Query complexity of matroids

Raghav Kulkarni* and Miklos Santha **

[1] LIAFA - University of Paris 7 and LRI - University of Paris 11, France
kulraghav@gmail.com
[2] LIAFA - University of Paris 7, France and Center for Quantum Technologies, National University of Singapore, Singapore
miklos.santha@liafa.jussieu.fr

Abstract. Let $\mathcal{M}$ be a bridgeless matroid on ground set $\{1,\ldots,n\}$ and $f_{\mathcal{M}} : \{0,1\}^n \to \{0,1\}$ be the indicator function of its independent sets. A folklore fact is that $f_{\mathcal{M}}$ is *evasive,* i.e., $D(f_{\mathcal{M}}) = n$ where $D(f)$ denotes the deterministic decision tree complexity of f. Here we prove query complexity lower bounds for $f_{\mathcal{M}}$ in three stronger query models: (a) $D_{\oplus}(f_{\mathcal{M}}) = \Omega(n)$, where $D_{\oplus}(f)$ denotes the parity decision tree complexity of f; (b) $R(f_{\mathcal{M}}) = \Omega(n/\log n)$, where $R(f)$ denotes the bounded error randomized decision tree complexity of f; and (c) $Q(f_{\mathcal{M}}) = \Omega(\sqrt{n})$, where $Q(f)$ denotes the bounded error quantum query complexity of f.

To prove (a) we propose a method to lower bound the *sparsity* of a Boolean function by upper bounding its partition size. Our method yields a new application of a somewhat surprising result of Gopalan et al. [11] that connects the sparsity to the *granularity* of the function. As another application of our method, we confirm the Log-rank Conjecture for XOR functions [27] for a fairly large class of AC^0- XOR functions.

To prove (b) and (c) we relate the *ear decomposition* of matroids to the *critical* inputs of appropriate *tribe* functions and then use the existing randomized and quantum lower bounds for these functions.
Keywords: (parity, randomized, quantum) decision tree complexity, matroids, Fourier spectrum, read-once formulae, AC^0

1 Introduction

1.1 Decision tree models

The decision tree or query model of computing is perhaps one of the simplest models of computation. Due to its fundamental nature, it has been extensively studied over last few decades; yet it remains far from being completely understood.

Fix a Boolean function $f : \{0,1\}^n \to \{0,1\}$. A deterministic decision tree D_f for f takes $x = (x_1,\ldots,x_n)$ as an input and determines the value of $f(x_1,\ldots,x_n)$

* Supported by the French ANR Defis program under contract ANR-08-EMER-012 (QRAC project)
**

using queries of the form " is $x_i = 1$? ". Let $C(D_f, x)$ denote the cost of the computation, that is the number of queries made by D_f on input x. The *deterministic decision tree complexity* of f is defined as $D(f) = \min_{D_f} \max_x C(D_f, x)$. A bounded error randomized decision tree R_f is a probability distribution over all deterministic decision trees such that for every input, the expected error of the algorithm is bounded by some fixed constant less than $1/2$. The cost $C(R_f, x)$ is the highest possible number of queries made by R_f on x, and the *bounded error randomized decision tree complexity* of f is $R(f) = \min_{R_f} \max_x C(R_f, x)$. A bounded error quantum decision tree Q_f is a sequence of unitary operators, some of which depends on the input string. Broadly speaking, the cost $C(Q_f, x)$ is the number of unitary operators (quantum queries) which depend on x. The *bounded error quantum query complexity* of f is $Q(f) = \min_{Q_f} \max_x C(Q_f, x)$, where the minimum is taken over all quantum decision trees computing f. For a more precise definition we refer the reader to the excellent survey by Buhrman and de Wolf [8].

A natural theme in the study of decision trees is to understand and exploit the *structure* within f in order to prove strong lower bounds on its query complexity. A classic example is the study of non-trivial monotone graph properties. In the deterministic case it is known [23] that any such f of n vertex graphs has complexity $\Omega(n^2)$, and a famous conjecture [15] asserts that it is *evasive*, that is of maximal complexity, $D(f) = \binom{n}{2}$. In the randomized case the best lower bound (up to some polylogarithmic factor) is $\Omega(n^{4/3})$, and it is widely believed that in fact $R(f) = \Omega(n^2)$. In both models of computation, the structure that makes the complexity high is monotonicity and symmetry.

In this paper we study the decision tree complexity of another *structured* class, called *matroidal* Boolean functions, which arise from *matroids*. They form a subclass of monotone Boolean functions. These are the indicator functions of the independent sets of matroids. The matroidal Boolean functions inherit the rich combinatorial structure from matroids. Naturally, one may ask: what effect does this structure have on the decision tree complexity? It is a folklore fact that (modulo some degeneracies) such functions are *evasive*. Our main results in this paper are query complexity lower bounds for such functions in three stronger query models, namely: parity decision trees, bounded error randomized decision trees, and bounded error quantum decision trees. We give here a brief overview of the relatively less known model of *parity decision trees*.

A *parity decision tree* may query " is $\sum_{i \in S} x_i \equiv 1 \pmod 2$? " for an arbitrary subset $S \subseteq [n]$. We call such queries *parity queries*. For a parity decision tree P_f for f, let $C(P_f, x)$ denote the number of parity queries made by P_f on input x. The *parity decision tree complexity* of f is

$$D_{\oplus}(f) = \min_{P_f} \max_x C(P_f, x).$$

Note that $D_{\oplus}(f) \leq D(f)$ as " is $x_i = 1$? " can be treated as a parity query.

Parity decision trees were introduced by Kushilevitz and Mansour [18] in the context of learning Boolean functions by estimating their Fourier coefficients. The *sparsity* of a Boolean function f, denoted by $||\widehat{f}||_0$, is the number of its non-zero Fourier coefficients. It turns out that the logarithm of the sparsity is

a lower bound on $D_{\oplus}(f)$ [18, 24, 20]. Thus having a small depth parity decision tree implies only small number of Fourier coefficients to estimate.

Parity decision trees came into light recently in an entirely different context, namely in investigations of the *communication complexity* of XOR functions. Shi and Zhang [24] and Montanaro and Osborne [20] have observed that the deterministic communication complexity $DC(f^{\oplus})$ of computing $f(x \oplus y)$, when x and y are distributed between the two parties, is upper bounded by $D_{\oplus}(f)$. They have also both conjectured that for some positive constant c, every Boolean function f satisfies $D_{\oplus}(f) = O((\log ||\widehat{f}||_0)^c)$. Settling this conjecture in affirmative would confirm the famous Log-rank Conjecture in the important special case of XOR functions. Montanaro and Osborne [20] showed that for a monotone Boolean function $D_{\oplus}(f) = O((\log ||\widehat{f}||_0)^2)$, and conjectured that actually $c = 1$.

1.2 Our results and techniques

In this paper $[n] := \{1, \ldots, n\}$. Let $\mathcal{M}$ be a matroid on ground set $[n]$ and $f_{\mathcal{M}}$ be the indicator function of the independent sets of $\mathcal{M}$. We refer the reader to Section 2 for relevant definitions. We describe now our lower bounds in the three computational model. We think that the most interesting case is the parity decision tree model since it brings together quite a few ideas.

Fourier spectrum of matroids is dense

Our main technical result is that the Fourier spectrum of *matroidal* Boolean functions is *dense.*

Theorem 1. *If $\mathcal{M}$ is a bridgeless matroid on ground set $[n]$ then*

$$\log ||\widehat{f_{\mathcal{M}}}||_0 = \Omega(n).$$

An immediate corollary of this result is the lower bound on the parity decision tree complexity.

Corollary 1. *If $\mathcal{M}$ is a bridgeless matroid on ground set $[n]$ then*

$$D_{\oplus}(f_{\mathcal{M}}) = \Omega(n).$$

Another corollary of the theorem is that $Q^*(f(x \oplus y))$, the quantum communication complexity of $f(x \oplus y)$ in the exact computation model with shared entanglement is maximal. Indeed, Buhrman and de Wolf [7] have shown that, up to a factor of 2, it is bounded from below by the logarithm of the rank of the communication matrix $f(x \oplus y)$. Since Shi and Zhang have proven [27] that the rank of the communication matrix is exactly $||\widehat{f}||_0$, the corollary indeed follows from Theorem 1.

Corollary 2. *If $\mathcal{M}$ is a bridgeless matroid then $Q^*(f_{\mathcal{M}}(x \oplus y)) = \Omega(n)$.*

To prove Theorem 1 we bring together various concepts and ideas from several not obviously related areas. The first part of our proof which relates partition size to Fourier spectrum is actually valid for any Boolean function. Our main ingredient is a relation (Proposition 3) stating that a small Euler characteristic implies that the sparsity of the function is high, that is the number of its non-zero Fourier coefficients is large. To prove this we use a recent result of Gopalan et. al. [11] (originated in the context of property testing) that crucially uses the Boolean-ness to connect the sparsity to the *granularity* - the smallest k such that all Fourier coefficients are multiple od $1/2^k$. Our second ingredient is to show (Lemma 2) that the Euler characteristic can be bounded by the partition size of the Boolean function. Finally to make this strategy work, we need to choose an appropriate restriction of the function so that the Euler characteristic of the restriction is non-zero.

When the rank of the matroid is small, the proof of Theorem 1 is in fact relatively easy. To conclude the proof when the rank is large we use a powerful theorem of Björner [4] which bounds the partition size of a matroidal Boolean function by the number of maximum independent sets.

In fact, the same method can be used to lower bound the sparsity of another large subclass of (not necessarily monotone) Boolean functions, namely the AC^0 functions. Hence for such functions parity queries can be simulated by ordinary ones only with a polynomial factor loss. The formal statement, analogous to Theorem 1 is the following:

Theorem 2. *If $f : \{0,1\}^n \to \{0,1\}$ has a circuit of depth d and size m then*

$$\log ||\widehat{f}||_0 = \Omega(\deg(f)/(\log m + d \log d)^{d-1}).$$

We would like to point out that the upper bound on the partition size for the class of AC^0 functions is highly non-trivial result(cf. [13]), whose proof relies crucially on the Switching Lemma.

Theorems 2 has an interesting corollary that the Log-rank conjecture holds for AC^0 XOR-functions. Indeed, as we have explained already, whenever $D_{\oplus}(f) = O((\log ||\widehat{f}||_0)^c)$, the Log-rank conjecture holds for $f^{\oplus}$. Obviously $D_{\oplus}(f) \leq D(f)$, and its is known [21] that $D(f) = \deg(f)^{O(1)}$. Therefore we have

Corollary 3. *Let M_f be the communication matrix of $f^{\oplus}$. If $f : \{0,1\}^n \to \{0,1\}$ is in AC^0 then*

$$DC(f^{\oplus}) \leq (\log \mathrm{rk}(M_f))^{O(1)}.$$

This means that in *exact* model [7] quantum and classical communication complexity of AC^0- XOR functions are polynomially related.

Randomized and quantum query complexity

We obtain a nearly optimal lower bound on the randomized query complexity of matroids.

Theorem 3. *If $\mathcal{M}$ is a bridgeless matroid on ground set $[n]$ then*

$$R(f_{\mathcal{M}}) = \Omega(n/\log n).$$

It is widely conjectured that for every total Boolean function f, the relation $D(f) = O(Q(f)^2)$ holds (Conjecture 1 in [1]). Barnum and Saks (Theorem 2 in [1]) confirm this conjecture for AND-OR read-once formulae, and we are able to extend their result to read-once formulae over matroids.

Theorem 4. *If $f : \{0,1\}^n \to \{0,1\}$ is a read-once formula over matroids then*

$$Q(f) = \Omega(\sqrt{n}).$$

Our simple but crucial observation for proving lower bounds for randomized and quantum query complexity is that for any *matroidal* Boolean function f, one can associate, via the *ear decomposition* of matroids, a *tribe* function g such that f matches with g on all *critical* inputs. The lower bounds then follow from the partition bound for *tribe* functions obtained by Jain and Klauck [14] and the adversary bound for AND-OR read-once formulae by Barnum and Saks [1]. Our main contribution here is observing that certain lower bound methods for *tribe* functions generalize for the larger class of *matroidal* Boolean functions.

2 Preliminaries

2.1 Matroids and matroidal Boolean functions

Definition 1 (Matroid). *Let E be a finite set. A collection $\mathcal{M} \subseteq 2^E$ is called a* matroid *if it satisfies the following properties:*
(1) (non-emptiness) $\emptyset \in \mathcal{M}$;
(2) (hereditary property) *if $A \in \mathcal{M}$ and $B \subseteq A$ then $B \in \mathcal{M}$;*
(3) (augmentation property) *if $A, B \in \mathcal{M}$ and $|A| > |B|$ then there exists $x \in A \backslash B$ such that $x \cup B \in \mathcal{M}$.*

We call E the *ground set* of $\mathcal{M}$. The members of $\mathcal{M}$ are called *independent sets* of $\mathcal{M}$. If $A \notin \mathcal{M}$ then A is called *dependent* with respect to $\mathcal{M}$. A *circuit* in $\mathcal{M}$ is a minimal dependent set. For $A \subseteq E$, the *rank* of A with respect to $\mathcal{M}$ is defined as follows:

$$\mathrm{rk}(A, \mathcal{M}) := \max\{|B| \mid B \subseteq A \text{ and } B \in \mathcal{M}\}.$$

The *rank* or *dimension* of $\mathcal{M}$, denoted by $rk(\mathcal{M})$, is defined to be the rank of E with respect to $\mathcal{M}$. Appendix A contains some examples of matroid.

A matroid $\mathcal{M}$ on ground set E can be identified with a Boolean function $f_{\mathcal{M}} : \{0,1\}^{|E|} \to \{0,1\}$ as follows: first identify $x \in \{0,1\}^{|E|}$ with a subset $S(x) := \{e \in E \mid x_e = 1\}$ of E; now let $f_{\mathcal{M}}(x) := 0 \iff S(x) \in \mathcal{M}$.

A function $f : \{0,1\}^n \to \{0,1\}$ is said to be *monotone increasing* if:

$$(\forall x, y \in \{0,1\}^n)(x \leq y \implies f(x) \leq f(y)),$$

where $x \leq y$ if for every $i \in [n] := \{1, \ldots, n\}$ we have $x_i \leq y_i$. The hereditary property of $\mathcal{M}$ translates to $f_{\mathcal{M}}$ being monotone.

We call a Boolean function f *matroidal* if there exists a matroid $\mathcal{M}$ such that $f \equiv f_{\mathcal{M}}$. Examples: AND, OR, MAJORITY, $\vee_{i=1}^{k} \wedge_{i=1}^{\ell} x_{ij}$.

An element $e \in E$ is called a *bridge* in $\mathcal{M}$ if e does not belong to any circuit of $\mathcal{M}$. If e is a bridge in $\mathcal{M}$ then the corresponding variable x_e of $f_{\mathcal{M}}$ is *irrelevant*, i.e., the function $f_{\mathcal{M}}$ does not depend on the value of x_e. Thus, for the purpose of query complexity, we can delete all the bridges and focus our attention on bridgeless matroids.

Ear decomposition of bridgeless matroids

Let $\mathcal{M}$ be a matroid on ground set E. Let $T \subseteq E$. The *contraction* of $\mathcal{M}$ by T, denoted by $\mathcal{M}/T$, is a matroid on the ground set $E - T$ defined as follows:

$$\mathcal{M}/T := \{A \subseteq E - T \mid rk(A \cup T, \mathcal{M}) = |A| + rk(T, \mathcal{M})\}.$$

Definition 2 (Ear Decomposition [26]). *A sequence $(C_1, \ldots, C_k)$ of circuits of $\mathcal{M}$ is called an* ear decomposition *of $\mathcal{M}$ if:*
(1) $L_i := C_i - \bigcup_{j<i} C_j$ is non-empty and
(2) L_i is a circuit in $\mathcal{M}/\bigcup_{j<i} C_j$.

For $i = 1, \ldots, k$, the sets L_i are called *lobes*. An ear decomposition is *complete* if $\bigcup_{i=1}^{k} L_i = E$. Every bridgeless matroid admits a complete ear decomposition [10]. We identify complete ear decompositions with their lobe partition $E = \bigcup_{i=1}^{k} L_i$. For our randomized and quantum lower bounds we will crucially use the following proposition (Appendix B).

Proposition 1. *Let $\mathcal{M}$ be a bridgeless matroid on ground set E and let $E = \bigcup_{i=1}^{k} L_i$ be a complete ear decomposition of $\mathcal{M}$. Let $e_1, \ldots, e_k \in E$ such that $e_i \in L_i$ and $L'_i := L_i - \{e_i\}$. Then $\bigcup_{i=1}^{k} L'_i$ is a maximum independent set of $\mathcal{M}$.*

2.2 Read-once formulae

Let $\mathcal{F}$ be a family of Boolean functions. A *read-once formula over $\mathcal{F}$* is a Boolean function represented by a rooted tree whose internal nodes are labeled by members of $\mathcal{F}$, and whose leaves are labelled by distinct variables. The inputs to each function are the outputs of its children.

If $\mathcal{F} = \{\wedge_n, \vee_n : n \in \mathbb{N}\}$ then we get the (unbounded fan-in) AND-OR read-once formulae. Given a complete ear decomposition $\bigcup_{i=1}^{k} L_i = E$ of a matroid, we associate to it the AND-OR read-once formula $g = \bigvee_{i=1}^{k} \bigwedge_{e \in L_i} x_e$. Such functions (OR's of AND's) are also called *tribe* functions.

Definition 3 (Critical Inputs of AND-OR Read-once Formulae). *An input is* critical *for an AND-OR read-once formula if for every AND gate at most one child evaluates to* 0 *and for every OR gate at most one child evaluates to* 1.

2.3 Fourier spectrum of Boolean functions

Every Boolean function $f : \{0,1\}^n \to \{0,1\}$ can be uniquely represented by a real multilinear polynomial: $f(x_1, \ldots, x_n) = \sum_{S \subseteq [n]} \beta_S \prod_{i \in S} x_i$. Moreover, the coefficients β_S are integers. The *polynomial degree* of f is $deg(f) := max\{|S| \mid \beta_S \neq 0\}$. The *degree over* $\mathbb{F}_2$ of f is $deg_{\oplus}(f) := max\{|S| \mid \beta_S \neq 0 \mod 2\}$. The *Euler Characteristic* of f is $\chi(f) := \sum_{x \in \{0,1\}^n} (-1)^{|x|} f(x)$, where $|x|$ denotes the number of 1's in x. One can obtain the following expression for $\beta_{[n]}$ (cf. [2]):

$$\beta_{[n]} = \sum_{T \subseteq [n]} (-1)^{n-|T|} f(T) = (-1)^n \chi(f). \tag{1}$$

Fourier spectrum

Let $f_{\pm} : \{-1,1\}^n \to \{-1,1\}$ be obtained from f as follows: $f_{\pm}(z_1, \ldots, z_n) := 1 - 2f(\frac{1-z_1}{2}, \ldots, \frac{1-z_n}{2})$. Let $f_{\pm} : \{-1,1\}^n \to \{-1,1\}$ be represented by the following polynomial with real coefficients: $f_{\pm}(z_1, \ldots, z_n) = \sum_{S \subseteq [n]} \widehat{f}(S) \prod_{i \in S} z_i$. The above polynomial is unique and it is called the Fourier expansion of f. The $\widehat{f}(S)$ are called the Fourier coefficients of f. Note that:

$$\widehat{f}([n]) = \frac{(-1)^{n-1} \beta_{[n]}}{2^{n-1}} = \frac{\chi(f)}{2^{n-1}}. \tag{2}$$

The *sparsity* of a Boolean function f is $||\widehat{f}||_0 := |\{S \mid \widehat{f}(S) \neq 0\}|$. The *granularity* of a Boolean function is the smallest non-negative integer k such that each of its Fourier coefficients is an integer multiple of $1/2^k$.

3 Parity decision tree complexity

In this section we prove Theorem 1. The following lemma which lower bounds the parity decision tree complexity by the sparsity is our starting point.

Lemma 1 (Shi and Zhang [27], Montanaro and Osborne [20]).

$$D_{\oplus}(f) = \Omega(\log ||\widehat{f}||_0).$$

The proof distinguishes two cases, according to the size of the rank of the matroid. In the first case, when the rank is small, the only property of matroidal Boolean functions we use is monotonicity. In the second case, when the rank is large,we proceed in two distinct steps as explained in the Introduction. Firstly we show that if the partition size of the function is small then its sparsity is high, a fact which is valid for any Boolean function. Secondly, in order to upper bound the partition size, we use *partitionability*, a strong topological property of matroids.

3.1 The small rank case

A Boolean function f is said to be sensitive on i^{th} bit of input $x = (x_1, \ldots, x_n)$ if $f(x_1, \ldots, x_{i-1}, 1 - x_i, x_{i+1}, \ldots, x_n) \neq f(x)$. The sensitivity of f on input x, denoted by $s(f, x)$ is the number of sensitive bits of f on x. The sensitivity of a Boolean function f, denoted by $s(f)$ is $\max_x s(f, x)$.

Proposition 2. *If $\mathcal{M}$ is a matroid of rank r on ground set $[n]$ then*

$$\log ||\widehat{f_{\mathcal{M}}}||_0 \geq n - r.$$

Proof. It is easy to see that $s(f_{\mathcal{M}}) \geq n - r$ if $\mathcal{M}$ is a matroid of rank r on ground set $[n]$. In [3]) it is shown that for any Boolean function f we have $\log ||\widehat{f}||_0 \geq \deg_{\oplus}(f)$. In [20] it is proven that for monotone f we also have $\deg_{\oplus}(f) \geq s(f)$.

3.2 The large rank case

Small Euler characteristic implies high sparsity

Theorem 5 (Gopalan et. al., Theorem 12 in [11]). *If the sparsity of a Boolean function is s then its granularity is at most $\lfloor \log s \rfloor - 1$.*

Proposition 3. *If $f : \{0,1\}^n \to \{0,1\}$ such that $\chi(f) \neq 0$ then*

$$\log ||\widehat{f}||_0 = \Omega(n - \log |\chi(f)|).$$

Proof. If $\widehat{f}([n]) \neq 0$ then the granularity of f is $\Omega(\log(1/|\widehat{f}([n])|))$. From Equation 2 we know that $\widehat{f}([n]) = \chi(f)/2^{n-1}$. Together with Theorem 5 this gives the desired lower bound on the sparsity.

Euler characteristic is upper bounded by partition size

Definition 4 (Sub-cube Partition). *A Boolean sub-cube of the Boolean cube $\{0,1\}^n$ is an interval $[x, y] := \{z \mid x \leq z \leq y\}$, where $x, y \in \{0,1\}^n$. The sub-cube partition size of f, denoted by $P(f)$ is the smallest integer such that $f^{-1}(1)$ can be partitioned into $P(f)$ disjoint Boolean sub-cubes.*

Lemma 2. *For any Boolean function f, we have $|\chi(f)| \leq P(f)$.*

Proof. First note that no $x \in f^{-1}(0)$ contributes to $\chi(f)$. Let $\mathcal{C}$ be a sub-cube in the partition of $f^{-1}(1)$ into $P(f)$ parts. We can identify $\mathcal{C}$ with a partial Boolean assignment C that assigns 0 or 1 value to a subset $S_C \subseteq [n]$ variables. Note that this partial Boolean assignment certifies that the value of f is 1 on the entire $\mathcal{C}$, i.e., on any extension of C. If $|S_C| < n$ then:

$$|\{x \in \mathcal{C} \mid |x| \equiv 0 \pmod 2\}| = |\{x \in \mathcal{C} \mid |x| \equiv 1 \pmod 2\}|.$$

Therefore, the only $\mathcal{C}$'s that contributes to $\chi(f)$ have $|S_C| = n$ and hence $|\mathcal{C}| = 1$. In effect, such a $\mathcal{C}$ contributes ± 1 to $\chi(f)$.

Upper bounding the Euler characteristic of matroids

Definition 5 (Partitionable Boolean Functions, cf. [16]). *A monotone decreasing Boolean function f is said to be partitionable if for every input $A \in f^{-1}(1)$ with maximal number of 1s, we can associate $\phi(A) \in f^{-1}(1)$ such that the $[\phi(A), A]$ partition $f^{-1}(1)$.*

Theorem 6 (Björner [4]). *If $\mathcal{M}$ is a matroid then $\neg f_{\mathcal{M}}$ is partitionable.*

Lemma 3. *If matroid $\mathcal{M}$ has N maximum independent sets then $|\chi(f_{\mathcal{M}})| \leq N$.*

Proof. From Theorem 6 we know that $\neg f_{\mathcal{M}}$ is partitionable. Thus for every maximum independent set A of $\mathcal{M}$ one can associate an independent set $\phi(A) \subseteq A$ such that $[\phi(A), A]$ form a partition of $\mathcal{M}$. Since each $[\phi(A), A]$ is a Boolean sub-cube, we get a sub-cube partition of $\neg f_{\mathcal{M}}$ with at most N parts. Now the lemma follows from Lemma 2 and from the fact that $|\chi(f)| = |\chi(\neg f)|$.

3.3 Putting things together

In order to use Proposition 3 we need to show that the Euler characteristic of bridgeless matroids is non-zero.

Proposition 4. *If $\mathcal{M}$ is a bridgeless matroid then we have $\chi(f_{\mathcal{M}}) \neq 0$.*

Proof. We prove by induction on the cardinality of the ground set of bridgeless matroids that $|\chi(\mathcal{M})| \neq 0$. For every matroid $\mathcal{M}$ on ground set E and for every $e \in E$, by definition $\mathcal{M} - \{e\}$ is the matroid whose ground set is $E \setminus \{e\}$ and whose independent sets are those of $\mathcal{M}$ not containing e. An element $e \in E$ is called *loop* if $\{e\}$ is a circuit in $\mathcal{M}$.

The inductive step distinguishes two cases. If there is a loop $e \in E$ then it is easy to check that $|\chi(f_{\mathcal{M}})| = |\chi(f_{\mathcal{M}-\{e\}})|$. If there is a non-loop element $e \in E$ then we denote by $\mathcal{C}_e$ the collection of the circuits of $\mathcal{M}$ that contain e. Kook shows that $|\chi(f_{\mathcal{M}})|$ satisfies the following recurrence (Theorem 1 in Kook [17]) :

$$|\chi(f_{\mathcal{M}})| = \sum_{C \in \mathcal{C}_e} |\chi(f_{\mathcal{M}/C})|.$$

Note that the operations contracting a cycle and deleting a loop both preserve the bridgelessness and reduce the cardinality of the ground set by at least one.

The only base case, under the assumption of bridgelessness, is a matroid on ground set $\{e\}$ where $\{e\}$ is a circuit. It is easy to see that $\chi \neq 0$ in this case.

We can now give the proof of Theorem 1.

Proof. Let r be the rank of $\mathcal{M}$ and N be the number of maximum independent sets of $\mathcal{M}$. If $n - r \geq \frac{2n}{3}$ then the lower bound follows from Proposition 2. If $n - r < \frac{2n}{3}$ then:

$$|\chi(f)| \leq N \leq \binom{n}{r} = \binom{n}{n-r} \leq 2^{H(1/3)n},$$

where $|\chi(f)| \leq N$ follows from Lemma 3, and $N \leq \binom{n}{r}$ follows from the fact that every maximal independent set of a matroid has the same cardinality. The last inequality uses the assumption: $n - r < \frac{2}{3}n$. The H there denotes the binary entropy function: $H(\epsilon) = -\epsilon \log \epsilon - (1-\epsilon)\log(1-\epsilon)$. Since $H(1/3) < 1$, the theorem follows from Proposition 3 and Proposition 4.

Remark A. Since intersection of two intervals is again an interval, the partition size of the intersection of two matroid can be upper bounded when the rank of either of the matroid is small. Hence our proof goes through for the indicator functions of intersection of two matroids.

Remark B. The tribe function $\bigvee_{i=1}^{\sqrt{n}} \bigwedge_{j=1}^{\sqrt{n}} x_{ij}$ shows that Theorem 1 does not hold by replacing $\log ||\widehat{f}||_0$ with $s(f)$. We do not know if it holds with $\deg_{\oplus}(f)$.

4 Randomized query complexity

Let $\mathcal{M}$ be a bridgeless matroid on ground set $[n]$ with a complete ear decomposition $[n] = \cup_{i=1}^{r} L_i$. First we do some preprocessing. For $0 \leq t \leq \log n$, let

$$E_t := \bigcup_{i:2^t \leq |L_i| < 2^{t+1}} L_i.$$

Choose an index t_0 such that $|E_{t_0}| \geq n/\log n$. Let f' be a restriction of $f_{\mathcal{M}}$ obtained by fixing the variables outside E_{t_0} as follows: For each $L_i \nsubseteq E_{t_0}$, fix some $e_i \in L_i$ and set $x_{e_i} = 0$, and for $e \in L_i - \{e_i\}$ set $x_e = 1$. Furthermore for each $L_i \subseteq E_{t_0}$, fix arbitrarily all but 2^{t_0} variables in L_i and set their values to 1.

We re-label the indices so that $L_1, \ldots, L_k \subseteq E_{t_0}$ and $L_{k+1}, \ldots, L_r \nsubseteq E_{t_0}$. This allows us to index the variables of f' by x_{ij} for $i \in [k]$ and $j \in [\ell]$, where $\ell = 2^{t_0}$ and x_{ij} is the j^{th} among the ℓ unrestricted variables in L_i. Thus f' is a function on $k \times \ell$ variables where and $k \times \ell \geq n/(2\log n)$.

$$g := \bigvee_{i=1}^{k} \bigwedge_{j=1}^{\ell} x_{ij}.$$

Lemma 4. *If f is a monotone increasing Boolean function on $k \times \ell$ variables that matches with g on all the critical inputs then*

$$R(f) = \Omega(k \times \ell).$$

Jain and Klauck prove the above Lemma for the case $k = \ell$ (Theorem 4 in [14]). An adaptation of their proof (Appendix C) gives the general case. From Proposition 1 we have:

Lemma 5. *The function f' matches with g on all critical inputs.*

Theorem 3 is an immediate consequence of Lemma 4 and Lemma 5.

5 Quantum query complexity

Let $\mathcal{M}$ be a bridgeless matroid on ground set $[n]$ with a complete ear decomposition $[n] = \cup_{i=1}^{k} L_i$, and let g be the tribe function associated with it.

Lemma 6 (Barnum and Saks, Theorem 2 in [1]). *If f is a Boolean function on n variables that matches with g on all the critical inputs then: $Q(f) = \Omega(\sqrt{n})$.*

From Proposition 1 we have:

Lemma 7. *The function $f_{\mathcal{M}}$ matches with g on all critical inputs.*

Theorem 7. *If $\mathcal{M}$ is a bridgeless matroid on ground set $[n]$ then:*

$$Q(f_{\mathcal{M}}) = \Omega(\sqrt{n}).$$

Theorem 4 is an extension of the above theorem to read-once formulae over the family of matroidal Boolean function. Its proof is deferred to Appendix D.

An upper bound

The following theorem follows along the lines of Theorem 11 in Childs and Kothari [9] (Appendix E).

Theorem 8. *If $\mathcal{M}$ is a matroid of rank r on ground set $[n]$ then*

$$Q(f_{\mathcal{M}}) = O(\sqrt{rn}).$$

References

1. Howard Barnum, Michael E. Saks: A lower bound on the quantum query complexity of read-once functions. J. Comput. Syst. Sci. 69(2): 244-258 (2004)
2. Richard Beigel: The Polynomial Method in Circuit Complexity. Structure in Complexity Theory Conference 1993: 82-95
3. Anna Bernasconi, Bruno Codenotti: Spectral Analysis of Boolean Functions as a Graph Eigenvalue Problem. IEEE Trans. Computers 48(3): 345-351 (1999)
4. Anders Björner: Matroid Applications: (Ch. 7.) Homology and Shellability of Matroids and Geometric Lattices pp. 226-283 (1992)
5. Anders Björner, László Lovász, Andrew Chi-Chih Yao: Linear Decision Trees: Volume Estimates and Topological Bounds STOC 1992: 170-177
6. G. Brassard, P. Hoyer, M. Mosca, and A. Tapp: Quantum amplitude amplification and estimation. In Quantum computation and information, volume 305 of Contemporary Mathematics, pages 53-74. AMS, 2002.
7. Harry Buhrman, Ronald de Wolf: Communication Complexity Lower Bounds by Polynomials. IEEE Conference on Computational Complexity 2001: 120-130
8. Harry Buhrman, Ronald de Wolf: Complexity measures and decision tree complexity: a survey. Theor. Comput. Sci. 288(1): 21-43 (2002)
9. Andrew M. Childs, Robin Kothari: Quantum query complexity of minor-closed graph properties. STACS 2011: 661-672

10. Collette R. Coullard, Lisa Hellerstein: Independence and Port Oracles for Matroids, with an Application to Computational Learning Theory. Combinatorica 16(2): 189-208 (1996)
11. Parikshit Gopalan, Ryan O'Donnell, Rocco A. Servedio, Amir Shpilka, Karl Wimmer: Testing Fourier Dimensionality and Sparsity. ICALP 2009 (1): 500-512
12. Lov K. Grover: A Fast Quantum Mechanical Algorithm for Database Search. STOC 1996: 212-219
13. Russell Impagliazzo, William Matthews, Ramamohan Paturi: A satisfiability algorithm for AC0. SODA 2012: 961-972
14. Rahul Jain, Hartmut Klauck: The Partition Bound for Classical Communication Complexity and Query Complexity. IEEE Conference on Computational Complexity 2010: 247-258
15. Jeff Kahn, Michael E. Saks, Dean Sturtevant: A topological approach to evasiveness. Combinatorica 4(4): 297-306 (1984)
16. Peter Kleinschmidt, Shmuel Onn: Signable Posets and Partitionable Simplicial Complexes. Discrete and Computational Geometry, Vol 15 (4) 443-466 (1996)
17. W. Kook: A new formula for an evaluation of the Tutte polynomial of a matroid. Discrete Mathematics, Vol. 300, Issue 1-3, 2005: 235-238
18. Eyal Kushilevitz, Yishay Mansour: Learning Decision Trees Using the Fourier Spectrum. SIAM J. Comput. 22(6): 1331-1348 (1993)
19. Nikos Leonardos, Michael Saks: Lower Bounds on the Randomized Communication Complexity of Read-Once Functions. Computational Complexity 19(2): 153-181 (2010)
20. Ashley Montanaro, Tobias Osborne: On the communication complexity of XOR functions CoRR abs/0909.3392: (2009)
21. Noam Nisan, Mario Szegedy: On the Degree of Boolean Functions as Real Polynomials. Computational Complexity 4: 301-313 (1994)
22. Noam Nisan, Avi Wigderson: On Rank vs. Communication Complexity. Combinatorica 15(4): 557-565 (1995)
23. Ronald L. Rivest, Jean Vuillemin: On Recognizing Graph Properties from Adjacency Matrices. Theor. Comput. Sci. 3(3): 371-384 (1976)
24. Yaoyun Shi, Zhiqiang Zhang: Communication Complexities of XOR functions CoRR abs/0808.1762: (2008)
25. Daniel R. Simon: On the Power of Quantum Computation. SIAM J. Comput. 26(5): 1474-1483 (1997)
26. Balázs Szegedy, Christian Szegedy: Symplectic Spaces And Ear-Decomposition Of Matroids. Combinatorica 26(3): 353-377 (2006)
27. Zhiqiang Zhang, Yaoyun Shi: On the parity complexity measures of Boolean functions. Theor. Comput. Sci. 411(26-28): 2612-2618 (2010)

A Examples of matroid

(1) Let $E = [n] := \{1, \ldots, n\}$. For each $0 \leq r \leq n$ one can define $\mathcal{M}_{n,r} := \{A \subseteq E \mid |A| \leq r\}$. This gives a matroid of dimension r.
(2) Fix a graph $G = (V, E)$. Let $\mathcal{M} := \{A \subseteq E \mid A \text{ is acyclic}\}$. If G has c connected components then this gives a matroid of dimension $n - c$.
(3) Let $v_1, \ldots, v_n$ be n vectors in a vector space. Let $\mathcal{M} := \{A \subseteq [n] \mid$ the vectors $\{v_i \mid i \in A\}$ are linearly independent$\}$. In particular, if v_i are the column vectors of

some matrix M then this gives a matroid of dimension equal to the column rank of M.
(4) Fix a graph $G = (V, E)$. Let V be the ground set of $\mathcal{M}$. Define $S \subseteq V$ to be independent iff there is a matching in G that saturates all the vertices in S. This gives a matroid with rank equal to twice the cardinality of maximum matching in the graph.

B Proof of Proposition 1

Proof. For $r = 1, \ldots, k$, let $E_r := \bigcup_{i=1}^{r} L_i$ and $E'_r := \bigcup_{i=1}^{r} L'_i$. We prove the predicate $P_r \wedge P'_r$ by induction on r, where $P_r : \mathrm{rk}(E_r, \mathcal{M}) = \sum_{i=1}^{r}(|L_i| - 1)$ and $P'_r : \mathrm{rk}(E'_r, \mathcal{M}) = \sum_{i=1}^{r}(|L_i| - 1)$.

This implies that $\mathrm{rk}(E, \mathcal{M}) = \mathrm{rk}(E'_k, \mathcal{M}) = |E'_k|$, and therefore we conclude that E'_k must be a maximum independent set of $\mathcal{M}$.

Base Case: Since $E_1 = L_1 = C_1$, which is a minimal dependent set in $\mathcal{M}$, we have that P_1 and P'_1 holds.

Inductive Hypothesis: Let us assume that P_{r-1} and P'_{r-1} holds.

Inductive Step: We will prove that P_r and P'_r holds.

First we prove that P_r *holds:*

It follows immedietely from the definition of contraction that:

$$\mathrm{rk}(A \cup T, \mathcal{M}) = \mathrm{rk}(A, \mathcal{M}/T) + \mathrm{rk}(T, \mathcal{M}). \tag{3}$$

From Equation 3 we have:

$$\mathrm{rk}(E_r, \mathcal{M}) = \mathrm{rk}(L_r, \mathcal{M}/E_{r-1}) + \mathrm{rk}(E_{r-1}, \mathcal{M}).$$

Since L_r is a circuit in $\mathcal{M}/E_{r-1}$ we have:

$$\mathrm{rk}(L_r, \mathcal{M}/E_{r-1}) = |L_r| - 1$$

and by inductive hypothesis (P_{r-1}) we have:

$$\mathrm{rk}(E_{r-1}, \mathcal{M}) = \sum_{i=1}^{r-1}(|L_i| - 1).$$

Hence P_r holds.

Now we prove that P'_r *holds:*
From Equation 3 we have:

$$\mathrm{rk}(E'_r, \mathcal{M}) = \mathrm{rk}(L'_r, \mathcal{M}/E'_{r-1}) + \mathrm{rk}(E'_{r-1}, \mathcal{M}).$$

By inductive hypothesis ($P_{r-1} \wedge P'_{r-1}$) we have:

$$\mathrm{rk}(E'_{r-1}, \mathcal{M}) = \mathrm{rk}(E_{r-1}, \mathcal{M}).$$

We will prove that:

$$\textit{claim: } \mathrm{rk}(L'_r, \mathcal{M}/E'_{r-1}) = \mathrm{rk}(L'_r, \mathcal{M}/E_{r-1}).$$

This would imply that $\mathrm{rk}(E'_r, \mathcal{M}) = \mathrm{rk}(E_r, \mathcal{M})$. Together with P_r we can then conclude that P'_r holds.

Proof of the claim: Since rank is monotone and $E'_r \subseteq E_r$, we have:

$$\mathrm{rk}(L'_r \cup E'_{r-1}, \mathcal{M}) \leq \mathrm{rk}(L'_r \cup E_{r-1}, \mathcal{M}).$$

Thus:

$$\mathrm{rk}(L'_r, \mathcal{M}/E'_{r-1}) \leq \mathrm{rk}(L'_r \cup E_{r-1}, \mathcal{M}) - \mathrm{rk}(E_{r-1}, \mathcal{M}) = \mathrm{rk}(L'_r, \mathcal{M}/E_{r-1}).$$

On the other hand we have:

$$\mathrm{rk}(L'_r, \mathcal{M}/E'_{r-1}) \geq \mathrm{rk}(L'_r, \mathcal{M}/E_{r-1}).$$

This is because if B is independent in $\mathcal{M}/T$ then it is also independent in $\mathcal{M}/T'$ for any $T' \subseteq T$.

Thus we have: $\mathrm{rk}(L'_r, \mathcal{M}/E'_{r-1}) = \mathrm{rk}(L'_r, \mathcal{M}/E_{r-1})$.

C Adaptation of Theorem 4 of Jain and Klauck [14]

Proof of Lemma 4

Proof. The proof is similar to that of Theorem 4 in [14] except for some minor changes. We borrow the notation from [14] with some differences that we explain below.

Jain and Klauck [14] consider the (AND-OR) function $\bigwedge_{i=1}^{\sqrt{n}} \bigvee_{j=1}^{\sqrt{n}} x_{ij}$ whereas we are interested in the (OR-AND) function $g \equiv \bigvee_{i=1}^{k} \bigwedge_{j=1}^{\ell} x_{ij}$, where $k\ell = n$. We work with $f \equiv \neg g$. It is easy to see that $R(f) = R(g)$.

Jain and Klauck's critical inputs for tribe functions

Jain and Klauck (implicit in proof of Theorem 4 in [14]) define the critical inputs for such functions as follows:

(a1) Critical inputs of type T_1 : For each i choose one j and set $x_{ij} = 0$. Set the rest of the variables to 1.

(a2) Critical inputs of type T_2 : Choose a critical input of type T_1 and re-set an additional variable to 0.

(b) Critical inputs of type T_0 : Choose a critical input of type T_1. Choose an ij such that $x_{ij} = 0$ and re-set $x_{ij} = 1$.

Note that if a monotone increasing Boolean function matches with g on T_1 and T_0 then it must also match with g on T_2.

It is easy to see that $|T_1| = \ell^k$, $|T_0| = k \times \ell^{k-1}$, and $|T_2| = k \times \binom{\ell}{2} \times \ell^{k-1}$.

A solution to the dual

Let $opt_\epsilon(f)$ denote the optimum value of the dual program considered by Jain and Klauck (proof of Theorem 4 in [14]):

$\max \sum_{x:f(x)=1}(1-\epsilon)\mu_x - \sum_{x:f(x)=0}\epsilon\mu_x + \phi_x$,
such that for any partial assignment A :
$\sum_{f^{-1}(1)\cap A}\mu_x - \sum_{f^{-1}(0)\cap A}\mu_x + \phi_x \leq 2^{|A|}$; and
for each $x : \mu_x \geq 0$ and $\phi_x \leq 0$.

Below we describe a feasible solution to the above linear program.

Let $\delta := \frac{1}{4} - 4\epsilon$.

For $x \in T_1 : \mu_x = \frac{2^{\delta n}}{|T_1|}$; $\phi_x = 0$.

For $x \in T_0 : \mu_x = \frac{1}{4\epsilon} \times \frac{2^{\delta n}}{|T_0|}$; $\phi_x = 0$.

For $x \in T_2 : \mu_x = 0$; $\phi_x = -\frac{2}{3} \times \frac{2^{\delta n}}{|T_2|}$.

For $x \notin T_1 \cup T_2 \cup T_0 : \mu_x = \phi_x = 0$.

We need to show that (μ, ϕ) is a feasible solution for the dual for $opt_\epsilon(f)$.

Let A be an assignment.

We need to show that the total contribution to the dual constraint corresponding to A from the critical inputs that are consistent with A is at most $2^{|A|}$

Case 1: $|A| \geq \delta n$.

Since the contribution from T_0 and T_2 inputs is negative, it suffices to bound the contribution from T_1 inputs, which is at most $2^{\delta n} \leq 2^{|A|}$.

Case 2: The assignment A fixes $x_{ij} = x_{ij'} = 0$ for some i and some $j \neq j'$.

The only critical inputs that are consistent with A will be of type T_2, whose contribution is always negative, hence $\leq 0 \leq 2^{|A|}$.

Case 3: The assignment A, for each i, fixes at most one variable $x_{ij} = 0$.

Let α_i and β_i denote the number of variables (number of j s) x_{ij} that are fixed to 1 and 0 respectively. We are in the case where $\beta_i \in \{0, 1\}$.

Let γ_i be the number of x_{ij} that are left free by the assignment A.

Let $k' := \sum_{i=1}^{k} \beta_i$ and w.l.o.g. assume that the last k' values β_i are 1.

Case 3 (a): $k' \leq (1 - 4\epsilon)k$.

The number of inputs in T_1 consistent with A, denoted by a_1, is exactly $\prod_{i=1}^{k-k'} \gamma_i$.

The number of inputs in T_0 that are consistent with A, denoted by a_0, is:

$$\sum_{i=1}^{k-k'} \prod_{j\in[k-k']:j\neq i} \gamma_j = \left(\sum_{i=1}^{k-k'} \frac{1}{\gamma_i}\right) \prod_{j\in[k-k']} \gamma_j \geq \frac{k-k'}{\ell} \prod_{j\in[k-k']} \gamma_j$$

Thus:

$$a_0 \geq \frac{4\epsilon k}{\ell} \times a_1.$$

The total contribution is at most:

$$\frac{2^{\delta n}}{\ell^{k-1}} \times \left(\frac{a_1}{\ell} - \frac{a_0}{4\epsilon k}\right),$$

which we can upper bound by $0 \leq 2^{|A|}$ using the above lower bound on a_0 in terms of a_1.

Case 3 (b): $k' \geq (1-4\epsilon)k$. Again w.l.o.g. the last k' β_i are 1.

The number of inputs in T_1 consistent with A, denoted by a_1, is exactly $\prod_{i=1}^{k-k'} \gamma_i$.

The number of inputs in T_2 consistent with A, denoted by a_2, is at least:

$$\left(\prod_{i=1}^{k-k'} \gamma_i\right)\left(\sum_{i=k-k'+1}^{k} \gamma_i\right).$$

This is because for $i \leq k-k'$ we can fix any of the γ_i variables to 0 and then we can choose some $k-k' < i \leq k$ and then fix any of the γ_i variables to 0 to get a critical input of type 2 T_2.

Since we are in the case that $|A| \leq \delta n$ and $k' \geq (1-4\epsilon)k$, the total number of free variables among the last k' blocks of size ℓ is:

$$\sum_{i=k-k'+1}^{k} \gamma_i \geq k'\ell - \delta n = n \cdot (1-\delta-4\epsilon).$$

Thus:

$$a_2 \geq \frac{3}{4} \times k \times \ell \times a_1.$$

The total contribution can be upper bounded by:

$$\frac{2^{\delta n}}{\ell^{k-1}} \times \left(\frac{a_1}{\ell} - \frac{2}{3} \cdot \frac{a_2}{k\binom{\ell}{2}}\right)$$

Using the above lower bound on a_2 in terms of a_1, we can conclude that the total contribution is (for some poisitve real number M) at most $M \times (1/\ell - 1/(\ell-1))$, which is at most $0 \leq 2^{|A|}$.

D Extension of Barnum and Saks's result to read-once formulae over matroids

Let $\mathcal{F}$ be the family of all matroidal Boolean functions and let f be a read-once formula over $\mathcal{F}$. Let $f_{\mathcal{M}_1}, \ldots, f_{\mathcal{M}_t}$ be the matroidal Boolean functions used at the nodes of the tree. We construct an AND-OR read-once formula g by replacing $f_{\mathcal{M}_i}$ by g_i, the tribe function associated with a complete ear-decomposition of $\mathcal{M}_i$.

Using Observation 7 one can prove the following:

Observation 9 *The function f matches with g on all critical inputs.*

Proof. Let f be a read-once formula over matroids and g be the associated read-once formula obtained by replacing $f_{\mathcal{M}_i}$ by g_i. We prove by induction on the height of the node in the tree that the sub-formula under that node matches with the corresponding read-once formula on all *critical* inputs.

The base case holds for nodes of height one because of Observation 7.

The inductive hypothesis is that for any node at height $h-1$ the sub-formula under it matches with the corresponding read-once formula on all *critical* inputs.

Now let f' be a matroid function at a node at height h and suppose it has t children. It follows directly from the definition that an input is *critical* for the read-once sub-formula at the node at height h iff it is critical for the read-once sub-formulae at the children and the outputs of the children give a critical input to g'.

From the inductive hypothesis we know that for $i = 1, \ldots, t$, the matroidal-read-once sub-formula under children i matches with the corresponding read-once formula on all its *critical* inputs. Moreover, f' matches with g' on all critical inputs of g'.

Now Theorem 4 easily follows from the above Observation and Theorem 2 in [1].

E An upper bound

The "sparse graph detection and extraction" described in Section 4.1 in [9] can be applied to any *sparse* Boolean function. In particular, matroid of rank r are r-sparse as every independent set has at most r elements.

Lemma 8 (cf. Childs and Kothari, Lemma 10 in [9]). *If $x : [n] \to \{0,1\}$ be a black-box function such that $|\{i \mid x(i) = 1\}| \leq k$ then quantum query complexity of constructing $\{i \mid x(i) = 1\}$ is $O(\sqrt{nk})$.*

Theorem 10 (Approximate quantum counting, Theorem 15 of [6]). *Let $x : [n] \to \{0,1\}$ be a black-box function with $|\{i \mid x(i) = 1\}| = K > 0$, and let $\epsilon \in (0,1]$. There is a quantum algorithm that produces an estimate $\tilde{k}$ of k satisfying $|k - \tilde{k}| \leq \epsilon k$ with probability at least $2/3$, using $O(\sqrt{nk}/\epsilon)$ queries to x. If $k = 0$, the algorithm outputs $\tilde{k} = 0$ with certainty in $O(\sqrt{n})$ queries.*

Proof of Theorem 8

Proof. The proof is identical to the proof of Theorem 11 in [9].

First reject the inputs x such that $|x| \geq 2r$ using Theorem 10 and then use Lemmma 8 to construct the entire x.