, 2020*, pages 208–221. ACM, 2020.

[EKLM22] Ronen Eldan, Guy Kindler, Noam Lifshitz, and Dor Minzer. Isoperimetric inequalities made simpler. *CoRR*, abs/2204.06686, 2022.

[FHH+19] Yuval Filmus, Lianna Hambardzumyan, Hamed Hatami, Pooya Hatami, and David Zuckerman. Biasing boolean functions and collective coin-flipping protocols over arbitrary product distributions. In Christel Baier, Ioannis Chatzigiannakis, Paola Flocchini, and Stefano Leonardi, editors, *46th International Colloquium on Automata, Languages, and Programming, ICALP 2019, July 9-12, 2019, Patras, Greece*, volume 132 of *LIPIcs*, pages 58:1–58:13. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019.

[GVW15] Oded Goldreich, Emanuele Viola, and Avi Wigderson. On randomness extraction in AC0. In *IEEE Conf. on Computational Complexity (CCC)*, 2015.

[HIV22] Xuangui Huang, Peter Ivanov, and Emanuele Viola. Affine Extractors and AC0-Parity. In Amit Chakrabarti and Chaitanya Swamy, editors, *Approximation,* *Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2022)*, volume 245 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 9:1–9:14, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[IMV23] Peter Ivanov, Raghu Meka, and Emanuele Viola. Efficient resilient functions. In Nikhil Bansal and Viswanath Nagarajan, editors, *Proceedings of the 2023 ACM-SIAM Symposium on Discrete Algorithms, SODA 2023, Florence, Italy, January 22-25, 2023*, pages 2867–2874. SIAM, 2023.

[Jan90] Svante Janson. Poisson approximation for large deviations. *Random Structures & Algorithms*, 1(2):221–229, 1990.

[KKL88] Jeff Kahn, Gil Kalai, and Nathan Linial. The influence of variables on Boolean functions. In *29th IEEE Symp. on Foundations of Computer Science (FOCS)*, pages 68–80, 1988.

[KZ07] Jesse Kamp and David Zuckerman. Deterministic extractors for bit-fixing sources and exposure-resilient cryptography. *SIAM J. Comput.*, 36(5):1231–1247, 2007.

[Lez98] Pascal Lezaud. Chernoff-type bound for finite Markov chains. *The Annals of Applied Probability*, 8(3):849 – 867, 1998.

[LSS+21] Nutan Limaye, Karteek Sreenivasaiah, Srikanth Srinivasan, Utkarsh Tripathi, and S. Venkitesh. A fixed-depth size-hierarchy theorem for $AC^0[\oplus]$ via the coin problem. *SIAM journal on computing*, 50(4):1461–1499, 2021.

[Mek17] Raghu Meka. Explicit resilient functions matching ajtai-linial. In *ACM-SIAM Symp. on Discrete Algorithms (SODA)*, pages 1132–1148, 2017.

[RR17] Shravas Rao and Oded Regev. A sharp tail bound for the expander random sampler. *CoRR*, abs/1703.10205, 2017.

[RZ98] A. Russell and D. Zuckerman. Perfect information leader election in log*n+o(1) rounds. In *Proceedings 39th Annual Symposium on Foundations of Computer Science*, pages 576–583, 1998.

[Wag08] Roy Wagner. Tail estimates for sums of variables sampled by a random walk. *Comb. Probab. Comput.*, 17(2):307–316, mar 2008.

[Wel20] Jake Wellens. *Assorted results in boolean function complexity, uniform sampling and clique partitions of graphs.* PhD thesis, Massachusetts Institute of Technology, 2020.

7 Deferred proofs

7.1 Proof of Fact 8

We use the inequalities $e^{-x(1+cx)} \le e^{-\frac{x}{1-x}} \le 1-x \le e^{-x}$ for $x \in (0,1)$, and $e^x \le 1+2x$ for $x \le 1$. First we lower bound $bias(u,v,w,\sigma)$. We have

$$(1-\sigma^w)^v \le e^{-v\sigma^w} \le \ln 2/u.$$

Thus

$$bias(u,v,w,\sigma) \geq (1-\ln 2/u)^u \geq e^{-\ln 2(1+c/u)} \geq 1/2 - c/u.$$

To upper bound $bias(u,v,w,\sigma)$, note

$$(1-\sigma^w)^v \geq e^{-\sigma^w v(1+c\sigma^w)} \geq e^{-(\ln(u/\ln 2)+\sigma^w)(1+c\sigma^w)} \geq (\ln 2/u)(1-c\sigma^w).$$

Thus

$$bias(u,v,w,\sigma) \leq (1-(\ln 2/u)(1-c\sigma^w))^u \leq e^{-\ln 2(1-c\sigma^w)} \leq 1/2 + c\sigma^w.$$

From here we can conclude since $u^{-1} \leq v^{-1} \leq \sigma^w$.

7.2 Proof of Claim 10

First suppose $\mathbb{E}_{i\in[u]}[\alpha^{F(G(i))}] \leq e^{c\beta\alpha\mu} \leq 1 + c\beta\alpha\mu$. The last $\leq$ follows since $e^x \leq 1+2x$ for $x \in [0,1]$. Next, note that

$$\mathop{\mathbb{E}}_{i\in[u]}[\alpha^{F(G(i))}\mathbf{1}_{F(G(i))\neq 0}] = \mathop{\mathbb{E}}_{i\in[u]}[\alpha^{F(G(i))}] - \mathbb{P}_{i\in[u]}[F(G(i))=0].$$

By Markov's inequality, $\mathbb{P}[F(G(i))=0] = 1-\mathbb{P}[F(G(i))\geq 1] \geq 1-\mathbb{E}[F(G(i))] \geq 1-c\beta\alpha\mu$. The last inequality follows by Jensen's inequality.

Now suppose $\mathbb{E}_{i\in[u]}[\alpha^{F(G(i))}\mathbf{1}_{F(G(i))\neq 0}] \leq c\beta\alpha\mu$. Then since $1+x \leq e^x$, $\mathbb{E}_{i\in[u]}[\alpha^{F(G(i))}] \leq 1 + c\beta\alpha\mu \leq e^{c\beta\alpha\mu}$.

7.3 Proof of Fact 12

For the first inequality, let $\mu_k := \mathbb{E}[f_k]$ for each $k \in [w]$. Since $1+x \leq e^x$,

$$\mathbb{E}[\alpha^X] = \prod_{k\in[w]} \mathbb{E}[\alpha^{X_k}] = \prod_{k\in[w]} (1+(\alpha-1)\mu_k) \leq \prod_{k\in[w]} e^{(\alpha-1)\mu_k} = e^{(\alpha-1)\mu}.$$

The second inequality follows by similar reasoning as in the proof of Claim 10.

7.4 Proof of Proposition 24

The statement follows by repeating the proof in [AS92] (c.f. [LSS$^+$21]) and avoiding the inequality $1+x \leq e^x$ in the end. We follow the presentation of [LSS$^+$21] up until equation (A.4), stated next. The probabilities below are over D, and recall $L(C,i) = \sum_{i'\in[n]:i'<i,i'\sim i} \mathbb{P}[C_{i'} \wedge C_i], \Delta(C) = \sum_{i\in[n]} L(C,i)$.

$$\mathbb{P}[C=0] \leq \prod_{i\in[n]} \Big(\mathbb{P}[C_i=0](1+2L(C,i))\Big).$$

Then by the AM-GM inequality,

$$\prod_{i\in[n]}(1+2L(C,i)) \leq \left(1+\frac{2\Delta(C)}{n}\right)^n \leq 1 + \sum_{\ell=1}^{n} \frac{2^\ell}{\ell!}\Delta(C)^\ell.$$