Quantum Random Access Codes for Boolean Functions

João F. Doriguello¹,² and Ashley Montanaro²,³

¹Quantum Engineering Centre for Doctoral Training, University of Bristol, United Kingdom
²School of Mathematics, University of Bristol, United Kingdom
³Phasecraft Ltd.

An $n \rightarrow m$ random access code (RAC) is an encoding of $n$ bits into $m$ bits such that any initial bit can be recovered with probability at least $p$, while in a quantum RAC (QRAC), the $n$ bits are encoded into $m$ qubits. Since its proposal, the idea of RACs was generalized in many different ways, e.g. allowing the use of shared entanglement (called entanglement-assisted random access code, or simply EARAC) or recovering multiple bits instead of one. In this paper we generalize the idea of RACs to recovering the value of a given Boolean function $f$ on any subset of fixed size of the initial bits, which we call $f$-random access codes. We study and give protocols for $f$-random access codes with classical ($f$-RAC) and quantum ($f$-QRAC) encoding, together with many different resources, e.g. private or shared randomness, shared entanglement ($f$-EARAC) and Popescu-Rohrlich boxes ($f$-PRRAC). The success probability of our protocols is characterized by the noise stability of the Boolean function $f$. Moreover, we give an upper bound on the success probability of any $f$-QRAC with shared randomness that matches its success probability up to a multiplicative constant (and $f$-RACs by extension), meaning that quantum protocols can only achieve a limited advantage over their classical counterparts.

1 Introduction

One of the possible origins of quantum computers' power is the exponential size of the Hilbert space: a $n$-qubit quantum state is a unit vector in a $2^n$ dimensional complex vector space. On the other hand, one of the fundamental results in quantum information theory – Holevo's theorem [29] – states that no more than $n$ bits of classical information can be transmitted by $n$ qubits without entanglement. Nonetheless, interesting scenarios arise when allowing a small chance of transmitting the wrong message or/and obtaining partial information at the expense of losing information about the rest of the system. One of these scenarios is the concept of quantum random access codes (QRACs), where a number of bits are encoded into a smaller number of qubits such that any one of the initial bits can be recovered with some probability of success. A QRAC is normally denoted by $n \rightarrow^p m$, meaning that $n$ bits are encoded into $m$ qubits such that any initial bit can be recovered with probability at least $p > 1/2$ (greater than $1/2$ since $p = 1/2$ can be achieved by pure guessing), and a classical version, called simply random access code (RAC), is similarly defined, with the encoding message being $m$ bits. The idea of QRACs first appeared in a paper by Stephen Wiesner [64] in 1983 under the name of conjugate coding, and was later rediscovered by Ambainis et al. in 1999 [4].

Quantum random access codes found application in many different contexts, e.g. quantum finite automata [4, 43], network coding [26, 27], quantum communication complexity [10, 22, 35], locally decodable codes [8, 33, 34, 62], non-local games [42, 60], cryptography [47], quantum state learning [1], device-independent dimension witnessing [2, 3, 63], self-testing measurements [19, 20].

João F. Doriguello: joaof.doriguello@gmail.com, http://joaodoriguello.com

Accepted in Quantum 2021-02-22, click title to verify. Published under CC-BY 4.0.
randomness expansion [38], studies of no-signaling resources [23], and characterization of quantum correlations from information theory [49]. The 2 \rightarrow 1 and 3 \rightarrow 1 QRACs were first experimentally demonstrated in [56]. See [21, 25, 42, 59, 61] for subsequent demonstrations.

In this paper we further generalize the idea of (quantum) random access codes to recovering not just an initial bit, but the value of a fixed Boolean function on any subset of the initial bits with fixed size. We call them \(f\)-random access codes. The case of the Parity function was already considered in [8], and here we generalize to arbitrary Boolean functions \(f : \{-1, 1\}^k \rightarrow \{-1, 1\}\).

### 1.1 Related Work

An \(n \xrightarrow{p} m\) (Q)RAC is an encoding of \(n\) bits into \(m\) (qu)bits such that any initial bit can be recovered with probability at least \(p\). This probability is the worst case success probability over all possible pairs \((x, i)\) of input string \(x \in \{-1, 1\}^n\) and recoverable bit \(i \in \{1, \ldots, n\}\). Many different resources can be used during the encoding and decoding, e.g. private randomness (PR), shared randomness (SR), shared entanglement, and even super-quantum correlations like Popescu-Rohrlich boxes [50].

Regarding the classical RAC, Ambainis et al. [4] proved that there is no \(2 \xrightarrow{1} 1\) RAC (and \(2^m \xrightarrow{1} m\) RAC by extension) with PR and worst case success probability \(p > 1/2\). On the other hand, Ambainis et al. [5] showed that RACs with SR can achieve success probability \(p > 1/2\).

**Theorem 1** ([5, Equation (25)]). The optimal \(n \xrightarrow{p} 1\) RAC with SR has success probability

\[
p = \frac{1}{2} + \frac{1}{2^n} \left( \frac{n-1}{n} \right) = \frac{1}{2} + \frac{1}{\sqrt{2\pi n}} - O\left(\frac{1}{n^{3/2}}\right).
\]

For a general number of encoded bits, Ambainis et al. [4] developed a RAC with PR using a specific code from [14] which matches their classical lower bound \(m \geq (1 - H(p))n\) up to an additive logarithmic term, where \(H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p)\) is the binary entropy function.

**Theorem 2** ([4, Theorem 2.2]). There is an \(n \xrightarrow{p} m\) RAC with PR and \(m \leq (1 - H(p))n + 7 \log_2 n\) for any \(p > \frac{1}{2}\).

As for QRACs, Ambainis et al. [4] showed the existence of a \(2 \xrightarrow{1} 1\) QRAC with PR\(^1\) and \(p = \frac{1}{2} + \frac{1}{2\sqrt{2}} \approx 0.85\), and the existence of a \(3 \xrightarrow{1} 1\) QRAC with PR and \(p = \frac{1}{2} + \frac{1}{2\sqrt{3}} \approx 0.79\) (the second attributed to Chuang). Later Hayashi et al. [26] showed the impossibility of a \(4 \xrightarrow{1} 1\) QRAC (and \(4^m \xrightarrow{1} m\) QRAC by extension) with PR and success probability \(p > 1/2\). Similarly to the classical case, Ambainis et al. [5] showed that QRACs can also benefit from SR.

**Theorem 3** ([5, Theorem 6]). There is an \(n \xrightarrow{p} 1\) QRAC with SR and \(^2\)

\[
p = \frac{1}{2} + \sqrt{\frac{2}{3\pi n}} + O\left(\frac{1}{n^{3/2}}\right).
\]

The specific case of \(m = 2\) encoding qubits was explored in [26, 31, 39]. For the general case of \(m > 1\), Iwama et al. [32] constructed an \((4^m - 1) \xrightarrow{1} m\) QRAC with PR and \(p = \frac{1}{2} + \frac{1}{2(2^m - 1)\sqrt{2^{m-1} + 1}}\) (such construction also works for all \(n < 4^m\)). On the other hand, Ambainis et al. [4] proved that if an \(n \xrightarrow{p} m\) QRAC with PR and \(p > 1/2\) exists, then \(m = \Omega(n/\log n)\), which was later improved to \(m \geq (1 - H(p))n\) by Nayak [43], thus matching the same classical lower bound from [4].

The idea of decoding a function of the initial bits instead of a single bit was already considered by Ben-Aroya, Regev and de Wolf [8] (who also considered recovering multiple bits rather than

---

\(^1\)Usually private randomness is already assumed in QRACs under the encoding onto density matrices.

\(^2\)Ambainis et al. [5] do not give the high order terms, but these can be calculated by following their procedure together with [30, Equation 2.198].
just one). More specifically, they defined an $n \xrightarrow{p} m$ XOR$_k$-QRAC, where $n$ bits are encoded into $m$ qubits such that the parity of any $k$ initial bits can be recovered with success probability at least $p$. Using their hypercontractive inequality for matrix-valued functions, they proved the following upper bound on the success probability.

**Theorem 4** ([8, Theorem 7]). For any $\eta > 2 \ln 2$ there is a constant $C_\eta$ such that, for any $n \xrightarrow{p} m$ XOR$_k$-QRAC with SR and $k = o(n)$,

$$p \leq \frac{1}{2} + C_\eta \left(\frac{mn}{n}\right)^{k/2}.$$  \hfill (1)

They conjectured that the factor $\eta > 2 \ln 2$ can be dropped from the above bound, and thus extended to $m/n > 1/(2 \ln 2) \approx 0.72$, although it might require a strengthening of their hypercontractive inequality.

The use of shared entanglement in random access codes was first considered by Klauck [35, 36]. Here the encoding and decoding parties are allowed to use an arbitrary amount of shared entangled states (note that shared entanglement can be used to obtain both private and shared randomness). The figure of merit in this generalization is the relation between $n$, $m$, and $p$, while the amount of shared entanglement is not taken into account. Klauck [35, 36] considered an $n \xrightarrow{p} m$ QRAC with shared entanglement and, by its equivalence to the quantum one-way communication complexity for the index function, proved the lower bound $m \geq (1 - H(p))n/2$, similar to Nayak's bound. Later Pawlowski and Żukowski [48] coined the term entanglement-assisted random access code (EARAC), which is a RAC with shared entanglement, and studied the case when $m = 1$, giving protocols with better decoding probabilities compared to the usual $n \xrightarrow{p} 1$ QRAC with SR. Recently Tănăsescu et al. [58] expanded the idea of $n \xrightarrow{p} 1$ EARACs to recovering an initial bit under a specific request distribution.

**Theorem 5** ([48] and [58, Corollary 2 and Theorem 5]). The optimal $n \xrightarrow{p} 1$ EARAC with SR has success probability

$$p = \frac{1}{2} + \frac{1}{2 \sqrt{n}}.$$

The idea of (Q)RAC was generalized in other ways, e.g. parity-oblivious [7, 13, 56] and multiparty [53] versions, encoding on $d$-valued qubits (qudits) [6, 12, 19, 39, 59], a wider range of information retrieval tasks [18] and a connection to Popescu-Rohrlich boxes. It was shown [66] that a Popescu-Rohrlich box can simulate a RAC by means of just one bit of communication, while in [23] the converse was proven. An object called racbox [23] was defined, which is a box that implements a RAC when supported with one bit of communication, and it was shown that a non-signaling racbox is equivalent to a Popescu-Rohrlich box. A quantum version of a racbox was later proposed in [24]. Finally, we mention that RACs were also studied within “theories” that violate the uncertainty relation for anti-commuting observables and present stronger-than-quantum correlations [57].

### 1.2 Our Results

This paper focuses on generalizing the classical, quantum and entanglement-assisted random access codes. Instead of recovering a single bit from the initial string $x \in \{-1,1\}^n$, we are interested in evaluating a Boolean function $f : \{-1,1\}^k \rightarrow \{-1,1\}$ on any sequence of $k$ bits from $x$. We generically call them $f$-random access codes. Let $S_k^k = \{(S_i)_{i=1}^k \in \{1, \ldots, n\}^k \mid S_i \neq S_j \forall i, j\}$ be the set of sequences of different elements from $\{1, \ldots, n\}$ with length $k$ and let $x_S \in \{-1,1\}^k$ denote the substring of $x \in \{-1,1\}^n$ specified by $S \in S_k^k$. Alice gets $x \in \{-1,1\}^n$ and she needs to encode her data and send it to Bob, so that he can decode $f(x_S)$ for any $S \in S_k^k$ with probability $p > 1/2$. Such problem was already considered by Sherstov in a two-way communication complexity

---

3In their definition the success probability is the average over random $k$-subsets and random inputs, which, in our context, is equivalent to using SR.
setting [54] and later used in his pattern matrix method [55] in order to prove other communication complexity lower bounds. Even though our results are expressed in a random access code language, they can also be seen as in a one-way communication complexity setting. If two-way communication is allowed, Bob can send the identity of his sequence to Alice with \(O(k \log n)\) bits of communication, whereas (as we will see) significantly more communication may be required in the one-way scenario.

In the following, \(\Pi\) will refer to a sample space with some probability distribution. As before, PR and SR stand for private and shared randomness, respectively. Moreover, since we require the success probability to always be greater than \(1/2\), given that one can always guess the correct result with probability \(1/2\), from now on it will be convenient to use the bias \(\varepsilon\) of the prediction, defined as \(\varepsilon = 2p - 1\), instead of its success probability \(p\).

We start with \(n \xrightarrow{\varepsilon} m\) f-RAC, the \(f\)-classical random access code on \(m\) bits with bias \(\varepsilon\).

**Definition 6.** An \(n \xrightarrow{\varepsilon} m\) f-RAC with PR is an encoding map \(E : \{-1,1\}^n \times \Pi_A \rightarrow \{-1,1\}^m\) satisfying the following: for every \(S \in \Delta^k_n\) there is a decoding map \(D_S : \{-1,1\}^m \times \Pi_B \rightarrow \{-1,1\}\) such that \(Pr_{r_A, r_B}[D_S(E(x, r_A), r_B) = f(x_S)] \geq \frac{1}{2} + \frac{\varepsilon}{2}\) for all \(x \in \{-1,1\}^n\).

**Definition 7.** An \(n \xrightarrow{\varepsilon} m\) f-RAC with SR is an encoding map \(E : \{-1,1\}^n \times \Pi \rightarrow \{-1,1\}^m\) satisfying the following: for every \(S \in \Delta^k_n\) there is a decoding map \(D_S : \{-1,1\}^m \times \Pi \rightarrow \{-1,1\}\) such that \(Pr_{r}[D_S(E(x, r)) = f(x_S)] \geq \frac{1}{2} + \frac{\varepsilon}{2}\) for all \(x \in \{-1,1\}^n\).

We define \(n \xrightarrow{\varepsilon} m\) f-QRAC, the \(f\)-quantum random access code on \(m\) qubits with bias \(\varepsilon\).

**Definition 8.** An \(n \xrightarrow{\varepsilon} m\) f-QRAC with PR is an encoding map \(E : \{-1,1\}^n \rightarrow \mathbb{C}^{2^m \times 2^m}\) that assigns an \(m\)-qubit density matrix to every \(x \in \{-1,1\}^n\) and satisfies the following: for every \(S \in \Delta^k_n\) there is a POVM \(M^S = \{M^S_{-1,x}, M^S_{1,x}\}\) such that \(\text{Tr}(M^S_{f(x_S)}, E(x)) \geq \frac{1}{2} + \frac{\varepsilon}{2}\) for all \(x \in \{-1,1\}^n\).

**Definition 9.** An \(n \xrightarrow{\varepsilon} m\) f-QRAC with SR is an encoding map \(E : \{-1,1\}^n \rightarrow \mathbb{C}^{2^m}\) that assigns an \(m\)-qubit pure state to every \(x \in \{-1,1\}^n\) and satisfies the following: for every \(S \in \Delta^k_n\) there is a set of POVMs \(\{M^S_r\}_{r \in \Pi}\), with \(M^S_{-1,x} = \{M^S_{-1,r}, M^S_{1,r}\}\), such that \(\mathbb{E}_r[E(x, r)\dagger M^S_{f(x_S)} E(x, r)] \geq \frac{1}{2} + \frac{\varepsilon}{2}\) for all \(x \in \{-1,1\}^n\).

Similarly, we define \(n \xrightarrow{\varepsilon} m\) f-EARAC, the \(f\)-entanglement-assisted random access code on \(m\) bits with bias \(\varepsilon\).

**Definition 10.** An \(n \xrightarrow{\varepsilon} m\) f-EARAC is an \(n \xrightarrow{\varepsilon} m\) f-RAC with SR where the encoding and decoding parties share an unlimited amount of entangled quantum states.

Due to shared entanglement being a source of SR, we already include SR in f-EARACs. We note that [48] focused on EARACs without SR.

Finally, we define \(n \xrightarrow{\varepsilon} m\) f-PRRAC, the \(f\)-Popescu-Rohrlich random access code on \(m\) bits with bias \(\varepsilon\). A Popescu-Rohrlich box [50] is a bipartite system shared by two parties with two inputs \(x, y \in \{0, 1\}\) and two outputs \(a, b \in \{0, 1\}\) and is defined by the joint probability distribution

\[
Pr[ab|xy] = \begin{cases} \frac{1}{2} & \text{for } a \oplus b = xy, \\ 0 & \text{otherwise}. \end{cases}
\]

**Definition 11.** An \(n \xrightarrow{\varepsilon} m\) f-PRRAC is an \(n \xrightarrow{\varepsilon} m\) f-RAC with SR where the encoding and decoding parties share an unlimited amount of Popescu-Rohrlich boxes.

In Section 3 we devise encoding-decoding strategies for all the \(f\)-random access codes just defined, thus deriving lower bounds on their biases given the encoding/decoding parameters \(n, m\) and \(k\). These \(f\)-random access codes are built based on previous ideas from [4, 5, 48]. The Boolean function \(f : \{-1,1\}^k \rightarrow \{-1,1\}\) that needs to be evaluated directly influences the final bias and such influence in our results is captured by the single quantity called noise stability [9, 45]. Informally it is a measure of how resilient to noise a Boolean function is. Given a uniformly random
input $x \in \{-1,1\}^n$, one might imagine a process that flips each bit of $x$ independently with some probability $\frac{1}{2} - \frac{1}{2}q$, where $q \in [-1, 1]$, which leads to some final string $y \in \{-1,1\}^n$. The noise stability $\text{Stab}_q[f]$ of $f$ with parameter $q$ is the correlation between $f(x)$ and $f(y)$ (see Section 2 for a formal definition).

Our positive results can be summarized by the following theorem.

**Theorem 12.** Let $f: \{-1,1\}^k \to \{-1,1\}$ be a Boolean function and $\text{Stab}_q[f]$ its noise stability with parameter $q$.

(a) Let $\ell \in \mathbb{N}$. If $m = \Omega(\ell \log n)$ and $k = o(\sqrt{\ell})$, there is an $n \mapsto m$ $f$-$\text{RAC}$ with $\text{PR}$ and bias $\epsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ with $q \geq \sqrt{\frac{m}{n}} - \frac{\log_2 (m/\ell)}{n/\ell}$.

(b) If $k = o(\sqrt{m})$, there is an $n \mapsto m$ $f$-$\text{RAC}$ with $\text{SR}$ and $\epsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ with $q \geq \sqrt{\frac{m}{n}} - \frac{\log_2 (m)}{n}$.

(c) If $k = o(\sqrt{m})$, there is an $n \mapsto m$ $f$-$\text{QRAC}$ with $\text{SR}$ and $\epsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ with $q \geq \sqrt{\frac{m}{n}} - \frac{\log_2 (m)}{n}$.

(d) If $k = o(\sqrt{m})$, there is an $n \mapsto m$ $f$-$\text{EARAC}$ with $\epsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ and $q = \sqrt{\frac{m}{n}}$.

(e) For any $n \in \mathbb{N}$, there is an $n \mapsto 1$ $1$-$f$-$\text{PRRAC}$.

Results (a), (b), (c) and (d) use an encoding scheme reminiscent of the concatenation idea from \cite{48,49,58} (and suggested to us by Ronald de Wolf). The underlying idea is to randomly break the initial string $x \in \{-1,1\}^n$ into different ‘blocks’ and encode them via a standard $\text{RAC}$/$\text{QRAC}$/$\text{EARAC}$. Result (a) breaks $x$ into $\ell$ blocks and employs the $n/\ell \mapsto m/\ell$ $\text{RAC}$ from Theorem 2 on every block, each with $n/\ell$ elements, while in results (b)/(c)/(d) we employ the $n/m \mapsto 1$ $\text{RAC}$/$\text{QRAC}$/$\text{EARAC}$ from Theorems 1/3/5 in order to encode $m$ blocks, each with $n/m$ elements, into a single (qu)bit each, resulting in $m$ encoded (qu)bits. With high probability all the bits from the needed string $x_S \in \{-1,1\}^k$ will be encoded into different blocks and therefore can be decoded and $f$ evaluated. The decoded string $y \in \{-1,1\}^k$ can be viewed as a ‘noisy’ $x_S$, to which the noise stability framework can be applied. The bias of the base $\text{RAC}$/$\text{QRAC}$/$\text{EARAC}$ thus becomes the parameter $q$ in the noise stability of the corresponding $f$-random access code. As a quick remark, since we opted to lower-bound the parameters $q$ in Theorem 12, in result (b) $q$ does not exactly equal the bias from Theorem 1. One could write, though, $q \approx \sqrt{\frac{2m}{n}}$.

Result (a) is our strongest bound, since it also applies to all other $f$-random access codes. Moreover, there is some freedom in setting the number of blocks $\ell$, since the number of encoded bits in Theorem 2 is not fixed to a single number (as opposed to Theorems 1, 3 and 5). The result is a trade-off between the number of bits $k$ of the Boolean function and the number of encoded bits $m$. However, the number of encoded bits in result (a) is limited to $m = \Omega(\log n)$, a characteristic inherited from the $\text{RAC}$ in Theorem 2. It is possible to go below this limit by using $\text{SR}$, as demonstrated by results (b), (c) and (d).

The above results show that quantum resources offer a modest advantage over the classical $f$-random access code. On the other hand, result (e) demonstrates that stronger-than-quantum resources like Popescu-Rohrlich boxes can lead to extremely powerful $f$-random access codes. This is a consequence of violating Information Causality \cite{49}, since one bit transfer allows the access to any bit in a database via Popescu-Rohrlich boxes. From $x \in \{-1,1\}^n$ a long bit-string $x_f \in \{-1,1\}^t$, where $t = |S_h^k|$, can be constructed with the values $f(x_S)$ for all $S \in S_h^k$. All bits from $x_f$ are readable with the aid of Popescu-Rohrlich boxes, with non-signaling constraining the readout to just one bit. The protocol for $f$-$\text{PRRACs}$ is taken from \cite{49} and uses a pyramid of Popescu-Rohrlich boxes and nests a van Dam’s protocol \cite{16}.

In Section 4 we prove an upper bound on the bias of any $f$-$\text{QRAC}$ with $\text{SR}$ (and $f$-$\text{RAC}$) using the same method of the hypercontractive inequality for matrix-valued functions from \cite{8}.
Theorem 13. Let \( f : \{-1, 1\}^k \to \{-1, 1\} \) be a Boolean function. For any \( n \to m \) \( f \)-QRAC with SR and \( k = o(n) \) the following holds: for any \( \eta > 2 \ln 2 \) there is a constant \( C_\eta \) such that

\[
\varepsilon \leq C_\eta \sum_{\ell=0}^k L_{1, \ell}(f) \left( \frac{\eta}{n} \right)^{\ell/2},
\]

where \( L_{1, \ell}(f) = \sum_{|T|=\ell} \left| \hat{f}(T) \right| \) is the 1-norm of the \( \ell \)-th level of the Fourier transform of \( f \).

One can see that the above result is a generalization of Theorem 4. Indeed, for Parity on \( k \) bits, \( L_{1, \ell}(\text{XOR}_k) = 1 \) iff \( \ell = k \), and so Eq. (1) is recovered. The following corollary from Theorem 13 helps to compare the bias upper bound to the bias lower bounds from Theorem 12.

Corollary 14. Let \( f : \{-1, 1\}^k \to \{-1, 1\} \) be a Boolean function. For any \( n \to m \) \( f \)-QRAC with SR and \( k = o(n) \) the following holds: for any \( \eta > 2 \ln 2 \) there is a constant \( C_\eta \) such that

\[
\varepsilon \leq C_\eta 2^{\deg(f)-1} \text{Stab}_q[f],
\]

where \( \deg(f) = \max\{|S| : \hat{f}(S) \neq 0\} \) is the degree of \( f \) and \( q = \sqrt{\frac{m}{n}} \).

Taking \( \deg(f) \) to be upper-bounded by a constant (for example, if \( k = O(1) \)), our upper bound matches our bias lower bounds for \( f \)-RAC/QRAC with SR up to a global multiplicative constant and a multiplicative constant \( \sqrt{\eta} \) in the parameter \( q \). We conjecture that the parameter \( q \) can be improved to \( \sqrt{\frac{m}{n}} \), which might require a stronger version of the hypercontractive inequality.

Other corollaries from Theorem 13 are derived in Section 4 and compared to our bias lower bounds.

Upper bound (2) does not apply to \( f \)-EARACs. Previously, it was known that for the special case of standard EARACs \( (m = 1) \), the bias \( \varepsilon \) is upper-bounded by \( 1/\sqrt{n} \) (Theorem 5). This upper bound can generalised to EARACs with \( m > 1 \) assuming an independence condition (Section 3.4). The resulting bound is \( \varepsilon \leq \sqrt{m/n} \). We view this as evidence that the bias lower bound for the general case of \( f \)-EARACs given in Theorem 12 should actually be tight.

Regarding the quantity \( \text{Stab}_q[f] \) itself, it can be nicely related to the Fourier coefficients of \( f \) (see Theorem 17 in the next section). We briefly mention the noise stability for a few functions. For Parity \( \langle \text{XOR}_k \rangle \), \( \text{Stab}_q[\text{XOR}_k] = q^k \), and, more generally, for any function \( \chi_S(x) = \prod_{i \in S} x_i \), \( \text{Stab}_q[\chi_S] = q^{|S|} \). As for the Majority function \( \langle \text{MAJ}_k \rangle \), one can show that \( 4 \arcsin q \leq \text{Stab}_q[\text{MAJ}_k] \leq 2 \arcsin q + O\left(\frac{1}{\sqrt{1-q^2}}\right)\). Other examples can be found in [41]. Moreover, a randomized algorithm for approximating the noise stability of monotone Boolean functions up to relative error was proposed in [52].

In Section 3 we present protocols for all our \( f \)-random access codes, and in Section 4 we derive an upper bound on the bias of \( f \)-QRACs with SR.

## 2 Preliminaries

We shall briefly revise some results from Boolean analysis that are going to be useful. For an introduction to the analysis of Boolean functions, see O’Donnell’s book [46] or de Wolf’s paper [65]. In the following, we write \( [n] = \{1, \ldots, n\} \) and \( S_n \) is the set of all permutations of \([n]\). As before, let \( S_n^k = \{S \in [n]^k : S_1 \neq S_2 \forall i, j \} \) be the set of sequences of different elements from \([n]\) with length \( k \) and let \( x_S \in \{-1, 1\}^k \) denote the substring of \( x \in \{-1, 1\}^n \) specified by \( S \in S_n^k \).

The inner product \( \langle \cdot, \cdot \rangle \) on the vector space of all functions \( f : \{-1, 1\}^n \to \mathbb{R} \) is defined by

\[
\langle f, g \rangle = \frac{1}{2^n} \sum_{x \in \{-1, 1\}^n} f(x) g(x).
\]

Every function \( f : \{-1, 1\}^n \to \mathbb{R} \) can be uniquely expressed as a multilinear polynomial, its Fourier expansion, as

\[
f(x) = \sum_{S \subseteq [n]} \hat{f}(S) \chi_S(x),
\]
where, for $S \subseteq [n]$, $\chi_S : \{-1, 1\}^n \to \{-1, 1\}$ is defined by

$$\chi_S(x) = \prod_{i \in S} x_i.$$ 

The real number $\hat{f}(S)$ is called the Fourier coefficient of $f$ on $S$ and is given by

$$\hat{f}(S) = \langle f, \chi_S \rangle = \frac{1}{2^n} \sum_{x \in \{-1, 1\}^n} f(x) \chi_S(x).$$

An important and useful concept for Boolean functions is noise stability. As previously mentioned, it is a measure of how resilient to noise a Boolean function is, and is defined from the concept of $q$-correlated pairs of random strings given below.

**Definition 15** ([46, Definitions 2.40 and 2.41]). Let $q \in [-1, 1]$. For fixed $x \in \{-1, 1\}^n$ we write $y \sim N_q(x)$ to denote that the random string $y$ is drawn as follows: for each $i \in [n]$ independently,

$$y_i = \begin{cases} x_i & \text{with probability } \frac{1}{2} + \frac{1}{2}q, \\ -x_i & \text{with probability } \frac{1}{2} - \frac{1}{2}q. \end{cases}$$

We say that $y$ is $q$-correlated to $x$. If $x \sim \{-1, 1\}^n$ is drawn uniformly at random and then $y \sim N_q(x)$, we say that $(x, y)$ is a $q$-correlated pair of random strings.

Given these definitions, we can formally define the concept of noise stability, which measures the correlation between $f(x)$ and $f(y)$ when $(x, y)$ is a $q$-correlated pair.

**Definition 16** ([46, Definition 2.42]). For $f : \{-1, 1\}^n \to \mathbb{R}$ and $q \in [-1, 1]$, the noise stability of $f$ at $q$ is

$$\text{Stab}_q[f] = \mathbb{E}_{(x, y) \sim \text{q-correlated}} [f(x)f(y)].$$

The noise stability of $f$ is nicely related to $f$’s Fourier coefficients as stated in the following theorem.

**Theorem 17** ([46, Theorem 2.49]). For $f : \{-1, 1\}^n \to \mathbb{R}$ and $q \in [-1, 1]$,

$$\text{Stab}_q[f] = \sum_{k=0}^{n} q^k W^k[f],$$

where $W^k[f] = \sum_{|S| = k} \hat{f}(S)^2$ is the Fourier weight of $f$ at degree $k$.

The above result makes it clear that $\text{Stab}_q[f]$ is an increasing function of $q$ for $q \geq 0$.

Theorem 17 is obtained from one of the most important operators in analysis of Boolean functions: the noise operator $T_q$.

**Definition 18** ([46, Definition 2.46]). For $q \in [-1, 1]$, the noise operator with parameter $q$ is the linear operator $T_q$ on functions $f : \{-1, 1\}^n \to \mathbb{R}$ defined by

$$T_q f(x) = \mathbb{E}_{y \sim N_q(x)} [f(y)].$$

**Proposition 19** ([46, Proposition 2.47]). For $f : \{-1, 1\}^n \to \mathbb{R}$, the Fourier expansion of $T_q f$ is

$$T_q f = \sum_{S \subseteq [n]} q^{|S|} \hat{f}(S) \chi_S.$$
It is not hard to prove from the above results that 
\( \text{Stab}_q[f] = \langle f, T_q f \rangle \).

Some of the above concepts can be generalized to matrix-valued functions. The Fourier transform \( f \) of a matrix-valued function \( f : \{−1, 1\}^n \rightarrow \mathbb{C}^{m \times m} \) is defined similarly as for scalar functions: it is the function \( \hat{f} : \{−1, 1\}^n \rightarrow \mathbb{C}^{m \times m} \) defined by
\[
\hat{f}(S) = \frac{1}{2^n} \sum_{x \in \{−1, 1\}^n} f(x) \chi_S(x).
\]

Here the Fourier coefficients \( \hat{f}(S) \) are also \( m \times m \) complex matrices. Moreover, given \( A \in \mathbb{C}^{m \times m} \) with singular values \( \sigma_1, \ldots, \sigma_m \), its trace norm is defined as \( \|A\|_{\text{tr}} = \text{Tr}|A| = \sum_{i=1}^{m} \sigma_i \).

We shall make use of the following result from Ben-Aroya, Regev and de Wolf [8], which stems from their hypercontractive inequality for matrix-valued functions.

**Theorem 20** ([8, Lemma 6]). For every \( f : \{−1, 1\}^n \rightarrow \mathbb{C}^{2^m \times 2^m} \) and \( \delta \in [0, 1] \),
\[
\sum_{S \subseteq [n]} 2^{\|S\|} \|\hat{f}(S)\|_{\text{tr}}^2 \leq 2^{2\delta m}.
\]

Finally, \( H : [0, 1] \rightarrow [0, 1] \) given by \( H(p) = -p \log_2 p - (1 - p) \log_2 (1 - p) \) is the binary entropy function. The following bounds hold.

**Theorem 21** ([11, Theorem 2.2]). \( \forall p \in [0, 1], 1 - 4 \left( p - \frac{1}{2} \right)^2 \leq H(p) \leq 1 - \frac{4}{m^2} \left( p - \frac{1}{2} \right)^2 \).

### 3 Bias Lower Bounds

#### 3.1 \( f \)-RAC with PR

We start by studying the \( f \)-RAC with PR. The following result is based on Ambainis et al. [4] and uses a procedure reminiscent of the concatenation idea from [48, 49, 58]: the initial string is broken in blocks, which in turn are encoded using the code from [14]. First we state a slightly modified version of Newman’s Theorem [44] (see also [37, Theorem 3.14] and [51, Theorem 3.5]) which is going to be useful to us.

**Theorem 22** ([44]). Let \( \mathcal{E}(x, r) \) be an event depending on \( x \in \{−1, 1\}^n \times \{−1, 1\}^n \) and \( r \in R \) such that
\[
\Pr_{x \sim_R} [\mathcal{E}(x, r)] \geq p
\]
for all \( x \in \{−1, 1\}^n \times \{−1, 1\}^n \), with \( p \in (0, 1) \). Let \( \delta \in (0, p] \). Then there is \( R_0 \subseteq R \) with size at most \( n/\delta^2 \) such that
\[
\Pr_{r \sim_{R_0}} [\mathcal{E}(x, r)] \geq p - \delta
\]
holds for all \( x \in \{−1, 1\}^n \times \{−1, 1\}^n \).

**Theorem 23.** Let \( \ell \in \mathbb{N}, \ell|n, m = \Omega(\ell \log n) \) and \( k = o(\sqrt{\ell}) \). Let \( f : \{−1, 1\}^k \rightarrow \{−1, 1\} \) be a Boolean function. For sufficiently large \( n \) and \( \ell \), there is an \( n \mapsto m \) \( f \)-RAC with PR and bias \( \varepsilon \geq (1 - o_n(1)) \text{Stab}_q[f] \) with
\[
q \geq \sqrt{\frac{m}{n} - \frac{5\log_2 (n/\ell)}{n/\ell}}.
\]

**Proof.** Consider a code \( C \subseteq \{−1, 1\}^n \) such that, for every \( x \in \{−1, 1\}^n \), there is a \( y \in C \) within Hamming distance \( (1 - p - \frac{1}{n})n \), with \( p > 1/2 \) (the extra \( 1/n \) term will be used to counterbalance
the decrease in probability from Newman’s theorem. It is known [14] that there is such a code $C$
of size

$$\log_2 |C| = (1 - H(p + 1/n)) n + 2 \log_2 n \leq (1 - H(p)) n + 4 \log_2 n.$$ 

Let $C(x)$ denote the closest codeword to $x$. Hence at least $(p + 1/n)n$ out of $n$ bits of $C(x)$ are the same as $x$, and the probability over a uniformly random $i$ that $x_i = C(x_i)$, is at least $p + 1/n$.

Let $\ell \in \mathbb{N}$ such that $\ell$ divides $n$. Our protocol involves breaking up $x \in \{-1, 1\}^n$ into $\ell$ parts and encoding each part with the above code $C \subseteq \{-1, 1\}^{n/\ell}$. Define the map

$$C^{(\ell)}(x) = C(x_1 \ldots x_{n/\ell}) C(x_{n/\ell+1} \ldots x_{2n/\ell}) \ldots C(x_{(\ell-1)n/\ell+1} \ldots x_n)$$

that applies $C$ to the first $\ell$ bits of $x$, and to next $\ell$ bits of $x$ and so on. Hence the probability that $x_i = C^{(\ell)}(x)$ over a uniformly random $i$ is at least $p + \ell/n$. In order to consider this probability for every bit instead of just an average over all bits, we employ the following randomization process. Let $r \in \{-1, 1\}^n$ and $\pi \in S_n$, both taken uniformly at random. Given $x \in \{-1, 1\}^n$, denote $\pi(x) = x_{\pi(1)} x_{\pi(2)} \ldots x_{\pi(n)}$. We define the encoding $C^{(\ell)}(\pi(x \cdot r)) \cdot r$, where $x \cdot r$ denotes the bit-wise product of $x$ and $r$. Let $\mathcal{E}_S$ be the event that all indices in $S \in \delta_k^h$ are encoded in different codes $C$, i.e., in different blocks from $C^{(\ell)}$. There are $\ell$ blocks, each with $n/\ell$ elements. The probability that $k$ specific elements fall into $k$ different blocks is

$$\Pr_{S \sim \delta_k^h}[\mathcal{E}_S] = \left( \binom{n}{k} \frac{k}{\ell} \right)^k \prod_{j=1}^{k-1} \left( 1 - \frac{j}{n} \right) \geq \prod_{j=1}^{k-1} \left( 1 - \frac{j}{\ell} \right)^{\binom{\ell}{k}} = 1 - \frac{k(k-1)}{2\ell}, \quad (3)$$

where inequality (a) can easily be proven by induction or the union bound.

We shall first present a protocol using shared randomness, and at the end we shall transform it into a protocol with private randomness by using Newman’s theorem. The protocol is the following. Select $\pi \in \{-1, 1\}^n$ and $\pi \in S_n$ uniformly at random. Encode $x$ as $C^{(\ell)}(x)$. To decode $f(x_S)$, first we check if all the indices of $S$ are encoded into different blocks. If no, the value for $f(x_S)$ is drawn uniformly at random. If yes, just consider $C^{(\ell)}(\pi(x \cdot r)) \cdot r$ and evaluate $f(C^{(\ell)}(\pi(x \cdot r)))$. Conditioned on the event $\mathcal{E}_S$, happening, the probability that $x_{S_i} = C^{(\ell)}(x_{S_i})$ is at least $p + \ell/n$ independently for all $i \in [k]$, meaning that

$$\Pr_{\pi, r}[f(x_S) = f(C^{(\ell)}(\pi(x) \cdot r)) | \mathcal{E}_S] \geq \Pr_{(x, y)}[f(x) = f(y)] = \frac{1}{2} + \frac{1}{2} \text{Stab}_{q, \frac{2}{\ell}}[f], \quad \text{(q}^\perp\text{-correlated)}$$

where $q := 2p - 1$, and the inequality follows from monotonicity of the noise stability of $f$. With these considerations, the success probability of the protocol is

$$\Pr_{\pi, r}[f(x_S) = f(C^{(\ell)}(\pi(x) \cdot r)) S] \geq \frac{1}{2} \left( 1 - \frac{k(k-1)}{2\ell} \right) \left( \frac{1}{2} + \frac{1}{2} \text{Stab}_{q, \frac{2}{\ell}}[f] \right)$$

$$\geq \frac{1}{2} + \frac{1}{2} \left( 1 - \frac{k(k-1)}{2\ell} \right) \left( \text{Stab}_{q}[f] + \text{Stab}_{\frac{2}{\ell}}[f] \right)$$

$$= \frac{1}{2} + \frac{1}{2} (1 - o_n(1)) \left( \text{Stab}_{q}[f] + \text{Stab}_{\frac{2}{\ell}}[f] \right),$$

where we used that $k = o(\sqrt{\ell})$.

We now transform the shared randomness into private randomness. By Newman’s theorem (Theorem 22) there is a small set of permutation-string pairs (note that Alice’s input is size $n$ bits and Bob’s input is at most $n$ bits) with size

$$l \leq \frac{4n}{(1 - o_n(1)) \text{Stab}_{\frac{2}{\ell}}[f]^2} \leq \frac{n^{2k+1}}{(1 - o_n(1)) 2^{2k - 2\ell^2}},$$

(we have used that $\text{Stab}_{q}[f] \geq a^k$) such that $f(x_S) = f(C^{(\ell)}(\pi(x) \cdot r))$ continues to hold with probability at least $\frac{1}{2} + \frac{1}{2} (1 - o_n(1)) \text{Stab}_{\frac{2}{\ell}}[f]$ if $\pi, r$ are chosen uniformly at random from this set. Hence the
randomization can be encoded together with $x$ at the cost of a small overhead. The final protocol chooses $j \in [t]$ uniformly at random, encodes $x$ as $C_{\pi_j, r_j}(x)_S$ and then proceeds like the protocol with shared randomness. Fix $m = \log_2(t|C|)$. The result follows by using the first inequality from Theorem 21 to observe that

$$m \leq (1 - H(p))n + 4\ell \log_2 n + 2\ell \log_2 \frac{n^{2k+1}}{n} \leq q^2 \ell n + 4(1 + o_\ell(1))\ell \log_2 \frac{n}{\ell} \implies 2p - 1 \geq \sqrt{\frac{m - 4(1 + o_\ell(1))\ell \log_2 (n/\ell)}{n/\ell}}$$

for sufficiently large $n$, where we used $k = o(\sqrt{\ell})$ again.

**Remark.** The parameter $\ell$ in Theorem 23 controls the number of encoding blocks in the protocol. By tweaking it, we can adjust the range of $m$ and $k$, e.g. if $\ell = \Theta(\log n)$, then $m = \Omega(\log^2 n)$ and $k = o(\sqrt{\log n})$ If $\ell = \Theta(\sqrt{n})$, then $m = \Omega(\sqrt{n} \log n)$ and $k = o(n^{1/4})$.

In the protocol from Theorem 23 we broke the initial string into $\ell$ different blocks and used $\ell$ different copies of $C$. This was done in order to guarantee the independence of the $C(x)_S_i$’s and hence analyse the influence of the code $C$ on the function $f$. Interestingly enough, for the special case of the Parity function this is not required and a single copy of $C$ can be used.

**Theorem 24.** Let $\text{XOR}_k : \{-1,1\}^k \to \{-1,1\}$ be the Parity function and let $m = \Omega(k \log n)$.

There is an $n \xrightarrow{\varepsilon} m$ XOR$_{k}$-RAC with PR and bias $\varepsilon \geq 1 \left(\frac{m}{n}\right) H_{k,n} \left(\frac{n}{2} \sqrt{\frac{m - 7k \log_2 n}{n}}\right)$, (4)

where $H_{k,n}(x) = \sum_{j=0}^{k}(-1)^{j} \binom{n-j}{k-j}$ is the Krawtchouk polynomial.

**Proof.** Consider the encoding $C_{\pi, r}(x) = \pi^{-1}(C(\pi(x \cdot r))) \cdot r$, where $C \subseteq \{-1,1\}^n$ is the code described in Theorem 23. Let $\delta n$ be the Hamming distance between $x$ and $C(x)$, with $\delta \leq 1 - p - 1/n$ by the properties of $C$. Then

$$\Pr_{S \sim \text{RAC}} \left[ \prod_{i=1}^{k} x_{S_i} = \prod_{i=1}^{k} C(x)_{S_i} \right] = \sum_{\ell=0}^{\frac{m}{7k \log_2 n}} \binom{k}{\ell} \binom{n}{\frac{m}{7k \log_2 n}} = 1 + \frac{1}{2} \frac{\ell \log_2 n}{n} \frac{1}{\ell} \frac{1}{(\frac{n}{k})} + \frac{1}{(\frac{n}{k})}$$

where we used $\sum_{\ell=0}^{\frac{m}{7k \log_2 n}} (-1)^{\ell} \binom{n}{\ell} = \binom{n}{k}$ on the second equality and $H_{k,n}(\delta n) - H_{k,n}(\delta n + 1) = 2$ on the final inequality, which can be obtained via the recurrence relation $H_{k,n}(x) = H_{k,n}(x - 1) - H_{k-1,n}(x - 1)$ and $H_{1,n}(x) = n - 2x$ (see e.g. [15]).

By Newman’s theorem (Theorem 22) there is a small set of permutation-string pairs with size $t = n \binom{2t}{n}$ such that $\prod_{i=1}^{k} x_{S_i} = \prod_{i=1}^{k} C(x)_{S_i}$ continues to hold with bias at least $H_{k,n}((1 - p)n)/\binom{n}{k}$ for any $x$ and $S$ if $\pi, r$ are chosen uniformly at random from this set.

Our protocol is the following. Select $j \in [t]$ uniformly at random. Encode $x$ as $C_{\pi_j, r_j}(x)$. To decode $\prod_{i=1}^{k} x_{S_i}$, just consider $C_{\pi_j, r_j}(x)_S$ and evaluate $\prod_{i=1}^{k} C_{\pi_j, r_j}(x)_{S_i}$. Now fix $m = \log_2(t|C|)$. The result follows by using the first inequality from Theorem 21 to observe that

$$m \leq (1 - H(p))n + 5 \log_2 n + 2 \log_2 \left(\frac{n}{k}\right) \implies 1 - p \leq 1 \left(\frac{m}{n}\right) \frac{7k \log_2 n}{n}.$$

**Remark.** Since $H_{k,n}(x) = n - 2x$, we note that, for $k = 1$, Eq. (4) reduces to $\varepsilon \geq \sqrt{\frac{m}{n} - \frac{7k \log_2 n}{n}}$, which is the result from Ambainis et al. [4] (see Theorem 2).

**Remark.** If $k = O(1)$, then the Krawtchouk polynomial has the asymptotic limit as $n \to \infty$ of $H_{k,n}(x) \sim \frac{2^k x^k}{k!} \left(\frac{1}{2} - \frac{x}{n}\right)^k$ [17, Eq. (29)], thus the bias from Theorem 24 has the asymptotic limit

$$\varepsilon \sim \frac{n^k}{k! \binom{n}{k}} \left(\frac{m}{n} - \frac{7k \log_2 n}{n}\right)^{k/2} \geq \left(\frac{m}{n} - \frac{7k \log_2 n}{n}\right)^{k/2}. $$
Note that this result is very similar to the one that would follow from Theorem 23, but slightly
tighter (without the \( \ell \) parameter and the multiplicative constant \( 1 - o_n(1) \)).

### 3.2 \( f \)-RAC with SR

There is a lower limit of \( m = \Omega(\log n) \) on the number of encoded bits in Theorem 23. It is possible
to go below this limit by using SR: the blocks are now encoded via the \( n \to 1 \) RAC with SR from
Theorem 1 instead of the code \( C \).

**Theorem 25.** Let \( m/n \) and \( k = o(\sqrt{m}) \). Let \( f : \{-1, 1\}^k \to \{-1, 1\} \) be a Boolean function. There
is an \( n \to m \) \( f \)-RAC with SR and bias \( \varepsilon \geq (1 - o_n(1)) \mathbf{Stab}_q[f] \) with

\[
q = \frac{2}{2n/m} \left( \frac{n/m - 1}{2} \right) \geq \left\{ \begin{aligned}
\sqrt{\frac{2n}{\pi n}} = O \left( \frac{1}{(n/m)^{\varepsilon/4}} \right), \\
\sqrt{\frac{2n}{\pi n}}.
\end{aligned} \right.
\]

**Proof.** Consider the RAC with SR from Theorem 1. Our protocol is the following. For the encoding
of \( x \in \{-1, 1\}^n \), its \( n \) bits are randomly divided into \( m \) sets \( T_1, \ldots, T_m \), each with \( n/m \) elements.
Each set is encoded into 1 bit with the \( n/m \to 1 \) RAC, and the encoded string is \( E(x) \in \{-1, 1\}^m \).
For decoding, one checks with the help of SR if all the \( k \) indices in \( S \) were encoded into different
sets. If no, the value for \( f(x_S) \) is drawn uniformly at random. If yes, let \( D_i : \{-1, 1\} \to \{-1, 1\} \)
be the decoding function for set \( T_i \), which corresponds to bit \( E(x)_i \). Then \( z_{\ell_i} := D_{\ell_i}(E(x)_{\ell_i}) \) is
the decoded \( x_{\ell_i} \), where, for all \( i \in [k], \ell_i \in [m] \) is such that \( S_i \in T_{\ell_i} \). Write \( z_T = z_{\ell_1} \ldots z_{\ell_k} \). We
output \( f(z_T) \) for \( f(x_S) \).

Let \( \mathcal{E}_S \) be the event that all indices in \( S \in \Delta_n^k \) are encoded in different sets. Similarly to Eq. (3),

\[
\Pr_{S \sim \Delta_n^k} [\tilde{\mathcal{E}}_S] \geq 1 - \frac{k(k - 1)}{2m}.
\]

The bias of correctly recovering any of the \( n/m \) encoded bits is \( q = \frac{2}{2n/m} \left( \frac{n/m - 1}{2} \right) \) by Theorem 1.
Conditioning on \( \mathcal{E}_S \) happening, we see that \( x_S \) and \( y_T \) are \( q \)-correlated according to Definition 15. Therefore

\[
\Pr_{T_1, \ldots, T_m} [f(x_S) = f(z_T) | \mathcal{E}_S] = \Pr_{(x, y) \sim q\text{-correlated}} [f(x) = f(y)] = \frac{1}{2} + \frac{1}{2} \mathbf{Stab}_q[f],
\]

where we used an input randomization via SR. With these considerations, the success probability
of the protocol is

\[
\Pr_{T_1, \ldots, T_m} [f(x_S) = f(z_T)] \geq \frac{1}{2} \frac{k(k - 1)}{2m} + \left( 1 - \frac{k(k - 1)}{2m} \right) \frac{1}{2} \frac{1}{2} \mathbf{Stab}_q[f]
\]

\[
= \frac{1}{2} + \frac{1}{2} \left( 1 - \frac{k(k - 1)}{2m} \right) \mathbf{Stab}_q[f]
\]

\[
= \frac{1}{2} + \frac{1}{2} (1 - o_n(1)) \mathbf{Stab}_q[f],
\]

using that \( k = o(\sqrt{m}) \), from where the result follows by noticing that

\[
q = \frac{2}{2n/m} \left( \frac{n/m - 1}{2} \right) \geq \left\{ \begin{aligned}
\sqrt{\frac{2n}{\pi n}} = O \left( \frac{1}{(n/m)^{\varepsilon/4}} \right), \\
\sqrt{\frac{2n}{\pi n}}.
\end{aligned} \right.
\]

with \( n! = \sqrt{2\pi n}(n/e)^n(1 + O(1/n)) \) and \( \left( \frac{2^n}{n!} \right) \geq 2^{2n}/(2\sqrt{n}) \) [40, Chapter 10, Lemma 7].

---

\(^4\)The decoding map of the RAC from Theorem 1 (see [5, Theorem 2]) is just the identity map, so \( z_{\ell_i} = E(x)_{\ell_i} \).
Remark. It is possible to use Newman’s theorem in the above theorem in order to transform SR into PR, but then $\Omega(\log n)$ encoding bits would need to be used to encode the randomization procedure, thus leading to $m = \Omega(\log n)$. Moreover, the final $f$-RAC would have worse bias compared to the one from Theorem 23.

Remark. The requirement $m \mid n$ can be dropped by adding extra bits into $x \in \{-1,1\}^n$ until $m \mid n'$, where $n'$ is the final number of bits.

Remark. For $m = n/2$ or $m = n/3$, we have $\frac{2}{\pi^2} \left( \frac{n/m-1}{n/m-1} \right) = \frac{1}{2}$, so the resulting biases have $q_{m=n/2} = q_{m=n/3} = 1/2$. Also, by using induction, $\frac{2}{\pi^2} \left( \frac{n-1}{n-1} \right) \leq \frac{1}{2}$ for any $n \geq 2$.

### 3.3 $f$-QRAC

Exactly the same procedure from Theorem 25 holds for $f$-QRACs if we replace the $n/m \mapsto 1$ RAC from Theorem 17 with the $n/m \mapsto 1$ QRA from Theorem 3 when encoding the sets $T_1, \ldots, T_m$.

**Theorem 26.** Let $m \mid n$ and $k = o(\sqrt{m})$. Let $f : \{-1,1\}^k \rightarrow \{-1,1\}$ be a Boolean function. There is an $n \mapsto m$ $f$-QRAC with SR and bias $\varepsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ with

$$q = \sqrt{\frac{8m}{3\pi n} + O \left( \frac{1}{(n/m)^{3/2}} \right)}.$$  

**Proof.** Replace the $n/m \mapsto 1$ RAC in the proof of Theorem 25 with the $n/m \mapsto 1$ QRA from Theorem 3 with bias $\varepsilon = \sqrt{\frac{8m}{3\pi n} + O \left( \frac{1}{(n/m)^{3/2}} \right)}$.  

**Remark.** If $m = n/2$ or $m = n/3$, the usual (and optimal) $2^{1/\sqrt{2}} \rightarrow 1$ QRA or $3^{1/\sqrt{3}} \rightarrow 1$ QRA with PR can be used, respectively. The resulting biases have $q_{m=n/2} = 1/\sqrt{2}$ and $q_{m=n/3} = 1/\sqrt{3}$.

### 3.4 $f$-EARAC

The same protocol can also be used for $f$-EARACs, now with the $n/m \mapsto 1$ EARAC from Theorem 5.

**Theorem 27.** Let $m \mid n$ and $k = o(\sqrt{m})$. Let $f : \{-1,1\}^k \rightarrow \{-1,1\}$ be a Boolean function. There is an $n \mapsto m$ $f$-EARAC with bias $\varepsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ and

$$q = \sqrt{\frac{m}{n}}.$$  

**Proof.** Replace the $n/m \mapsto 1$ RAC in the proof of Theorem 25 with the $n/m \mapsto 1$ EARAC from Theorem 5 with bias $\varepsilon = \sqrt{m/n}$.  

**Remark.** We could also define an entanglement-assisted $f$-QRAC ($f$-EAQRAC) similarly to Definition 10, i.e., as an $f$-QRAC with SR where both parties share an unlimited amount of entanglement. Due to super-dense coding and teleportation, an $n \mapsto m$ $f$-EAQRAC is equivalent to an $n \mapsto 2m$ $f$-EARAC, meaning that there is an $n \mapsto m$ $f$-EAQRAC with $k = o(\sqrt{m})$ and bias $\varepsilon \geq (1 - o_n(1)) \text{Stab}_q[f]$ with $q = \sqrt{\frac{2m}{m}}$.

If $f : \{-1,1\} \rightarrow \{-1,1\}$ is $f(x) = x$, i.e., when considering the usual $n \mapsto m$ EARAC, the above result tells us that the success probability is just

$$p = \frac{1}{2} + \frac{1}{2} \sqrt{\frac{m}{n}}. \quad (5)$$

Moreover, we note that the $n \mapsto m$ EARAC is formed by a grouping of $n/m \mapsto 1$ EARACs, such that the $m$ outcomes, i.e., the bits of the encoding message $E(x) \in \{-1,1\}^m$, are all independent of each other. More precisely, for each $i \in [n]$, there is a unique $j \in [m]$ such that $\text{Pr}[x_i|E(x)] = \frac{1}{2}$.
Pr[x_i|E(x)_j]. Under this assumption, we can prove that Eq. (5) is optimal by the optimality of its parts. Consider breaking the initial string $x \in \{-1,1\}^n$ into $m$ blocks, the $i$-th block containing $r_i$ elements. Then the success probability of the resulting $n \mapsto m$ EARAC is

$$\sum_{i=1}^{m} \frac{r_i}{n} \left(1 + \frac{1}{2^{r_i}}\right) = \frac{1}{2} + \frac{1}{2n} \sum_{i=1}^{m} \sqrt{r_i},$$

which is maximized by taking $r_i = n/m$ for all $i \in [m]$. Since the $n/m \mapsto 1$ EARACs are optimal by Theorem 5, so is Eq. (5) (under the assumption that the $n \mapsto m$ EARAC is formed by $m$ independent EARACs on 1 encoding bit).

We can use Theorem 17 to obtain the following corollary from Theorems 23, 25, 26 and 27.

**Corollary 28.** Let $f : \{-1,1\}^k \to \{-1,1\}$ be a Boolean function with pure high degree $h = \min\{|S| : \hat{f}(S) \neq 0\}$. Let $W^f[f] = \sum_{S \subseteq [k]} \hat{f}(S)^2$.

(a) Let $\ell \in \mathbb{N}$, $m = \Omega(\ell \log n)$ and $k = o(\sqrt{n})$. There is an $n \mapsto m$ $f$-RAC with PR and bias $\varepsilon \geq (1 - o_n(1)) W^f[f] \left(\frac{m}{n}\right)^{\frac{h}{2}}$.

(b) Let $k = o(\sqrt{n})$. There is an $n \mapsto m$ $f$-RAC with SR and bias $\varepsilon \geq (1 - o_n(1)) W^f[f] \left(\frac{m}{n}\right)^{\frac{h}{2}}$.

(c) Let $k = o(\sqrt{n})$. There is an $n \mapsto m$ $f$-QRAC with SR and bias $\varepsilon \geq (1 - o_n(1)) W^f[f] \left(\frac{m}{n}\right)^{\frac{h}{2}}$.

(d) Let $k = o(\sqrt{n})$. There is an $n \mapsto m$ $f$-EARAC with bias $\varepsilon \geq (1 - o_n(1)) W^f[f] \left(\frac{m}{n}\right)^{\frac{h}{2}}$.

3.5 $f$-P RRAC

We now present a protocol for the $f$-P RRAC, based on reducing the problem to the standard random access code setting, and then using a protocol defined in [49]. This protocol was used to show the violation of information causality by means of a pyramid of Popescu-Rohrlich boxes and nesting van Dam’s protocol [16], which allows us to decode the value of $f(x_S)$ for any $S \in \mathcal{B}_n$ with just one encoded bit. This procedure of pyramiding and nesting was also used in the context of EARACs in [48, 58] under the name of concatenation.

**Theorem 29.** Let $f : \{-1,1\}^k \to \{-1,1\}$ be a Boolean function. For any $n \in \mathbb{N}$, there is an $n \mapsto 1$ $f$-P RRAC.

**Proof.** To ease the notation, we shall use $\{0,1\}$ instead of $\{-1,1\}$ during the proof. We shall also name the encoding and decoding parties Alice and Bob, respectively, and refer to a Popescu-Rohrlich box as PR-box. Let $t := |S|^t = k^t \binom{n}{k}$ and define the string $a \in \{0,1\}^t$ as $a_S := f(x_S)$, where $S^t_n$ is arranged in lexicographic order.\(^5\) Bob is interested in bit $a_S$, whose index position can be described by a $t$-bit string $b = \sum_{i=0}^{t-1} b_i 2^i$, i.e., the considered function is $g_t(a,b) := a_b$. The remainder of the argument is the same as the protocol of [49], but we include the details for completeness. For $t = 1$ we have that

$$g_t((a_0,a_1),b_0) = a_0 \oplus b_0 (a_0 \oplus a_1).$$

Alice inputs $a_0 \oplus a_1$ into a PR-box, while Bob inputs $b_0$. Alice obtains the output $A$ and sends the message $y = a_0 \oplus A$ to Bob, who can obtain $y \oplus B = a_b$ using his output $B$, since, by the PR-box property, $A \oplus B = b_0 (a_0 \oplus a_1)$.

For $t > 1$, write $a = a'a''$, where $a' = a_0 \ldots a_{t/2-1} \in \{0,1\}^{t/2}$ and $a'' = a_{t/2} \ldots a_{t-1} \in \{0,1\}^{t/2}$. Then one can show that

$$g_t(a,b) = g_{t-1}(a',b') \oplus b_{t-1} (g_{t-1}(a',b') \oplus g_{t-1}(a'',b')).$$

\(^5\)If $f$ is symmetric, the size $t$ can be decreased to $\binom{n}{k}$ by ignoring all the redundant permutations of the $k$-sets.

\(^6\)Here we use $a_S$ to denote a single bit of $a$, whereas $x_S$ denotes a subsequence of $x$. 

Accepted in Quantum 2021-02-22, click title to verify. Published under CC-BY 4.0.
where \( b' = b_0, \ldots, b_{t-2} \in \{0,1\}^{t-1} \). Therefore we can construct a recursive protocol in \( t \), which will encompass all values of \( n \). The protocol uses a pyramid of \( 2^t - 1 \) Popescu-Rohrlich boxes placed on \( t \) levels. The case \( t = 1 \) was explained above. For \( t > 1 \), Alice and Bob use the protocol on inputs \( (a', b') \) and \( (a'', b') \), which involves \( 2^{t/2} - 1 \) PR-boxes in each one. Alice’s outputs of each protocol are \( y' \) and \( y'' \), which she inputs into the last PR-box, similarly to the case \( t = 1 \), as \( y' \oplus y'' \), while Bob inputs \( b_{t-1} \). Given Alice’s final output \( \rho \), she sends \( y = y' \oplus y'' \) to Bob, who uses his output \( B_{t-1} \) to obtain \( y' \oplus b_{t-1} (y' \oplus y'') \). If \( b_{t-1} = 0 \), he gets \( y' \), otherwise, if \( b_{t-1} = 1 \), he gets \( y'' \). With these, he can recursively go up the pyramid based on the protocol for \( t - 1 \) bits, which tells him which boxes to read. Looking at the binary decomposition of \( b \), Bob goes \( (t - r) \) times to the left bit, and \( r \) times to the right bit, where \( r = \sum_{i=0}^{t-1} b_i \). His final output will be \( y \oplus B_0 \oplus \cdots \oplus B_{t-1} \), where \( B_j \) is the output for the PR-box that Bob uses at level \( j \). Bob will only need the outputs of \( t \) PR-boxes, while Alice uses \( 2^t - 1 \) PR-boxes in total.

4 Bias Upper Bounds

In order to prove an upper bound on the bias of any \( n \mapsto m \) f-QRAC with SR, we shall use the following equivalent version of Definition 9, which comes from input randomization, i.e., from considering the average success probability over the inputs, and from the following fact.

**Fact 30** ([28]). Let \( \rho \) be an unknown state picked from the set \( \{\rho_0, \rho_1\} \) with probability \( p \) and \( 1 - p \), respectively. The optimal success probability of predicting which state it is by a POVM is

\[
\frac{1}{2} + \frac{1}{2} \| p \rho_0 - (1 - p) \rho_1 \|_{\text{tr}}.
\]

**Definition 31.** Let \( f : \{-1, 1\}^k \to \{-1, 1\} \) be a Boolean function. An \( n \mapsto m \) f-QRAC with SR is a map \( \rho : \{-1, 1\}^n \to \mathbb{C}^{2^m \times 2^m} \) that assigns an \( m \)-qubit density matrix \( \rho(x) \) to every \( x \in \{-1, 1\}^n \) and has the property that

\[
\mathbb{E}_{S \sim \Delta_n^k} \left[ \frac{1}{2^n} \left\| \sum_{x \in \{-1,1\}^n} f(x) \rho(x) \right\|_{\text{tr}} \right] \geq \varepsilon.
\]

**Theorem 32.** Let \( f : \{-1, 1\}^k \to \{-1, 1\} \) be a Boolean function. For any \( n \mapsto m \) f-QRAC with SR and \( k = o(n) \) the following holds: for any \( \eta > 2 \ln 2 \) there is a constant \( C_\eta \) such that

\[
\varepsilon \leq C_\eta \sum_{\ell=0}^{k} L_{1,\ell}(f) \left( \frac{\eta n}{m} \right)^{\ell/2},
\]

where \( L_{1,\ell}(f) = \sum_{|T|=\ell} \left| \hat{f}(T) \right| \) is the 1-norm of the \( \ell \)-th level of the Fourier transform of \( f \).

**Proof.** We start by writing the following.

\[
\frac{1}{2^n} \left\| \sum_{x \in \{-1,1\}^n} f(x) \rho(x) \right\|_{\text{tr}} = \frac{1}{2^n} \left\| \sum_{V \subseteq [n]} \sum_{T \subseteq [k]} \hat{f}(T) \hat{\rho}(V) \sum_{x \in \{-1,1\}^n} \chi_V(x) \chi_T(x) \rho(x) \right\|_{\text{tr}}
\]

\[
= \left\| \sum_{T \subseteq [k]} \hat{f}(T) \hat{\rho}(S_T) \right\|_{\text{tr}} \leq \sum_{T \subseteq [k]} \left| \hat{f}(T) \right| \left\| \hat{\rho}(S_T) \right\|_{\text{tr}},
\]

where \( S_T = \{ S_i \mid i \in T \} \). Then

\[
\varepsilon \leq \sum_{\ell=0}^{k} \sum_{|T|=\ell} \left| \hat{f}(T) \right| \mathbb{E}_{S \sim \Delta_n^k} \left[ \left\| \hat{\rho}(S_T) \right\|_{\text{tr}} \right].
\]
but, for a given $T \subseteq [k]$ with $|T| = \ell$,
$$
\mathbb{E}_{S \sim \mathcal{A}_h^k} [\|\tilde{\eta}(S)\|_{tr}] = \frac{1}{k!} \sum_{S \subseteq \mathcal{A}_h^k} \|\tilde{\eta}(S)\|_{tr} = \frac{\ell(k-\ell)!}{k!(n/\ell)^{\ell(n-\ell)}} \sum_{S \subseteq \mathcal{C}_h^\ell} \|\tilde{\eta}(S)\|_{tr} = \mathbb{E}_{S \sim \mathcal{C}_h^\ell} [\|\tilde{\eta}(S)\|_{tr}],
$$
and thus, using Jensen’s inequality,
$$
\varepsilon \leq \sum_{\ell=0}^{k} \sum_{|T| = \ell} |\hat{\mathcal{F}}(T)| \mathbb{E}_{S \sim \mathcal{C}_h^\ell} [\|\tilde{\eta}(S)\|_{tr}] \leq \sum_{\ell=0}^{k} L_{1,\ell}(f) \sqrt{\mathbb{E}_{S \sim \mathcal{C}_h^\ell} [\|\tilde{\eta}(S)\|_{tr}^2]}. \tag{7a}
$$

We now use Theorem 20 with $\delta = \frac{\ell(2 \ln 2)m}{n}$, taking only the sum on $S$ with $|S| = \ell$,
$$
\mathbb{E}_{S \sim \mathcal{C}_h^\ell} [\|\tilde{\eta}(S)\|_{tr}^2] \leq 2^{2m\delta - \ell} \left( \frac{n}{\ell} \right)^{-1} \left( \frac{2e \ln 2m}{\ell} \right) \left( \frac{\ell}{\ell} \right)^{-1},
$$
to finally obtain
$$
\varepsilon \leq \sum_{\ell=0}^{k} \left( \frac{n}{\ell} \right)^{-1/2} L_{1,\ell}(f) \left( \frac{2e \ln 2m}{\ell} \right)^{\ell/2}. \tag{7b}
$$

From here we can use Stirling’s approximation $n! = \Theta(\sqrt{n}(n/e)^n)$ to obtain
$$
\left( \frac{\ell}{\ell - n/\ell} \right)^n \left( \frac{n}{\ell} \right)^{-1} \left( 1 + \frac{\ell}{\ell - n/\ell} \right)^{n-\ell} = \Theta \left( \sqrt{\ell} \left( \frac{n}{\ell} \right)^{\ell/2} \right). \tag{7c}
$$

We use the fact that for large enough $n/\ell$ we have $(1 + \ell/\ell - n/\ell)^{(n-\ell)/\ell} > (2e \ln 2)^{-n/2}$, where $\eta > 2 \ln 2$, and that the factor $\sqrt{\ell} \left( \frac{n}{\ell} \right)^{\ell/2}$ can be absorbed by this approximation. Then there is a constant $C_n$ such that Eq. (6) holds. \hfill \qed

A few different bounds can be obtained from the above theorem, some with a clearer meaning.

**Corollary 33.** Let $f : \{-1,1\}^k \rightarrow \{-1,1\}$ be a Boolean function. Let $r \in [0,1]$. For any $n \sim m$ f-QRAC with SR and $k = o(n)$ the following holds: for any $\eta > 2 \ln 2$ there is a constant $C_n$ such that
\begin{align*}
\varepsilon \leq C_n \left( \sum_{S \subseteq [k]} q[S] |\mathcal{F}(S)| \right)^{\ell/2}, \tag{7a}
\end{align*}
\begin{align*}
\varepsilon \leq C_n \left\| f \right\|_1 \left( \frac{nm}{n} \right)^{\ell/2}, \tag{7b}
\end{align*}
\begin{align*}
\varepsilon \leq C_n 2^{\deg(f) - 1} \text{Stab}_q[f], \tag{7c}
\end{align*}

where $q = \sqrt{\frac{nm}{n}}$, supp$(\mathcal{F}) = \{ S \subseteq [k] \mid \mathcal{F}(S) \neq 0 \}$ is the support of $f$, $h = \min\{|S| : \mathcal{F}(S) \neq 0 \}$ is the pure high degree of $f$, $\deg(f) = \max\{|S| : \mathcal{F}(S) \neq 0 \}$ is the degree of $f$ and $\left\| f \right\|_1 = \sum_{S \subseteq [k]} |\mathcal{F}(S)|$ is the Fourier 1-norm of $f$.

**Proof.** From Theorem 32 we know that for any $\eta > 2 \ln 2$ there is a constant $C_n$ such that
$$
\varepsilon \leq C_n \sum_{\ell=0}^{k} L_{1,\ell}(f) \left( \frac{nm}{n} \right)^{\ell/2}. \tag{8}
$$

There are a couple of ways to bound the above quantity. We start by proving Eq. (7a). Define $g : \{-1,1\}^k \rightarrow \mathbb{R}$, $g = \sum_{S \subseteq \text{supp}(\mathcal{F})} \text{sgn}(\mathcal{F}(S)) \mathcal{X}_S$. Let $T_q$ be the noise operator with parameter $q = \sqrt{\frac{nm}{n}}$. Let $r, s \in [0,1]$ be such that $r + s = 1$. By Cauchy-Schwarz,
$$
\left( \sum_{S \subseteq [k]} q[S] |\mathcal{F}(S)| \right)^2 = |\langle T_{q'} f, T_{q''} g \rangle|^2 \leq \langle T_{q'} f, T_{q''} f \rangle \langle T_{q'} h, T_{q''} g \rangle = \text{Stab}_{q'}[f] \sum_{S \subseteq \text{supp}(\mathcal{F})} q^{2|S|}. \tag{7c}
$$

Accepted in Quantum 2021-02-22, click title to verify. Published under CC-BY 4.0.
By plugging the above equation into Eq. (8), Eq. (7a) follows.

Eqs. (7b) and (7c) follow, respectively, by

\[ \varepsilon \leq C_\eta \sum_{\ell=0}^{k} L_{1,\ell}(f) \left( \frac{\eta m}{n} \right)^{\ell/2} \leq C_\eta \|f\|_1 \left( \frac{\eta m}{n} \right)^{\ell/2} \]

and

\[ \varepsilon \leq C_\eta \sum_{\ell=0}^{k} L_{1,\ell}(f) \left( \frac{\eta m}{n} \right)^{\ell/2} \leq C_\eta \sum_{\ell=0}^{k} 2^{\deg(f)-1} W^{\ell}[f] \left( \frac{\eta m}{n} \right)^{\ell/2} = C_\eta 2^{\deg(f)-1} \text{Stab}_q[f], \]

where we used that \( f \)'s Fourier spectrum is \( 2^{1-\deg(f)} \)-granular in Eq. (9), i.e., \( \hat{f}(S) \) is an integer multiple of \( 2^{1-\deg(f)} \) for all \( S \subseteq [k] \) (see [46, Exercise 1.11]).

Corollary 33 helps with the comparison between the bias upper bound and the bias lower bounds for \( f \)-RAC and \( f \)-QRAC (Theorems 23, 25 and 26). By taking \( \deg(f) \) as constant, we see that Eq. (7c) matches the bias lower bounds in terms of the noise stability up to an overall multiplicative constant and up to the multiplicative constant \( \sqrt{q} \) in the parameter \( q \) in \( \text{Stab}_q[f] \). Another comparison is between Eq. (7b) and Corollary 28 in terms of the pure high degree of \( f \). Again both bounds match up to a global multiplicative constant and up to the constant \( \eta \). We conjecture that the constant \( \eta \) can be dropped from all these bounds with a more careful analysis.

5 Conclusions

In this paper we proposed a simple generalization of the concept of random access to recovering the value of a given Boolean function on any subset of fixed size of the initial bits. This generalization was made assuming different resources as encoding maps, i.e., encoding the initial string into bits or qubits, and different auxiliary resources, e.g. private and shared randomness, shared entanglement and Popescu-Rohrlich boxes. Given the lower bounds from our protocols, it seems reasonable to assume that the bias \( \text{Stab}_q[f] \) with \( q = \sqrt{\frac{m}{n}} \) is, if not optimal, at least close to optimal. The case with the weakest resources, the \( n \mapsto m \) \( f \)-RAC with PR, already achieves such bias up to an additive term \( O((\log n/\ell)/(n/\ell)) \) in the parameter \( q \). For more general values of \( m = O(\log n) \), the use of quantum resources progressively improves \( q \): from \( q \approx \sqrt{\frac{2m}{n}} \) using encoding bits and SR to \( q \geq \sqrt{\frac{2m}{n}} \) using encoding qubits and SR and finally to \( q = \sqrt{\frac{m}{2n}} \) using encoding bits and shared entanglement. Such an improvement offered by quantum resources is relatively modest, specially when compared to stronger-than-quantum resources like Popescu-Rohrlich boxes, which allows the recovery of \( f(x_S) \) with certainty for any \( S \).

On the other hand, the techniques from Fourier analysis lead to bias upper bounds that match our bias lower bounds up to a global multiplicative constant and a factor \( \sqrt{\eta} \approx \sqrt{2\ln 2} \) in the parameter \( q \). We conjecture that such upper bounds can be improved and the factor \( \eta \) dropped. Moreover, the upper bounds apply only to \( f \)-QRACs with SR, therefore not including \( f \)-EARACs. The understanding of EARACs is still limited, and even though we obtained an upper bound by making an independence assumption, a general upper bound for the case \( m > 1 \) is yet unknown.

Acknowledgements

We thank Ronald de Wolf for suggesting the block-encoding scheme, originally with the \( 2,3 \mapsto 1 \) QRACs, for pointing out Refs. [35, 36] and for feedback on the manuscript. We thank Máthé Farkas and Mark Howard for pointing out Refs. [2, 19, 20, 59] and [18], respectively. We acknowledge support from the QuantERA ERA-NET Cofund in Quantum Technologies implemented within the European Union’s Horizon 2020 Programme (QuQuantAlgo project) and EPSRC grants EP/R043957/1 and EP/T001062/1. This project has received funding from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation programme (grant agreement...
No. 817581). JFD was supported by the Bristol Quantum Engineering Centre for Doctoral Training, EPSRC Grant No. EP/L015730/1.

References


