Electronic Colloquium on Computational Complexity, Report No. 144 (2015)

Explicit resilient functions matching Ajtai-Linial

Raghu Meka
Department of Computer Science
University of California, Los Angeles

Abstract

A Boolean function on n variables is q-resilient if for any subset of at most q variables, the function is very likely to be determined by a uniformly random assignment to the remaining $n-q$ variables; in other words, no coalition of at most q variables has significant influence on the function. Resilient functions have been extensively studied with a variety of applications in cryptography, distributed computing, and pseudorandomness. The best known resilient function on n variables due to Ajtai and Linial [AL93] has the property that only sets of size $\Omega(n/(\log^2 n))$ can have influence bounded away from zero. However, the construction of Ajtai and Linial is by the probabilistic method and does not give an efficiently computable function.

In this work we give an explicit monotone depth three almost-balanced Boolean function on n bits that is $\Omega(n/(\log^2 n))$-resilient matching the work of Ajtai and Linial. The best previous explicit constructions of Meka [Mek09] (which only gives a logarithmic depth function), and Chattopadhyay and Zuckerman [CZ15] were only $(n^{1-\beta})$-resilient for any constant $0 < \beta < 1$. Our construction and analysis are motivated by (and simplifies parts of) the recent breakthrough of [CZ15] giving explicit two-sources extractors for polylogarithmic min-entropy; a key ingredient in their result was the construction of explicit constant-depth resilient functions.

An important ingredient in our construction is a new randomness optimal oblivious sampler which preserves moment generating functions of sums of variables and could be useful elsewhere.

1 Introduction

In this work we study *resilient functions* introduced by Ben-Or and Linial [BL85] in the context of collective-coin flipping. Consider the following game: There are n players who communicate by broadcast and want to agree on a random coin-toss. If all the players are honest, this is trivial: pick a player, have the player toss a coin and use the resulting value as the collective coin-toss. Now suppose that there are a few *bad* players who are computationally unbounded, can collude amongst themselves, and broadcast last in each round, i.e., they broadcast after observing the bits broadcast by the good players in each round. The problem of *collective coin-flipping* is to design protocols so that the bad players cannot bias the collective-coin too much. An important and well-studied special-case of protocols are *one-round* collective coin-flipping protocols. We will adopt the notation of boolean functions instead of protocols, as both are equivalent for a single round.

Definition 1.1. *For a Boolean function $f : \{0,1\}^n \to \{0,1\}$, and $Q \subseteq [n]$, let $I_Q(f)$ be the probability that f is not-determined by a uniformly random partial assignment to the bits not in Q. Let $I_q(f) = \min_{Q\subseteq[n],|Q|\leq q} I_Q(f)$. We say the function f is q-resilient if $\Pr_{x\in_u\{0,1\}^n}[f(x) = 1] = 1/2 \pm 1/10$ and $I_{\varepsilon q}(f) \leq O(\varepsilon)$.*[1]

[1]The choice of constants here is arbitrary, and one can work with any constants where $I_q(f) \ll \min(\Pr_{x\in_u\{0,1\}^n}[f(x) = 1], \Pr_{x\in_u\{0,1\}^n}[f(x) = 0])$.

ISSN 1433-8092

Intuitively, $I_q(f)$ quantifies the amount of influence any set of q variables can exert on the evaluation of the function f. If f is almost-balanced and $I_q(f)$ is small, say $o(1)$, then evaluating f gives a one-round coin-flipping protocol that outputs a nearly unbiased bit even in the presence of up to q bad players. While we focus here on one-round coin flipping protocols, the general model with multiple rounds has been extensively studied as well: [BL85, KKL88, Sak89, AN93, BN00, RZ01, Fei99, RSZ02]; more information and discussion of other models can be found in the survey of Dodis [Dod06].

In their work introducing the problem, Ben-Or and Linial gave an explicit n^α-resilient function for $\alpha = \log_3 2 = 0.63...$. Subsequently, the seminal work of Kahn, Kalai, and Linial [KKL88] showed that for any function f, $I_q(f) = 1 - o(1)$ for $q = \omega(n/\log n)$. Following this, Ajtai and Linial [AL93] showed the *existence* of a $\Omega(n/(\log^2 n))$-resilient function; this remains the best bound known to date. However, the construction in Ajtai and Linial is probabilistic and does not lead to an efficiently computable resilient function or one-round coin-flipping protocol. The goal of this work is to given an explicit Boolean function matching the existential result of Ajtai and Linial:

Theorem 1.2. *For some universal constant $c' \geq 1$ the following holds. There exists an explicit depth three monotone function $f : \{0,1\}^n \to \{0,1\}$ which can be computed in time $n^{c'}$ such that*[2]

- *f is almost balanced:* $\Pr_{x \in_u \{0,1\}^n}[f(x) = 1] = 1/2 \pm 1/10$.
- *f has small influences: $I_q(f) \leq c' q(\log^2 n)/n$; that is, f is $\Omega(n/(\log^2 n))$-resilient.*

The existential guarantee of [AL93] is slightly stronger than the above in that they show the existence of a constant-depth function as above with bias $1/2 \pm o(1)$; however, their function is not monotone[3]. Our result essentially matches theirs while being explicit.

Applications of resilient functions Th present work builds on a recent breakthrough of Chattopadhyay and Zuckerman [CZ15] who gave an explicit *two-source extractor* for poly-logarithmic *min-entropy* sources—resolving a longstanding problem in pseudorandomness. One of the main building blocks of their work is an explicit resilient function computable in small-depth: they reduce[4] the problem of building two-source extractors to that of constructing a $n^{1-\delta}$-resilient function computable by a monotone constant-depth circuit for some constant $\delta > 0$ and then construct such a function. Indeed, while a prior unpublished work of [Mek09] gave an explicit $n^{1-o(1)}$-resilient function, the construction of [Mek09] does not seem useful in the context of two-source extractors as it is does not give a constant-depth function.

The importance of depth comes from the fact that if f is q-resilient and small-depth, then it also remains resilient in the setting where the bits of the good players only have limited independence instead of being truly independent. Let us formalize this next.

Definition 1.3. *For a Boolean function $f : \{0,1\}^n \to \{0,1\}$, $Q \subseteq [n]$, and a distribution $\mathcal{D}$ on $\{0,1\}^{[n]\setminus Q}$, let $I_{Q,\mathcal{D}}(f)$ be the probability that f is not-determined by setting the bits not in Q according to $\mathcal{D}$. Let $I_{q,t}(f) = \min\{I_{Q,\mathcal{D}}(f) : Q \subseteq [n], |Q| \leq q, \ \ \mathcal{D}$ is t-wise independent$\}$.*

By combining Theorem 1.2 with Braverman's result [Bra10] that polylog-wise independence fools constant-depth functions, we get an analogous bound on $I_{q,t}(f)$ for $t \gg (\log n)^{12}$. This can be improved by applying the results of [KLW10] on *read-k DNFs* directly to the function we study leading to the following corollary (our function is nicer than general depth three circuits).

Corollary 1.4. *For some universal constants $c' \geq 1$ the following holds. There exists an explicit depth three monotone function $f : \{0,1\}^n \to \{0,1\}$ which can be computed in time $n^{c'}$ such that for $t \geq c'(\log n)^2$*

[2] Henceforth, for a multi-set S, $x \in_u S$ denotes a uniformly random element of S.
[3] While it is possible to make their construction monotone, this blows up the depth.
[4] The reduction is also implicit in [Li15].

- *f is almost balanced: for any t-wise independent distribution $\mathcal{D}$ on $\{0,1\}^n$, $\Pr_{x\leftarrow\mathcal{D}}[f(x) = 1] = 1/2 \pm 1/9$.*
- *f has small influences: $I_{q,t}(f) \le c'q(\log^2 n)/n$.*

In fact, we can also use our arguments to slightly simplify the construction and analysis of [CZ15] to get polynomially resilient functions—$(n^{1-\delta})$-resilient for any $\delta > 0$—from Reed-Solomon codes (see Corollary 6.4). This also leads to slightly better parameters: [CZ15] give a two-source extractor when the sources have min-entropy at least $C(\log n)^{74}$. Using Corollary 1.4 in their reduction gives a two-source extractor with constant-error for sources with min-entropy at least $C(\log n)^{10}$ and using Corollary 6.4 gives a two-source extractor with polynomially-small error for sources with min-entropy at least $C(\log n)^{18}$. We do not delve into this here.

Oblivious samplers preserving moment generating functions An important ingredient in our proof of Theorem 1.2 is an explicit *oblivious sampler* with optimal—up to constant factors—seed-length that approximates *moment generating functions*. We state this result next which may be of independent interest.

Theorem 1.5. *For all $0 < \gamma < 1$, $1 \le v, w$, there exists an explicit generator $G : \{0,1\}^r \to [v]^w$ such that for all functions $f_1, \ldots, f_w : [v] \to [0,1]$ with $\sum_{i=1}^w \mathbb{E}_{x\in_u[v]}[f_i(x)] = \mu \le 1$,*

$$\mathop{\mathbb{E}}_{y\in_u\{0,1\}^r}\left[2^{\sum_{i=1}^w f_i(G(y)_i)}\right] = 1 + O(\mu) + \gamma.$$

The seed-length of the generator is $r = O(w + (\log v) + \log(1/\gamma) + w(\log\log v)/(\log w))$.

We state a more precise version which works for estimating $\mathbb{E}\left[\rho^{\sum_i f_i(\,)}\right]$ for all $\rho \ge 1$ in Section 5 (as in a moment generating function); here we focus on the above for simplicity and as it suffices for our applications.

All previously known generators with a guarantee as above required a seed-length of $\Omega(\log v + w\log w)$; this can be obtained for instance by using an *expander sampler* on a graph of size v with eigenvalue gap $\ll 1/w$ [Gil98, Kah97, Hea08] or the Nisan or Impagliazzo, Nisan, and Wigderson [Nis92, INW94] pseudorandom generators (PRGs) for small-space machines. The improvement from $O(w\log w)$ to $O(w)$ is crucial in our application as we have to enumerate over all seed-lengths translating to an improvement from super-polynomial ($n^{O(\log\log n)}$) to polynomial running time.

The generator is obtained by instantiating the Nisan-Zuckerman [NZ96] PRG for small-space machines with k-wise independent seeds being fed into the *extractor* rather than truly independent ones. Concretely, let $E : [v^c]\times[D] \to [v]$ be a $(c(\log v)/2, \varepsilon)$-extractor (see Section 2 for formal definitions) with $\varepsilon = 1/w$. For $\ell = \Theta(w/(\log w))$, let $G_\ell : [D]^\ell \to [D]^w$ generate a ℓ-wise independent distribution. Then, our generator satisfying Theorem 1.5, $G : [v^c]\times[D]^\ell \to [v]^w$ is defined as follows:

$$G(x,y) = \left(E(x, G_\ell(y)_1), E(x, G_\ell(y)_2), \cdots, E(x, G_\ell(y)_w)\right). \tag{1.1}$$

While the above construction serves as the base, in our proof of Theorem 1.2, we need a generator that satisfies certain additional constraints: output strings on different seeds should be far from each other. We satisfy these constraints by careful modifications of the above construction.

1.1 Overview of construction: ANDs of Tribes

We next give a high level overview of our main construction and analysis. First, some notations:

- Throughout, by a partition P of $[n]$ we mean a division of $[n]$ into w-sized blocks $P_1, \ldots, P_v$, where $v = n/w$ (we assume w divides n).

- Let $\mathcal{D}_p$ denote the product distribution on $\{0,1\}^n$ where each bit is p-biased.

As in [AL93] and [CZ15] our construction will be an *AND* of several *Tribe* functions:

Definition 1.6. *For a partition $P = \{P_1, \ldots, P_v\}$ of $[n]$ into w-sized blocks, the associated* Tribes *function is defined by $T_P = \vee_{j=1}^{v} \left(\wedge_{\ell \in P_j} x_\ell\right)$. A collection of partitions $\mathcal{P} = \{P^1, \ldots, P^u\}$ defines a function $f \equiv f_{\mathcal{P}} : \{0,1\}^n \to \{0,1\}$ as follows:*

$$f_{\mathcal{P}}(x) := \bigwedge_{i=1}^{u} \bigvee_{j=1}^{v} \left(\bigwedge_{k \in P_j^i} x_k \right) = \bigwedge_{i=1}^{u} T_{P^i}(x).$$

The final function satisfying Theorem 1.2 will be $f_{\mathcal{P}}$ for a suitably chosen set of partitions. To analyze such functions, we first state two abstract properties of the partitions that allow us to analyze the bias as well as influences of such functions. Once we have these conditions, we will design partitions that satisfy these properties.

Analyzing bias We first specify some sufficient conditions for a collection of partitions $\mathcal{P} = \{P^1, \ldots, P^u\}$ that guarantee an explicit formula for the bias of the function $f_{\mathcal{P}}$.

Definition 1.7. *Let $\mathcal{P} = \{P^1, \ldots, P^u\}$ be a collection of partitions of $[n]$ into w-sized blocks. We say $\mathcal{P}$ is a (d, k, δ)-design if the following hold:*

- *For all $\alpha \neq \beta \in [u]$, and $i, j \in [v]$, $|P^\alpha(i) \cap P^\beta(j)| \leq w - d$.*
- *For $\alpha \in [u]$, and $i, j \in [v]$,*

$$\Pr_{\beta \in_u [u]} \left[|P_i^\alpha \cap P_j^\beta| \geq k \right] \leq \delta.$$

Intuitively, the first condition says that any two blocks arising in our partitions differ in at least d elements (i.e., do not overlap completely); in contrast, the second condition roughly says that most blocks in fact differ in at least $w - k$ elements (i.e, have very little overlap). When $\mathcal{P}$ satisfies the above condition, the following claim gives a formula for the bias of $f_{\mathcal{P}}$. We state the result for general p-biased distributions as the statement and its analysis are no more complicated.

Theorem 1.8. *Let $\mathcal{P} = \{P^1, \ldots, P^u\}$ be a collection of partitions of $[n]$ into w-sized blocks that is a (d, k, δ)-design for some $d \leq w/2$. Let $0 \leq p \leq 1$ with $v \geq p^{-w}$ and $\theta = (1 - p^w)^v$. Then, for all even integers $r \leq u$,*

$$\Pr_{x \leftarrow \mathcal{D}_p} [f_{\mathcal{P}}(x) = 1] = (1 - (1-p^w)^v)^u \pm O(1) \left(\left(v^2 r^2 \exp(2vr^2 p^{w+d})\right) \cdot \delta + (vr^2) \cdot p^{2w-k} \right) \cdot (1+\theta)^u \pm 2\theta^r \binom{u}{r}.$$

The above is a generalization of a similar claim in [CZ15] who only consider the case of $\delta = 0$. We need the more refined *average-case* statement as we only guarantee that *most* blocks differ significantly.

Analyzing influences We next specify some sufficient conditions on a collection of partitions $\mathcal{P} = \{P^1, \ldots, P^u\}$ which guarantee that small coalitions have small influence on $f_{\mathcal{P}}$.

Definition 1.9. *Let $\mathcal{P} = \{P^1, \ldots, P^u\}$ be a collection of partitions of $[n]$ into w-sized blocks. We say $\mathcal{P}$ is (q, τ, ρ)-load balancing if for all $Q \subseteq [n]$ with $|Q| \leq q$, and $j \in [v]$,*

$$\mathop{\mathbb{E}}_{\alpha \in_u [u]} \left[1(Q \cap P_j^\alpha \neq \emptyset) \rho^{|Q \cap P_j^\alpha|} \right] \leq \tau \cdot (q/v).$$

We say $\mathcal{P}$ is (q, τ)-load balancing if the above condition holds for $\rho = 2$.

To gain some intuition for the definition (and the use of the name *load balancing*) consider what happens for a random partition P^α of $[n]$ and a fixed subset Q with $|Q| \ll v$. In this case, we would expect Q to split in a balanced way across the different parts; in particular, for any $j \in [v]$, $P^\alpha_j \cap Q$ would be empty most of the time and $|P^\alpha_j \cap Q| = O(1)$ with high-probability in case it is not empty. Indeed, an easy calculation shows that the above condition holds with $\tau = O(1)$ for $q \leq v$ when P^α is a truly random partition.

Theorem 1.10. *Let $\mathcal{P} = \{P^1, \ldots, P^u\}$ be a collection of partitions of $[n]$ into w-sized blocks that is $(q, \tau, 1/p)$-load balancing. Then,*

$$I_{q,\mathcal{D}_p}(f_\mathcal{P}) \leq (u(1-p^w)^{v-q}) \cdot (\tau p^w) \cdot q.$$

A similar claim is used in the analysis of [AL93, CZ15]. However, [CZ15] work with the stronger condition that for any $Q \subseteq [n]$ with $|Q| \ll q$, $|Q \cap P^\alpha_j| \ll w$ for most α (as opposed to just having a bound on the expectation of $2^{|Q \cap P^\alpha_j|}$). The above generalization, while straightforward, is important as one cannot hope to satisfy their stronger requirement for Q very large ($n^{1-o(1)}$) as needed for the proof of Theorem 1.2.

Constructing nice partitions We next outline how to construct a collection of partitions which is a *good* design as well as load-balancing building on the ideas of [CZ15]. Fix v, w. For a string $\alpha \in [v]^w$, define an associated partition P^α of $[n] \equiv [vw]$ into w-sized blocks as follows:

- Write $\{1, \ldots vw\}$ from left to right in w blocks of length v each. Now, permute the k'th block by shifting the integers in that block by adding α_k modulo v.
- The i'th part now comprises of the elements in the i'th position in each of the w blocks.

Formally, for $i \in [v]$ $P^\alpha_i = \{(k-1)v + ((i - \alpha_k) \mod v) : k \in [w]\}$. As in [CZ15], our final function will be $f_\mathcal{P}$ for $\mathcal{P} := \mathcal{P}_\mathcal{U} = \{P^\alpha : \alpha \subseteq \mathcal{U}\}$ for a suitably chosen set of strings $\mathcal{U} \subseteq [v]^w$; in their work, $\mathcal{U}$ is chosen by using appropriate extractors.

For intuition, fix a constant $0 < \delta < 1$ and first consider the case where $\mathcal{U}$ is the set of Reed-Solomon codewords corresponding to degree $\ell \geq 1/\delta$ polynomials over $[v]$ [5]. Then, a simple calculation shows that $\mathcal{P}_\mathcal{U}$ is a $(w - \ell, \ell + 1, 0)$-design; that is, no two blocks in the partitions of $\mathcal{P}$ overlap in more than ℓ positions. Further, using the fact that a random element of $\mathcal{U}$ is ℓ-wise independent it can be shown from standard arguments that $\mathcal{P}$ is $(q, O_\delta(1))$-load balancing for $q \ll n^{1-\delta}$. Setting the parameters appropriately and applying Theorems 1.8 and 1.10 shows that $f_\mathcal{P}$ is almost-balanced and $(n^{1-\beta})$-resilient—recovering the result of [CZ15].

For the main theorem, Theorem 1.2, we use Theorem 1.5 to get a suitable set of partitions. For instance, taking $\mathcal{U}$ to be the range of the generator from Theorem 1.5, it follows without too much work (essentially from the definitions) that the corresponding $\mathcal{P}_\mathcal{U}$ is $(q, O(1))$-resilient even for $q = \Omega(n/\log n)$ as is needed. However, this may not satisfy the design properties needed to apply Theorem 1.8. We get around this at a high-level by encoding parts of the output of the oblivious sampler in Theorem 1.5 using a Reed-Solomon code. We leave the details to the actual proof.

2 Preliminaries

We first recall some standard notions from pseudorandomness that we need.

Definition 2.1. *A distribution $\mathcal{D}$ over $\{0,1\}^n$ is k-wise independent if for every $I \subseteq [n], |I| \leq k$, and $X \leftarrow \mathcal{D}$, the marginal of X on I is a product distribution.*

Definition 2.2. *For a distribution X, $H_\infty(X) = \min_{x \in Support(X)} \log(1/\Pr[X = x])$.*

[5] Assuming for simplicity that v is a prime.

Definition 2.3 ([NZ96]). *A function $E : [N] \times [D] \to [M]$ is a (k, ε)-*strong extractor *if for every distribution X over $[N]$ with $H_\infty(X) \geq k$, and $Y \in_u [D]$, $(Y, E(X, Y))$ is ε-close in statistical distance to the uniform distribution over $[D] \times [M]$.*

We need the following sampling properties of strong extractors, c.f., [Zuc97].

Lemma 2.4. *Let $E : [N] \times [D] \to [M]$ be a (k, ε)-strong extractor. Then, for all functions $g_1, \ldots, g_D : [M] \to \{0, 1\}$, with $\mu = (1/D) \sum_i \mathbb{E}_{x \in_u [M]}[g_i(x)]$, there are at most 2^k elements $x \in [N]$ such that*

$$\left| \frac{1}{D} \sum_{z \in [D]} g_z(E(x, z)) - \mu \right| \geq \varepsilon.$$

We also need the following explicit extractor construction due to Zuckerman [Zuc97]:

Theorem 2.5. *There exists a constant $C \geq 1$ such that for all $\varepsilon > 0$, and $1 \leq M \leq N^{1/3}$, there is an explicit $((\log N)/2, \varepsilon)$-strong extractor $E : [N] \times [D] \to [M]$ with $D = ((\log N)/\varepsilon)^C$. We also assume without loss of generality that $E(X, Y)$ is uniformly random over $[M]$ when X, Y are uniformly random over $[N]$ and $[D]$ respectively.*

Finally, we also need the following explicit generator of ℓ-wise independent distributions which follows for instance from using the Reed-Solomon code.

Definition 2.6. *For two sequences x, x' over an alphabet $[B]^d$, let $d_H(x, x') = \min_{a \in [B]} |\{i \in [d] : x_i - x'_i \neq a \mod B\}|$.*

Lemma 2.7. *For all prime v and $1 \leq \ell \leq m \leq v$, there exists an explicit function $G_\ell : [v]^\ell \to [v]^m$ such that for any $y \neq y' \in [v]^\ell$, $d_H(y, y') \geq m - \ell$ and $G_\ell(y)$ is ℓ-wise independent when $y \in_u [v]^\ell$.*

Proof. Follows by using the Reed-Solomon code over $[v]$ of degree ℓ and length m. □

We need the following theorem of [KLW10] on fooling read-k DNFs using limited independence. A DNF $f : \{0, 1\}^n \to \{0, 1\}$ is said to be a read-k formula if each variable appears in at most k terms of the DNF. The width of a DNF is the maximum length of any clause in the DNF.

Theorem 2.8. *There exists a constant C such that the following holds for all $0 < \varepsilon < 1$ and $t \geq Cwk \log(1/\varepsilon)$: For any width w read-k DNF $f : \{0, 1\}^n \to \{0, 1\}$ and t-wise independent distribution $\mathcal{D}$ on $\{0, 1\}^n$,*

$$\left| \Pr_{x \leftarrow \mathcal{D}}[f(x) = 1] - \Pr_{x \in_u \{0,1\}^n}[f(x) = 1] \right| \leq \varepsilon.$$

We need Janson's inequality from probability theory, c.f., [AS11]

Theorem 2.9. *Let $S_1, \ldots, S_m \subseteq [n]$ be a collection of sets and let $f_i : \{0, 1\}^n \to \{0, 1\}$ defined by $f_i(x) = \wedge_{j \in S_i} x_j$ be the corresponding collection of monotone terms. Then, for all $0 < p < 1$ and $x \leftarrow \mathcal{D}_p$,*

$$\prod_{i=1}^{m} \Pr[f_i(x) = 0] \leq \Pr\left[\wedge_{i=1}^{m}(f_i(x) = 0)\right] \leq \exp\left(\frac{\Delta}{1 - \gamma}\right) \cdot \prod_{i=1}^{m} \Pr[f_i(x) = 0],$$

where $\gamma = \max_{i=1}^{m} \Pr[f_i(x) = 1]$ and

$$\Delta = \sum_{i \neq j : S_i \cap S_j \neq \emptyset} \Pr[f_i(x) \wedge f_j(x)].$$

Definition 2.10. *For any collection of variables $x_1, \ldots, x_m$ and $1 \le a \le m$, $S_a(x_1, \ldots, x_m) = \sum_{I \subseteq [m], |I|=a} \prod_{i \in I} x_i$ denotes the a'th symmetric polynomial.*

We will use the following standard fact about symmetric polynomials.

Fact 2.11. *For all $1 \le a \le m$ and $0 \le q_1, \ldots, q_m$ with $\sum_i q_i \le \mu$, $S_a(q_1, \ldots, q_m) \le \binom{m}{a} \cdot (\mu/m)^a$.*

We need the following elementary approximations:

Fact 2.12. *For all $x \ge 2$, $e^{-1}(1 - 1/x) \le (1 - 1/x)^x \le e^{-1}$.*

Fact 2.13. *Let $1 \le w \le v \le u$, $B \ge 1$ with $0 \le v - 2^w(\ln(u/\ln 2)) \le B$, and $\theta = (1 - 2^{-w})^v$. Then, $(1 + \theta)^u = O(1)$ and $(1 - \theta)^u = 1/2 \pm O(B \ln u) 2^{-w}$.*

Proof. Note that under the assumptions we must have $v = \Omega(2^w w)$. Then, by the above claim,

$$(1 - 2^{-w})^{B + 2^w \ln(u/(\ln 2))} \le \theta \le (1 - 2^{-w})^{2^w \ln(u/(\ln 2))} \le (\ln 2)/u.$$

Therefore, $(1 + \theta)^u = O(1)$ and

$$(1 - \theta)^u \ge (1 - (\ln 2)/u)^u \ge 1/2(1 - (\ln 2)/u)^{\ln 2} \ge 1/2(1 - O(1)/u).$$

Further,

$$\theta \ge ((\ln 2)/u) \cdot (1 - 2^{-w})^{B + \ln((\ln 2)u)} \ge ((\ln 2)/u) \cdot (1 - O(B + \ln u) 2^{-w}).$$

Thus,

$$(1 - \theta)^u \le \exp(-u\theta) \le (1/2)^{\left(1 - O(B \ln u) 2^{-w}\right)} \le 1/2 \pm O(B \ln u) 2^{-w}.$$

□

3 Analyzing bias

Here we prove Theorem 1.8. We start with the following elementary lemma that follows from the inclusion-exclusion formula:

Lemma 3.1. *Let $Z_1, \ldots, Z_u$ be indicator random variables with $\Pr[Z_i = 0] = \theta$. Suppose that for some even integer $r \le u/2$ and $\gamma \ge 1$, for every $t \le r$,*

$$\binom{u}{t} \theta^t \le \mathop{\mathbb{E}}_{Z} [S_t(1 - Z_1, 1 - Z_2, \ldots, 1 - Z_u)] \le \gamma \binom{u}{t} \theta^t.$$

Then,

$$|\mathbb{E}[Z_1 Z_2 \cdots Z_u] - (1 - \theta)^u| \le 2(\gamma - 1) \cdot (1 + \theta)^u + 4 \binom{u}{r} \theta^r.$$

Proof. Without loss of generality, suppose that $\gamma \le 2$; else, the claim holds trivially. Let $Y_i = 1 - Z_i$. By the inclusion-exclusion principle, we have

$$\left| \mathbb{E}\left[\prod_i Z_i \right] - \sum_{t=0}^{r-1} (-1)^t \, \mathbb{E}[S_t(Y_1, \ldots, Y_u)] \right| \le \mathbb{E}[S_r(Y_1, \ldots, Y_u)].$$

Now, by our hypothesis, for any $t \le r$,

$$\theta^t \binom{u}{t} \le \mathbb{E}[S_t(Y_1, \ldots, Y_u)] \le \gamma \theta^t \binom{u}{t}.$$

Therefore,

$$\left|\mathbb{E}\left[Z_1 \cdots Z_u\right] - \sum_{t=0}^{r-1}(-1)^t \binom{u}{t}\theta^t\right| \leq (\gamma-1)\sum_{t=0}^{r-1}\theta^t\binom{u}{t} + \gamma\theta^r\binom{u}{r} \leq (\gamma-1)(1+\theta)^u + \gamma\theta^r\binom{u}{r}.$$

As the above equation is true with $\gamma = 1$ for the case when the Z_i's are independent of each other, we get that

$$\left|\mathbb{E}\left[Z_1 \cdots Z_u\right] - \prod_{i\in[u]}\mathbb{E}[Z_i]\right| \leq 2(\gamma-1)(1+\theta)^u + 2\gamma\binom{u}{r}\theta^r.$$

The claim now follows. □

Proof of Theorem 1.8. Let $x \leftarrow \mathcal{D}_p$ and $Z_\alpha = T_{P^\alpha}(x)$ for $\alpha \in [u]$. For $j \in [v]$, let $Z_{\alpha j} = \wedge_{\ell \in P_j^\alpha} x_\ell$ so that $Z_\alpha = \vee_{j=1}^v Z_{\alpha j}$. Then, $\Pr[Z_\alpha = 0] = \theta$ for $\theta = (1-p^w)^v$.

Fix $r \leq u/2$. We next estimate $E[\prod_{\alpha\in T}(1-Z_\alpha)]$ for $T \subseteq [u]$ with $|T| \leq r$. For $T \subseteq [u]$, let

$$\Delta(T) = \sum_{\alpha\neq\beta\in[T]}\ \sum_{j,\ell\in[v]:P_j^\alpha\cap P_\ell^\beta\neq\emptyset} \Pr[Z_{\alpha j}\wedge Z_{\beta\ell}].$$

Note that $\Pr[Z_{\alpha j} = 1] = p^w \leq 1/2$. As in [CZ], we now apply Janson's inequality—Theorem 2.9—to the event that $\wedge_{\alpha\in T}(Z_\alpha = 0)$; this gives us:

$$(1-p^w)^{v|T|} \leq \Pr\left[\wedge_{\alpha\in T, j\in[v]}(Z_{\alpha j}=0)\right] \leq \exp\left(2\Delta(T)\right)(1-p^w)^{v|T|}.$$

Thus,

$$\theta^{|T|} \leq \mathop{\mathbb{E}}_{Z}\left[\prod_{\alpha\in T}(1-Z_\alpha)\right] \leq \exp\left(2\Delta(T)\right)\theta^{|T|}. \tag{3.1}$$

Fix $t \leq r$. We next estimate $\mathbb{E}_T\left[\exp(\Delta(T))\right]$ for $T \in_u \binom{[u]}{t}$. Note that $\Delta(T) = \sum_{\alpha\neq\beta\in[T]}\Delta(\{\alpha,\beta\})$. We prove the following bounds on $\Delta(T)$.

Worst-case bound on $\Delta(T)$: Fix $\alpha \neq \beta \in [u]$. Fix an index $j \in [v]$, and let $\ell_1, \ldots, \ell_b \in [v]$ be the indices such that $P_j^\alpha \cap P_{\ell_i}^\beta \neq \emptyset$, and let $w_i = |P_j^\alpha \cap P_{\ell_i}^\beta|$. As $\mathcal{P}$ is a (d,k,δ)-design, $1 \leq w_1, \ldots, w_b \leq w - d$. Now,

$$\sum_{\ell\in[v]:P_j^\alpha\cap P_\ell^\beta\neq\emptyset}\Pr[Z_{\alpha j}\wedge Z_{\beta\ell}] = \sum_{i=1}^b p^{|P_j^\alpha\cup P_{\ell_i}^\beta|} = \sum_{i=1}^b p^{2w-w_i}.$$

As $w_i \in [w-d]$, $d \leq w/2$, and $\sum_i w_i = w$, the above expression is maximized by setting one of the w_i's to be $w-d$ and the other to be d. Therefore,

$$\sum_{\ell\in[v]:P_j^\alpha\cap P_\ell^\beta\neq\emptyset}\Pr[Z_{\alpha j}\wedge Z_{\beta\ell}=1] \leq p^{w+d} + p^{2w-d} \leq 2p^{w+d}.$$

Thus, by summing the above over all indices $j \in [v]$, we get $\Delta(\{\alpha,\beta\}) \leq 2vp^{w+d}$. Summing over all $\alpha \neq \beta \in [T]$, we get

$$\Delta(T) \leq 2|T|^2 vp^{w+d}. \tag{3.2}$$

Average-case bound on $\Delta(T)$: Fix $t \le r$. We next show a high-probability bound on $\Delta(T)$ for $T \in_u \binom{[u]}{t}$. Let $w(T) = \max_{\alpha \neq \beta \in [T], i,j, \in [v]} |P_i^\alpha \cap P_j^\beta|$. Then, for $\alpha \neq \beta \in T$, and $j \in [v]$,

$$\sum_{\ell \in [v] : P_j^\alpha \cap P_\ell^\beta \neq \emptyset} \Pr[Z_{\alpha j} \wedge Z_{\beta \ell} = 1] = \sum_{\ell \in [v] : P_j^\alpha \cap P_\ell^\beta \neq \emptyset} p^{|P_j^\alpha \cup P_{\ell_i}^\beta|} \le w \cdot p^{2w - w(T)}.$$

Therefore, $\Delta(T) \le (vw)|T|^2 p^{2w-w(T)}$. Further, as $\mathcal{P}$ is a (d,k,δ)-design, by a union bound,

$$\Pr_{T \in_u \binom{[u]}{t}} [w(T) \ge k] \le v^2 \cdot t^2 \cdot \delta. \tag{3.3}$$

Bounding the expectation of $\Delta(T)$: Combining Equations 3.2, 3.3, for $t \le r$ and $T \in_u \binom{[u]}{t}$, we get

$$\mathop{\mathbb{E}}_{T} [\exp(2\Delta(T))] \le (v^2 r^2 \delta) \exp\left(4r^2 v p^{w+d}\right) + \exp\left(2nr^2 p^{2w-k}\right) := \gamma.$$

Combining the above with Equation 3.1 we get

$$\binom{u}{t}\theta^t \le \mathop{\mathbb{E}}_{Z} [S_t(1 - Z_1, \ldots, 1 - Z_u)] \le \gamma \binom{u}{t} \theta^t.$$

Hence, by Lemma 3.1

$$|\mathbb{E}[Z_1 \ldots Z_u] - (1-\theta)^u| \le 2(\gamma - 1)(1+\theta)^u + 4\binom{u}{r}\theta^r.$$

The claim now follows by noting that we can assume without loss of generality that $2nr^2p^{2w-k} \ll 1$ (else, the bound is trivial) so that $\exp\left(2nr^2p^{2w-k}\right) \le 1 + 4nr^2p^{2w-k}$. □

We next a state a version of Theorem 1.8 for distributions with limited independence.

Corollary 3.2. *Let $\mathcal{P} = \{P^1, \ldots, P^u\}$ be a collection of partitions of $[n]$ into w-sized blocks that is a (d,k,δ)-design for some $d \le w/2$. Let $v \ge 2^w$ and $\theta = (1 - 2^{-w})^v$. Let $r \le u/2$ be an even integer and let $\mathcal{D}$ be a t-wise independent distribution on $\{0,1\}^n$ for $t \ge Crw\log(1/\varepsilon)$. Then,*

$$\Pr_{x \leftarrow \mathcal{D}}[f_{\mathcal{P}}(x) = 1] = (1 - (1-2^{-w})^v)^u \pm O(1)\left((v^2 x r^2 \delta) \cdot \exp(2vr^2 2^{-w-d}) + vr^2 2^{k-2w}\right) \cdot (1+\theta)^u \pm 2\theta^r \binom{u}{r} \pm O(r)\binom{u}{r}\varepsilon.$$

Proof. The proof of the above claim is similar to the above argument with one change. Using the notation from the above proof, for any $T \subseteq [u]$, the event that $\wedge_{\alpha \in T, j \in [v]}(Z_{\alpha j} = 0)$ corresponds to the (un)satisfiability of a read-$|T|$ width-w DNF. Therefore, by Theorem 2.8, we get an analogue of Equation 3.1 for the present case as well: for any $T \subseteq [u]$ with $|T| \le r$,

$$\theta^{|T|} - \varepsilon \le \mathop{\mathbb{E}}_{Z}\left[\prod_{\alpha \in T}(1 - Z_\alpha)\right] \le \exp\left(2\Delta(T)\right)\theta^{|T|} + \varepsilon. \tag{3.4}$$

The claim now follows by using the above inequality in place of Equation 3.1 in the rest of the proof of Theorem 1.8. □

4 Analyzing influence

Proof of Theorem 1.10. Let $Q \subseteq [n]$ with $|Q| = q$. Note that for every $\alpha \in [u]$, a partial assignment x to the variables not in Q leaves T_{P^α} undetermined if and only if

1. For every part P^α_j that does not intersect Q, $x_i = 0$ for some $i \in P^\alpha_j$.
2. For some $j \in [v]$ with $P^\alpha_j \cap Q \neq \emptyset$, $x_i = 1$ for every $i \in (P^\alpha_j \setminus Q)$.

The above two events are independent of each other. The probability of (1) is at most $(1-p^w)^{v-q}$ as there are at least $v-q$ parts of P^α that do not intersect Q. The probability of (2) is at most

$$\sum_{j \in [v] : P^\alpha_j \cap Q \neq \emptyset} p^{w - |P^\alpha_j \cap Q|}$$

Therefore, for $\alpha \in_u [u]$,

$$\begin{aligned}
I_{Q,\mathcal{D}_p}(f_{\mathcal{P}}) &\leq \sum_{\beta \in [u]} I_{Q,\mathcal{D}_p}(T_{P^\beta}) \leq u \cdot \mathbb{E}\left[I_{Q,\mathcal{D}_p}(T_{P^\alpha})\right] \\
&\leq u \cdot \mathbb{E}\left[(1-p^w)^{v-q} \cdot \left(\sum_{j \in [v] : P^\alpha_j \cap Q \neq \emptyset} p^{w - |P^\alpha_j \cap Q|}\right)\right] \\
&\leq u(1-p^w)^{v-q} p^w \cdot \left(\sum_{j \in [v]} \mathbb{E}\left[1(P^\alpha_j \cap Q \neq \emptyset)(1/p)^{|P^\alpha_j \cap Q|}\right]\right) \\
&\leq u(1-p^w)^{v-q} \cdot \tau \cdot (p^w q).
\end{aligned}$$

□

We next a state a version of Theorem 1.8 for distributions with limited independence.

Corollary 4.1. *Let $\mathcal{P} = \{P^1, \ldots, P^u\}$ be a collection of partitions of $[n]$ into w-sized blocks that is (q,τ)-load balancing. Then, for all $t \geq Cw\log(1/\varepsilon)$ for some sufficiently big constant C,*

$$I_{q,t}(f_{\mathcal{P}}) \leq (u(1-2^{-w})^{v-q}) \cdot (\tau p^w q) + (uv)\varepsilon.$$

Proof. Let $\mathcal{D}$ be a t-wise independent distribution on $\{0,1\}^n$. As in the above proof, observe that Q leaves T_{P^α} undetermined if and only if

1. For every part P^α_j that does not intersect Q, $x_i = 0$ for every $i \in P^\alpha_j$.
2. For some $j \in [v]$ with $P^\alpha_j \cap Q \neq \emptyset$, $x_i = 1$ for every $i \in (P^\alpha_j \setminus Q)$.

Let $J \subseteq [v]$ be all indices such that $P^\alpha_j \cap Q \neq \emptyset$ and let $I \subseteq [n]$ be all variables i that belongs to parts P^α_j not intersecting Q. Then, the above is equivalent to $\vee_{j \in V} f_j$, where

$$f_j(x) = \left(\bigwedge_{i \in P^\alpha_j \setminus Q} x_i\right) \bigwedge_{j \notin J} \left(\bigvee_{i \in P^\alpha_j} (\neg x_j)\right).$$

Note that the above is a read-once CNF. Therefore, by Theorem 2.8,

$$\Pr_{x \leftarrow \mathcal{D}}[f_j(x) = 1] \leq \Pr_{x \in_u \{0,1\}^n}[f_j(x) = 1] + \varepsilon \leq (1-2^{-w})^{v-q} \cdot 2^{-w + |P^\alpha_j \cap Q|} + \varepsilon.$$

The claim now follows by repeating the calculations of Theorem 1.10 with the above equation leading to an additional error of $(uv)\varepsilon$. □

5 Oblivious sampler preserving the moment generating function

Here we prove Theorem 1.5 which will be the main building block in proving Theorem 1.2. With a view towards future use, we modify the construction presented in the introduction (Equation **??**) even though the simpler construction described there suffices for proving the theorem. Let $\varepsilon = \mathrm{poly}(1/w)$ to be chosen later, and c a sufficiently big constant, let $E : [v^c] \times [D] \to [v/D]$ be a $((c \log v)/2, \varepsilon)$-strong extractor as in Theorem 2.5 with $D = ((c \log v)w)^C$ for some universal constant C. Without loss of generality, suppose that D is prime. For a parameter $\ell \geq 1$ to be chosen later, let $G_\ell : [D]^\ell \to [D]^w$ generate a ℓ-wise independent distribution as in Lemma 2.7.

Define $G : [v^c] \times [D]^\ell \to [v]^w$ as follows:

$$G(x, y)_i = G_\ell(y)_i \circ E(x, G_\ell(y)_i), \tag{5.1}$$

where we associate $[D] \times [v/D]$ with $[v]$ in a straightforward manner.

The main lemma of this section is the following:

Lemma 5.1. *Let $G : [v^c] \times [D]^\ell$ be as in Equation 5.1 and let $f_1, \ldots, f_w : [v] \to [0, 1]$ be functions with $\sum_i \mathbb{E}[f_i] = \mu$. Then, for all $\rho \geq 1$, and $\alpha = G(x, y)$ for $(x, y) \in_u [v^c] \times [D]^\ell$, and $\theta = \mu/(w-1) + \varepsilon$,*

$$\mathop{\mathbb{E}}_{\alpha}\left[\rho^{\sum_i f_i(\alpha_i)}\right] \leq 1 + 3(\rho-1)\mu \cdot (1 + (\rho-1)\theta)^{w-1} + 3\rho^w \mu \binom{w-1}{\ell} \theta^\ell + (2\rho)^w w \cdot v^{-c/2}.$$

Proof. Let $Y_i = f_i(\alpha_i)$ and $\mu_i = \mathbb{E}[f_i] = \mathbb{E}[Y_i]$. Let $Z = \rho^{Y_1 + \ldots Y_w}$ and $\delta = wv^{-c/2}$. We can assume without loss of generality that $\delta \leq 1/2$; otherwise, the claim is trivial. The proof of the lemma involves two modular steps: (1) We use properties of the extractor to argue that the Y_i's behave like almost ℓ-wise independent random variables. (2) We then argue that the moment generating function, in our setting of parameters, is *fooled* by Y_i's that are almost ℓ-wise independent in the above sense.

The following claim will control the correlations of the Y_i's:

Claim 5.2. *For every $i \in [w]$ and $I \subseteq [w] \setminus \{i\}$, with $|I| < \ell$,*

$$\mathbb{E}\left[Y_i \prod_{j \in I} Y_j\right] \leq (1 + 2\delta) \cdot \mu_i \cdot \prod_{j \in I} (\mu_j + \varepsilon) + \delta. \tag{5.2}$$

Proof. For $j \in [w]$, call $x \in [v^c]$ j-bad if $\left|\mathbb{E}_{z \in_u [D]}[f_j(z \circ E(x, z))] - \mu_j\right| \geq \varepsilon$. We next bound the number of bad strings x for any index $j \in [w]$. Fix $j \in [w]$. For $z \in [D]$, define $g_z : [v/D] \to [0, 1]$ by $g_z(x') = f_j(z \circ x')$. Then, $\sum_{z \in [D]} \mathbb{E}_{x' \in_u [v/D]}[g_z(x')] = D\,\mathbb{E}_j[f_j] = D\mu_j$; thus, x is j-bad if and only if

$$\left|(1/D) \sum_{z \in [D]} g_z(E(x, z)) - \mu_j\right| \geq \varepsilon.$$

By Lemma 2.4, for every $j \in [w]$, there are at most $v^{c/2}$ bad strings. Let $\mathcal{E}$ be the event that $x \in_u [v^c]$ is not j-bad for every $j \in w$. Then, $\Pr[\neg\mathcal{E}] \leq wv^{-c/2} = \delta$. As $G(y)$ is ℓ-wise independent, conditioned on $\mathcal{E}$, $(Y_j : j \in I)$ are independent random variables and for every $j \in I$,

$$\mathbb{E}[Y_j] = \mathop{\mathbb{E}}_{y \in_u D}[f_j(y \circ E(x, y)] = \mu_j \pm \varepsilon,$$

as x is not j-bad. Therefore,

$$\begin{aligned}\mathbb{E}\left[Y_i \prod_{j\in I} Y_j\right] &\le \Pr[\neg\mathcal{E}] + \mathop{\mathbb{E}}_{x}\left[\mathop{\mathbb{E}}_{y}\left[\left(Y_i \prod_{j\in I} Y_j\right)|\mathcal{E}\right]\right] = \Pr[\neg\mathcal{E}] + \mathop{\mathbb{E}}_{x}\left[\mathop{\mathbb{E}}_{y}[Y_i|\mathcal{E}] \cdot \prod_{j\in I}\mathop{\mathbb{E}}_{y}[Y_j|\mathcal{E}]\right] \\ &\le \delta + \prod_{j\in I}(\mu_j+\varepsilon)\cdot \mathbb{E}[Y_i|\mathcal{E}] \\ &\le \delta + \prod_{j\in I}(\mu_j+\varepsilon)\cdot \mu_i(1+2\delta),\end{aligned}$$

where the last inequality follows because $\mathbb{E}[Y_i] = \mu_i$ so that $\mathbb{E}[Y_i|\mathcal{E}] \le \mu_i/\Pr[\mathcal{E}] \le \mu_i(1+2\delta)$. The claim now follows. □

We next use the above claim to bound $\mathbb{E}[Z]$. Observe that

$$Z = \rho^{Y_1+\ldots+Y_w} \le \prod_{i=1}^{w}(1+(\rho-1)Y_i) = 1 + \sum_{a=1}^{w}(\rho-1)^a S_a(Y_1,\ldots,Y_w).$$

We will approximate $\mathbb{E}[Z]$ by truncating the above expansion to only involve the first ℓ symmetric polynomials: we have

$$\begin{aligned}Z \le 1 + \sum_{a=1}^{w}(\rho-1)^a S_a(Y_1,\ldots,Y_w) \le 1 + \sum_{a=1}^{\ell-1}(\rho-1)^a S_a(Y_1,\ldots,Y_w) + \rho^w S_\ell(Y_1,\ldots,Y_w) \le \\ 1 + \sum_{i=1}^{w}\cdot\sum_{a=0}^{\ell-1}(\rho-1)^{a+1}\cdot Y_i \cdot S_a((Y_j : j\neq i)) + \rho^w \sum_{i=1}^{w} Y_i S_{\ell-1}((Y_j : j\neq i)). \quad (5.3)\end{aligned}$$

We bound each of the terms in the above equation expression next. For $i \in [w]$ and $a \le \ell-1$, by Claim 5.2

$$\begin{aligned}\mathbb{E}\left[Y_i \cdot S_a((Y_j : j\neq i))\right] \le (1+2\delta)\,\mu_i \sum_{I\subseteq[w]\setminus\{i\},|I|=a}\prod_{j\in I}(\mu_j+\varepsilon) + \binom{w-1}{a}\delta \le \\ (1+2\delta)\mu_i\binom{w-1}{a}\theta^a + \binom{w-1}{a}\delta, \quad (5.4)\end{aligned}$$

where the last inequality follows from Fact 2.11.

Plugging the above inequality into Equation 5.3, we get

$$\begin{aligned}\mathbb{E}[Z] &\le 1 + \sum_{i=1}^{w} 3(\rho-1)\mu_i \sum_{a=0}^{\ell-2}\binom{w-1}{a}(\rho-1)^a\theta^a + \rho^w\left(\sum_{i=1}^{w}(3\mu_i)\binom{w-1}{\ell}\theta^\ell + \binom{w-1}{\ell}\delta\right) \\ &\le 1 + 3(\rho-1)\mu(1+(\rho-1)\theta)^{w-1} + 3\mu\rho^w\binom{w-1}{\ell}\theta^\ell + (2\rho)^w\delta.\end{aligned}$$

The claim now follows. □

Proof of Theorem 1.5. The theorem follows by setting $\varepsilon = 1/w$, $\rho = 2$, $\ell = 6w/(\log w)$, in the above lemma. As $\mu \le 1$, we have $\theta = \mu/(w-1) + \varepsilon \le 2/(w-1)$, and

$$\mathbb{E}\left[2^{\sum_i f_i(\alpha_i)}\right] \le 1 + O(\mu)\,(1+2/(w-1))^{w-1} + 2^w O(\mu)\binom{w-1}{\ell}(2/(w-1))^\ell + 4^w w v^{-c/2} = 1 + O(\mu) + \gamma,$$

for c chosen so that $v^{-c/2} < \gamma/4^w w$. In particular, it suffices to set $c = C\max(1, (w+\log(1/\gamma))/(\log v))$ for a sufficiently large universal constant C. The seed-length of the generator is $r = c\log v + \ell(\log D) = O(w + \log v + \log(1/\gamma) + w(\log\log v)/(\log w))$, proving the theorem. □

6 Explicit resilient functions

Here we present our main construction proving Theorem 1.2. Fix v, w. For a string $\alpha \in [v]^w$, define an associated partition P^α of $[n] \equiv [vw]$ into w-sized blocks as follows:

- Write $\{1, \ldots vw\}$ from left to right in w blocks of length v each. Now, permute the k'th block by shifting the integers in that block by adding α_k modulo v.
- The i'th part now comprises of the elements in the i'th position in each of the w blocks.

Formally, for $i \in [v]$ $P^\alpha_i = \{(k-1)v + ((i - \alpha_k) \mod v) : k \in [w]\}$. As in [CZ15], our final function will be $f_\mathcal{P}$ for $\mathcal{P} = \{P^\alpha : \alpha \subseteq \mathcal{U}\}$ for a suitably chosen set of strings $\mathcal{U} \subseteq [v]^w$.

6.1 Polynomially resilient functions from Reed-Solomon code

For intuition, we first use our arguments to present a simpler variant of the construction of [CZ15] (e.g., the function below is depth 3 as opposed to the depth 4 construction of [CZ15]) to get a $(n^{1-\delta})$-resilient function from Reed-Solomon codes as alluded to in the introduction; the main difference being that we use a k-wise independent generator as in Lemma 2.7 instead of an extractor as is done in [CZ15].

Let $1 \leq w \leq v$, where v is prime. For some parameter $\ell \geq 1$ to be chosen later, let $G_\ell : [v]^\ell \to [v]^w$ be as in Lemma 2.7 and let $\mathcal{RS} = \{G_\ell(x) : x \in [v]^\ell\}$. Let $f \equiv f_\mathcal{RS} = f_\mathcal{P}$, where $\mathcal{P} = \{P^\alpha : \alpha \in \mathcal{RS}\}$. We show that for any constant $0 < \beta < 1$, and $\ell \geq 1/2\beta$, $f_\mathcal{RS}$ is $\Omega(n^{1-\beta})$-resilient and has bias $1/2 \pm o(1)$.

Lemma 6.1. *For $1 \leq \ell \leq w$, $f_\mathcal{RS}$ as defined above is a $(w - \ell, \ell + 1, 0)$-design.*

Proof. First note that for any $\alpha, \beta \in [v]^w$ and $i, j \in [v]$,, $|P^\alpha_i \cap P^\beta_j| = |\{k \in [w] : \beta_k - \alpha_k = (j - i) \mod v\}| \leq w - d_H(\alpha, \beta)$. From the properties of $\mathcal{RS}$ as in Lemma 2.7, we get that for $\alpha \neq \beta \in \mathcal{RS}$, $|P^\alpha_i \cap P^\beta_j| \leq w - d_H(\alpha, \beta) \leq \ell$. The claim now follows from the definition of design. □

Lemma 6.2. *For $1 \leq \ell \leq w/2$, $\mathcal{RS}$ is (q, τ)-load balancing for $\tau = 2^{\ell+1} + 2^w (q/v)^{\ell-1}$.*

Proof. Let $Q \subseteq [n]$ with $|Q| = q \leq v$. For $1 \leq i \leq w$, let $Q_i = Q \cap \{(i-1)v + j : j \in [v]\}$. Fix an index $k \in [v]$ and for $i \in [w]$ define $f_i : [v] \to \{0, 1\}$ by $f_i(x) = 1$ if $((i-1)v + k - x) \mod v \in Q_i$ and 0 otherwise. Then, $X := |P^\alpha_k \cap Q| = \sum_{i=1}^w f_i(\alpha_i)$. Let $\alpha \in_u \mathcal{RS}$ and let $X_i = f_i(\alpha_i)$. Then, $X = \sum_i X_i$, where $X_1, \ldots, X_w$ are ℓ-wise independent. Let $\mu_i = \mathbb{E}[X_i]$ and $\mu = \mathbb{E}[X] = q/v$. Then, by a standard caluclation, for all $t > \ell$,

$$\Pr[X \geq t] \cdot \binom{t}{\ell} \leq \mathbb{E}[S_\ell(X_1, \ldots, X_w)] = \binom{w}{\ell} \sum_{I \subseteq [w], |I| = \ell} \prod_{i \in I} \mu_i \leq \binom{w}{\ell} \left(\frac{\mu}{w}\right)^\ell,$$

where the last inequality follows from Fact 2.11. Therefore, $\Pr[X \geq t] \leq (e\mu/t)^\ell$. Let $\mathcal{E}$ be the event that $1 \leq X \leq \ell$. Then, for $\ell \geq 3$,

$$\mathbb{E}\left[1(Q \cap P^\alpha_k \neq \emptyset) 2^{|Q \cap P^\alpha_k|}\right] = \mathbb{E}\left[1(X > 0) 2^X\right] =$$
$$\Pr[\mathcal{E}]\, \mathbb{E}\left[1(X > 0) 2^X | \mathcal{E}\right] + \Pr[X > \ell]\, \mathbb{E}\left[1(X > 0) 2^X | X > \ell\right] \leq$$
$$2^\ell \Pr[X > 0] + 2^w \Pr[X > \ell] \leq 2^\ell (q/v) + 2^w \mu^\ell.$$

The claim now follows from the definition of load balancing. □

We next use the above claims along with Theorems 1.8 and 1.10 for a suitable setting of parameters.

Lemma 6.3. *For all $0 < \delta < 1$, there exists a constant $c_\delta \geq 1$ and a suitable choice of $v = \Theta_\delta(2^w w)$ such that the following holds. For $\ell \geq 1/\delta$, the function $f_{\mathcal{RS}}$ as defined above is $c_\delta 2^{w(1-\delta)}$-resilient and $\Pr_{x \leftarrow \mathcal{D}_{1/2}}[f_{\mathcal{RS}}(x) = 1] = 1/2 \pm 2^{-\Omega(w)}$.*

Proof. Let $\ell = \max(3, \lceil 1/\delta \rceil)$. For v to be chosen in a little bit, let $u = v^\ell$ and $f \equiv f_{\mathcal{RS}}$. We would like our choice of v to minimize $|v - 2^w \ln((\ln 2)/u)|$ so that we can get an almost-balanced function using Fact 2.13. To this end, let $\phi : \mathbb{R}_+ \to \mathbb{R}$ be defined by

$$\phi(x) = x - 2^w \ln((\ln 2)v^\ell)$$

and let $x^* \geq 1$ be such that $\phi(x^*) = 0$. There exists such an x^* by the continuity of ϕ. It is also easy to check that for w sufficiently large, $\phi'(y) \geq 0$ for all $y \geq x^*$. We set v to be the smallest prime larger than x.[6] Note that $v \leq x^* + B$ where $B = 2^{c_1 w}$ for some universal constant $c_1 < 1$ (see [Wik] for instance), so that $0 = \phi(x^*) \leq \phi(v) \leq \phi(x^*) + B$. Let $\theta = (1 - 2^{-w})^v$. Then, by Fact 2.13, $(1 + \theta)^u = O(1)$ and

$$(1 - \theta)^u = 1/2 \pm O(1)2^{-\Omega(w)}.$$

Now, by Lemma 6.1 and Theorem 1.8 applied with $r = w$ and $p = 1/2$,

$$\Pr_{x \leftarrow \mathcal{D}_{1/2}}[f_{\mathcal{RS}}(x) = 1] = (1-\theta)^u \pm O(\ell)2^w w^3 2^{-2w+\ell+1} \pm 2^{-w} = (1-\theta)^u \pm O(\ell 2^\ell) w^3 2^{-w} = 1/2 \pm 2^{-\Omega(w)}.$$

Next, by Lemma 6.2 and Theorem 1.10, for any $q \leq 2^{w(1-\delta)}$, as $\ell \geq \lceil 1/\delta \rceil$,

$$I_q(f_{\mathcal{RS}}) \leq u(1 - 2^{-w})^{v-q} \cdot (2^{-w} q) \cdot \left(2^\ell + 2^w (q/v)^{\ell-1}\right) \leq O(2^{-w} q) \cdot (2^\ell + 2^w 2^{-\ell\delta w}) = O_\delta(2^{-w} q).$$

It follows that $f_{\mathcal{RS}}$ is $\left(c_\delta 2^{w(1-\delta)}\right)$-resilient for some constant c_δ. □

Corollary 6.4. *For all $0 < \delta < 1$, there exists a constant $c_\delta \geq 1$ such that the following holds. There exists an explicit depth three monotone function $f : \{0,1\}^n \to \{0,1\}$ which can be computed in time n^{c_δ} such that for $t \geq c_\delta (\log n)^4$*

- *f is almost balanced: for any t-wise independent distribution $\mathcal{D}$ on $\{0,1\}^n$, $\Pr_{x \leftarrow \mathcal{D}}[f(x) = 1] = 1/2 \pm n^{-\Omega(1)}$.*
- *f has small influences: $I_{q,t}(f) \leq c_\delta q / n^{1-\delta}$.*

Proof. We instantiate the previous lemma to get $f \equiv f_{\mathcal{RS}}$ for $\delta' = \delta/2$. Then, $n = O(2^w w^2)$ so that $2^{w(1-\delta')} = \Omega(n^{1-\delta})$. To analyze the bias under t-wise independent distributions, we apply Corollary 3.2 with $r = w = O(\log n)$, $\varepsilon = u^{-2r} = n^{-O(\log n)}$ instead of Theorem 1.8 in the above argument. Similarly, to analyze the influence under t-wise independent distributions we use Corollary 4.1 with $\varepsilon' = 1/(n^3)$ instead of Theorem 1.10. Then, the amount of independence needed is $O(wr \log(1/\varepsilon)) = O(\log^4 n)$. □

6.2 Proof of Theorem 1.2

We now prove Theorem 1.2. As mentioned in the introduction, the approach is similar to the above where we use the output of the generator from Theorem 1.5 instead of the Reed-Solomon code. We ensure the requisite *design* properties to apply Theorem 1.8, at a high-level, by *padding* the output of the generator with a Reed-Solomon encoding of length $2c$ for a sufficiently big constant c.

Let c be a parameter to be chosen later and suppose that v, D are prime numbers below. Let $E : [v^c] \times [D] \to [v/D]$ be a strong extractor with error $\varepsilon = \text{poly}(1/w)$ and $D = \text{poly}(w)$ to

[6] We can find such a prime in time $2^{O(w)}$ which is fine for us.

be chosen later. Let $\ell = \Theta(w/(\log w))$ be a parameter to be chosen later. Let $G_c : [v]^c \to [v]^{2c}$, $G_\ell : [D]^\ell \to [D]^{w-2c}$ generate a c-wise independent distribution over $[v]$ and a ℓ-wise independent distribution over $[D]$ respectively as guaranteed by Lemma 2.7.

Now, define $\mathcal{U} : [v^c] \times [D]^\ell \to [v]^w$ as follows:

$$\mathcal{U}(x,y)_i = \begin{cases} G_c(x)_i & \text{if } 1 \le i \le 2c \\ G_\ell(y)_{i-2c} \circ E(x, G_\ell(y)_{i-2c}) & \text{if } 2c < i \le w \end{cases}. \tag{6.1}$$

(Here, we associate an element of $[D] \times [v/D]$ with an element of v in a straightforward bijective manner.)

Abusing notation, we let $\mathcal{U} = \{\mathcal{U}(x,y) : x \in [v^c], y \in [D]^\ell\} \subseteq [v]^w$ as well. Our final function will be $f \equiv f_{\mathcal{P}}$ for $\mathcal{P} = \{P^\alpha : \alpha \in \mathcal{U}\}$. The following claims help us apply Theorem 1.8 and Theorem 1.10 to analyze $f_{\mathcal{P}}$.

Lemma 6.5. *For all $c < w - 2c - \ell$, $\mathcal{P}$ is a $(c, 2c+\ell, 1/D^\ell)$-design.*

Proof. Note that for any $\alpha, \beta \in [v]^w$, and any $i, j \in [v]$, $|P_i^\alpha \cap P_j^\beta| = |\{k \in [w] : \beta_k - \alpha_k = (j-i) \bmod v\}| \le w - d_H(\alpha, \beta)$.

Let $\alpha = G(x,y) \ne \beta = G(x',y') \in \mathcal{U}$. Now, if $y \ne y'$, then $d_H(\alpha,\beta) \ge d_H(G_\ell(y), G_\ell(y')) \ge w - 2c - \ell$; similarly, if $x \ne x'$, then $d_H(\alpha,\beta) \ge d_H(G_c(x), G_c(x')) \ge c$. Therefore, in either case $d_H(\alpha,\beta) \ge \min(c, w-2c-\ell) = c$.

Similarly, for any fixed $\alpha = G(x,y) \in \mathcal{U}$, and $\beta = G(x',y') \in_u \mathcal{U}$, unless $y = y'$, $d_H(\alpha,\beta) \ge w - 2c - \ell$. On the other hand, $\Pr[y' = y] \le 1/D^\ell$.

The above claims imply that $\mathcal{P}$ is a $(c, w-2c-\ell, 1/D^\ell)$-design as needed. □

We next use Lemma 5.1 to analyze the load-balancing properties of $\mathcal{P}$.

Lemma 6.6. *Let $\mathcal{U}$ be as in Equation 6.1 for E being a $((c \log v)/2, \varepsilon)$-extractor for $\varepsilon < 1/w$ and $\ell \ge 6w/(\log w)$. Then, $\mathcal{P} = \{P^\alpha : \alpha \in \mathcal{U}\}$ is (q,τ)-load balancing for $q \le v$ and $\tau = O(2^{2c} + w 2^w v^{-c/2+1})$.*

Proof. Let $Q \subseteq [n]$ with $|Q| = q \le v$. For $1 \le i \le w$, let $Q_i = Q \cap \{(i-1)v + j : j \in [v]\}$. Fix an index $k \in [v]$ and for $i \in [w]$ define $f_i : [v] \to \{0,1\}$ by $f_i(x) = 1$ if $((i-1)v + k - x) \bmod v \in Q_i$ and 0 otherwise. Then, $|P_k^\alpha \cap Q| = \sum_{i=1}^w f_i(\alpha_i)$. Further, $\sum_i \mathbb{E}_{x \in_u [v]}[f_i(x)] = \sum_i |Q_i|/v = q/v := \mu \le 1$.

In the following, let $\alpha \in_u \mathcal{U}$. For $1 \le i \le 2c$, let $X_i = f_i(\alpha_i)$ and for $1 \le j \le w - 2c$ let $Y_j = f_{j+2c}(\alpha_{j+2c})$. Let $\mu_i = \mathbb{E}[f_i]$, $X = \sum_{i=1}^{2c} X_i$, $Y = \sum_{j=1}^{w-2c} Y_j$, and $Z = X + Y$. We next bound $\mathbb{E}[2^Z]$ by applying Lemma 5.1 to Y combined with the trivial observation that X is at most $2c$:

$$\begin{aligned} \mathbb{E}\left[1(Q \cap P_k^\alpha \ne \emptyset) 2^{|Q \cap P_k^\alpha|}\right] &= \mathbb{E}\left[1(Z \ge 1) 2^Z\right] = \mathbb{E}\left[2^Z\right] - \Pr[Z = 0] \\ &= \mathbb{E}\left[2^Z\right] - 1 + \Pr[Z \ge 1] \le \mathbb{E}\left[2^Z\right] - 1 + \mathbb{E}[Z] \\ &= \mathbb{E}[2^X - 1] + \mathbb{E}[2^X(2^Y - 1)] + \mathbb{E}[X] + \mathbb{E}[Y] \\ &\le \mathbb{E}[2^X - 1] + 2^{2c} \cdot \mathbb{E}[2^Y - 1] + \mu \\ &\le \mathbb{E}[2^{2c}(X_1 + \ldots X_{2c})] + 2^{2c} \cdot \mathbb{E}[2^Y - 1] + \mu. \end{aligned}$$

By Lemma 5.1 applied to Y with $\rho = 2$, $\ell = 6w/(\log w)$, and $\varepsilon < 1/2w$, we get that

$$\mathbb{E}[2^Y - 1] \le O(\mu)(1 + 2/(w-1))^{w-1} + O(\mu) 2^{w-2c} \binom{w-1}{\ell} (2/w-1)^\ell + 2^{w-2c} w v^{-c/2} = O(\mu) + 2^{w-2c} w v^{-c/2}.$$

Further, $\mathbb{E}[X_1 + \ldots + X_{2c}] \le \mu$. Therefore, as $\mu \ge 1/v$,

$$\mathbb{E}\left[1(Q \cap P_k^\alpha \neq \emptyset) 2^{|Q \cap P_k^\alpha|}\right] \le O(2^{2c})\mu + O(1) w 2^w v^{-c/2} \le O(1) \cdot \mu \cdot (2^{2c} + w 2^w v^{-c/2+1}).$$

□

Proof of Theorem 1.2. We first set up some parameters. Let $c \ge 2$ be a sufficiently large constant to be chosen later. Let $w \ge 1$ be arbitrary and $\varepsilon = 1/w^3$. Let $D = ((c \log v) w)^C$ for some universal constant C so that there exists an explicit $(c(\log v)/2, \varepsilon)$-strong extractor $E : [v^c] \times [D] \to [v/D]$ for all $c \ge C$ as in Theorem 2.5. Set $v = \Theta(2^w w)$ to be chosen precisely in a little bit. For this setting of v, let $\mathcal{U} \subseteq [v]^w$ be as defined in Equation 6.1 with $\ell = 6w/(\log w)$ and E as the extractor. Let $\mathcal{P} = \mathcal{P}_{\mathcal{U}}$. Then, $|\mathcal{U}| := u = v^c \times D^\ell$. We will show that $f \equiv f_{\mathcal{P}}$ satisfies the conditions of Theorem 1.2 for c sufficiently large.

As in the proof of Lemma 6.3, we would like our choice of v to be such that $v = 2^w \ln((\ln 2)u)$. To this end, let $\phi : \mathbb{R}_+ \to \mathbb{R}$ be defined by

$$\phi(x) = x - 2^w \left(c \ln x + C\ell \ln(\log x) + C\ell \ln(cw) + \ln \ln 2\right)$$

and let $x^* \ge 1$ be such that $\phi(x^*) = 0$. There exists such an x^* by the continuity of ϕ. Let v be the smallest prime larger than x^*. Note that $v \le x^* + B$ where $B = 2^{c_1 w}$ for some universal constant $c_1 < 1$ (see [Wik] for instance), so that $0 = \phi(x^*) \le \phi(v) \le \phi(x^*) + B$. Let $\theta = (1 - 2^{-w})^v$. Then, by Fact 2.13, $(1+\theta)^u = O(1)$ and

$$(1-\theta)^u = 1/2 \pm O(1) 2^{-\Omega(w)}. \tag{6.2}$$

?

Analyzing bias: By Lemma 6.5, $\mathcal{P}$ is a $(c, 2c+\ell, 1/D^\ell)$-deisgn. Therefore, by Theorem 1.8 applied with $r = c$, $\Pr_{x \in_u \{0,1\}^n}[f_{\mathcal{P}}(x) = 1] = (1-\theta)^u \pm O(\delta_1) + O(\delta_2) + O(\delta_3)$, where

$$\begin{aligned}
\delta_1 &= v^2 c^2 (1/D^\ell) \cdot \exp(2vc^2 2^{-w-c})(1+\theta)^u \\
\delta_2 &= vc^2 2^{-2w+\ell+2c} \le wc^2 2^{-w+\ell+2c}(1+\theta)^u \\
\delta_3 &= 2(u\theta)^w (e/c)^c \le 2(e/c)^c.
\end{aligned}$$

We next bound each of these terms. Note that $1/D^\ell \le 1/w^\ell \le 1/6^w$. Therefore, as $c \ge C$, and $v = O(1)c2^w w$,

$$\delta_1 \le O(1)\left(\frac{w^2 c^2}{3^w}\right) \exp(O(1) w c^3 2^{-c}) = O(c^2) 2^{-\Omega(w)},$$

for c sufficiently large. Next,

$$\delta_2 \le O(1) wc^2 2^{-w+\ell+2c} \le O(c^2) 2^{-\Omega(w)},$$

for $c \le w/4$. Thus, for a universal constant C', if $C' \le c \le w/4$, by Equation 6.2,

$$\Pr_{x \in_u \{0,1\}^n}[f_{\mathcal{P}}(x) = 1] = 1/2 \pm O(c^2) 2^{-\Omega(w)} \pm 2(e/c)^c.$$

Analyzing influence: We claim that $f_{\mathcal{P}}$ has small influence for coalitions of size $o(2^w)$. Let $1 \leq q \leq v$ so that $q/v \leq 1$. Then, by Lemma 6.6, $\mathcal{P}$ is (q, τ)-load balancing for

$$\tau = O(2^{2c})(1 + v^{-c/2+1}) = O(2^{2c}).$$

Therefore, by Theorem 1.10, for all $q \leq v$,

$$I_q(f_{\mathcal{P}}) \leq u(1 - 2^{-w})^{v-q} \cdot 2^{2c}(2^{-w}q) = O(2^{2c})2^{-w}q = O(2^{2c})q(\log^2 n)/n,$$

where the last inequality follows as $2^w = \Theta(n/(\log^2 n))$. The theorem now follows by choosing c to be sufficiently large. □

We next prove Corollary 1.4.

Proof of Corollary 1.4. The proof is exactly the same as the above argument for Theorem 1.2 but instead of using Theorem 1.8 we use Corollary 3.2 with $r = O(c)$, $\varepsilon = u^{-O(r)}$ and instead of Theorem 1.10 we use Corollary 4.1 with $\varepsilon = 1/(uv^2)$. The amount of independence we need is $t \gg rw \log(1/\varepsilon) = O(\log^2 n)$ as required for the theorem. □

References

[AL93] Miklós Ajtai and Nathan Linial. The influence of large coalitions. *Combinatorica*, 13(2):129–145, 1993.

[AN93] Noga Alon and Moni Naor. Coin-flipping games immune against linear-sized coalitions. *SIAM J. Comput.*, 22(2):403–417, 1993.

[AS11] N. Alon and J.H. Spencer. *The Probabilistic Method*. Wiley Series in Discrete Mathematics and Optimization. John Wiley & Sons, 2011.

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

[BN00] Ravi B. Boppana and Babu O. Narayanan. Perfect-information leader election with optimal resilience. *SIAM J. Comput.*, 29(4):1304–1320, 2000.

[Bra10] Mark Braverman. Polylogarithmic independence fools AC^0 circuits. *J. ACM*, 57(5), 2010.

[CZ15] Eshan Chattopadhyay and David Zuckerman. Explicit two-source extractors and resilient functions. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:119, 2015.

[Dod06] Yevgeniy Dodis. Fault-tolerant leader election and collective coin-flipping in the full information model, 2006.

[Fei99] Uriel Feige. Noncryptographic selection protocols. In *40th Annual Symposium on Foundations of Computer Science, FOCS '99, 17-18 October, 1999, New York, NY, USA*, pages 142–153, 1999.

[Gil98] David Gillman. A chernoff bound for random walks on expander graphs. *SIAM J. Comput.*, 27(4):1203–1220, 1998.

[Hea08] Alexander Healy. Randomness-efficient sampling within nc^1. *Computational Complexity*, 17(1):3–37, 2008.

[INW94] Russell Impagliazzo, Noam Nisan, and Avi Wigderson. Pseudorandomness for network algorithms. In *STOC*, pages 356–364, 1994.

[Kah97] Nabil Kahale. Large deviation bounds for markov chains. *Combinatorics, Probability & Computing*, 6(4):465–474, 1997.

[KKL88] Jeff Kahn, Gil Kalai, and Nathan Linial. The influence of variables on boolean functions (extended abstract). In *FOCS*, pages 68–80, 1988.

[KLW10] Adam R. Klivans, Homin K. Lee, and Andrew Wan. Mansour's conjecture is true for random DNF formulas. In *COLT*, pages 368–380, 2010.

[Li15] Xin Li. Three-source extractors for polylogarithmic min-entropy. *Electronic Colloquium on Computational Complexity (ECCC)*, 22:34, 2015.

[Mek09] Raghu Meka. Explicit coin flipping protocols, 2009. Unpublished manuscript.

[Nis92] Noam Nisan. Pseudorandom generators for space-bounded computation. *Combinatorica*, 12(4):449–461, 1992.

[NZ96] Noam Nisan and David Zuckerman. Randomness is linear in space. *J. Comput. Syst. Sci.*, 52(1):43–52, 1996.

[RSZ02] Alexander Russell, Michael E. Saks, and David Zuckerman. Lower bounds for leader election and collective coin-flipping in the perfect information model. *SIAM J. Comput.*, 31(6):1645–1662, 2002.

[RZ01] Alexander Russell and David Zuckerman. Perfect information leader election in log* n+o (1) rounds. *J. Comput. Syst. Sci.*, 63(4):612–626, 2001.

[Sak89] Michael E. Saks. A robust noncryptographic protocol for collective coin flipping. *SIAM J. Discrete Math.*, 2(2):240–244, 1989.

[Wik] Wikipedia. Prime gap — Wikipedia, the free encyclopedia.

[Zuc97] David Zuckerman. Randomness-optimal oblivious sampling. *Random Struct. Algorithms*, 11(4):345–367, 1997.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de