On the AC$^0[⊕]$ Complexity of Andreev’s Problem

Aditya Potukuchi
Department of Computer Science, Rutgers University, USA
http://paul.rutgers.edu/~ap1311/
aditya.potukuchi@cs.rutgers.edu

Abstract
Andreev’s Problem is the following: Given an integer $d$ and a subset of $S \subset \mathbb{F}_q \times \mathbb{F}_q$, is there a polynomial $y = p(x)$ of degree at most $d$ such that for every $a \in \mathbb{F}_q$, $(a, p(a)) \in S$? We show an AC$^0[⊕]$ lower bound for this problem.

This problem appears to be similar to the list recovery problem for degree-$d$ Reed-Solomon codes over $\mathbb{F}_q$ which states the following: Given subsets $A_1, \ldots, A_q$ of $\mathbb{F}_q$, output all (if any) the Reed-Solomon codewords contained in $A_1 \times \cdots \times A_q$. In particular, we study this problem when the lists $A_1, \ldots, A_q$ are randomly chosen, and are of a certain size. This may be of independent interest.

2012 ACM Subject Classification Theory of computation → Circuit complexity

Keywords and phrases List Recovery, Sharp Threshold, Fourier Analysis

Digital Object Identifier 10.4230/LIPIcs.FSTTCS.2019.25


Funding Aditya Potukuchi: Research supported in part by NSF grant CCF-1514164.

Acknowledgements I would like to thank Swastik Kopparty for the discussions that led to Section 5, and Bhargav Narayanan for the discussions that led to Theorem 8.

1 Introduction

For a prime power $q$, let us denote by $\mathbb{F}_q$, the finite field of order $q$. Let us denote the elements of $\mathbb{F}_q = \{a_1, \ldots, a_q\}$. One can think of $a_1, \ldots, a_q$ as some ordering of the elements of $\mathbb{F}_q$. Let $\mathcal{P}_d = \mathcal{P}_d^q$ be the set of all univariate polynomials of degree at most $d$ over $\mathbb{F}_q$. Let us define the problem which will be the main focus of this paper:

**Input:** A subset $S \subseteq \mathbb{F}_q^2$, and integer $d$.

**Output:** Is there a $p \in \mathcal{P}_d^q$ such that $\{(a_i, p(a_i)) \mid i \in [q]\} \subseteq S$?

The problem of proving NP-hardness of the above function seems to have been first asked in [11]. It was called “Andreev’s Problem” and still remains open. One may observe that above problem is closely related to the List Recovery of Reed-Solomon codes. In order to continue the discussion, we first define Reed-Solomon codes:

**Definition 1 (Reed-Solomon code).** The degree $d$ Reed-Solomon over $\mathbb{F}_q$, abbreviated as $\text{RS}[q, d]$ is the following set:

$$\text{RS}[q, d] = \{(p(a_1), \ldots, p(a_q)) \mid p \in \mathcal{P}_d^q\}$$

Reed-Solomon codes are one of the most widely (if not the most widely) studied families of error-correcting codes. It can be checked that $\text{RS}[q, d]$ is a $(d+1)$-dimensional subspace of $\mathbb{F}_q^q$ such that every non-zero vector has at least $q - d$ non-zero coordinates. In coding theoretic language, we say that $\text{RS}[q, d]$ is a linear code of block length $q$, dimension $d + 1$ and distance $q - d$. 

© Aditya Potukuchi; licensed under Creative Commons License CC-BY
Editors: Arkadev Chattopadhyay and Paul Gastin; Article No. 25; pp. 25:1–25:14
Leibniz International Proceedings in Informatics (LIPIcs)
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany
The List Recovery problem for a code $C \subset \mathbb{F}_q^n$ is defined as follows:

**Definition 2** (List Recovery problem for $C$).

**Input:** Sets $A_1, \ldots, A_n \subseteq \mathbb{F}_q$.

**Output:** $C \cap (A_1 \times \cdots \times A_n)$.

Given the way we have defined these problems, one can see that Andreev’s Problem is essentially proving NP-hardness for the List Recovery of Reed-Solomon codes where one just has to output a Boolean answer to the question

$$C \cap (A_1 \times \cdots \times A_n) \neq \emptyset?$$

Indeed, let us consider a List Recovery instance where the code $C$ is $RS[q,d]$, and the input sets are given by $A_1, \ldots, A_q$. Let us identify $(A_1, \ldots, A_q)$ with the set

$$S = \bigcup_{i \in [q]} \{(a_i, z) \mid z \in A_i\} \subseteq F_q^n$$

and let us identify every codeword $w = (w_1, \ldots, w_q) \in C$, with a set $w_{\text{set}} = \{(a_i, w_i) \mid i \in [q]\}$. Clearly, we have that $w \in A_1 \times \cdots \times A_q$ if and only if $w_{\text{set}} \subseteq S$. Often, we will drop the subscript on $w_{\text{set}}$ and refer to $w$ both as a codeword, and as the set of points it passes through. Further identifying $F_q^n$ with $[q]^2$, and parameterizing the problem by $r = \frac{d}{q}$, we view Andreev’s Problem as a Boolean function $AP_r : \{0,1\}^{q \times q} \rightarrow \{0,1\}$.

The main challenge here is to prove (or at least conditionally disprove) NP-hardness for Andreev’s Problem, which has been open for over 30 years. Another natural problem one could study is the circuit complexity for $AP_r$. This is the main motivation behind this paper, and we will study the $AC^0[\oplus]$ complexity of $AP_r$. We shall eventually see that even this problem needs relatively recent results about the power of $AC^0[\oplus]$ in our proof. Informally, $AC^0$ is the class of Boolean functions computable by circuits of constant depth, and polynomial size, using $\land$, $\lor$, and $\neg$ gates. $AC^0[\oplus]$ is the class of Boolean functions computable by circuits of constant depth, and polynomial size, using $\land$, $\lor$, $\neg$, and $\oplus$ (MOD$_2$) gates. The interested and unfamiliar reader is referred to [3] (Chapter 14) for a more formal definition and further motivation behind this class. We show that $AP_r$ cannot be computed by $AC^0$ circuits for a constant $r$. This type of result is essentially motivated by a similar trend in the study of the complexity of Minimum Circuit Size Problem. Informally, the Minimum Size Circuit Problem (or simply MCSP) takes as input a truth table of a function on $m$ bits, and an integer $s$. The output is 1 if there is a Boolean circuit that computes the function with the given truth table and has size at most $s$. It is a major open problem to show the NP-hardness of MCSP. A lot of effort has also gone into understanding the circuit complexity of MCSP. Allender et al. [2] proved a superpolynomial $AC^0$ lower bound, and Hirahara and Santanam [9] proved an almost-quadratic formula lower bound for MCSP. A recent result by Golonev et al. [8] extends [2] and proves an $AC^0[\oplus]$ lower bound for MCSP. Thus one can seek to answer the same question about $AP_r$.

We now state our main theorem:

**Theorem 3** (Main Theorem). For any prime power $q$, and $r \in (0,1)$, we have that any depth $h$ circuit with $\land$, $\lor$, $\neg$, and $\oplus$ gates that computes $AP_r$ on $q^2$ bits must have size at least $\exp(\tilde{O}(h q^{\frac{2}{r^2}}))$.

We make a remark about the theorem. The most glaring aspect is that $r \in (0,1)$ is more or less a limitation of our proof technique. Of course, as $r$ gets very small, i.e., $r = O\left(\frac{1}{\log q}\right)$, one can find depth 2 circuits of size $q^{O(rq)} = q^{O(1)}$. But, we do not know that the case where, for example, $r = \Theta\left(\frac{1}{\log q}\right)$ is any easier for $AC^0[\oplus]$. 

The List Recovery problem for a code $C \subset \mathbb{F}_q^n$ is defined as follows:
Related prior work: A result of Bogdanov and Safra

Shortly after this paper was uploaded, Bogdanov pointed out to us that an alternative proof of the \( \text{AC}^0[\oplus] \) lower bound can be obtained (using some other theorems that are also used in this paper) from [4] (specifically Theorem 14). As stated, this bound works in the regime \( d = Kq \) where \( 0.89 < K < 1 \). One difference in approach is that the lower bound here proceeds via showing that \( \text{AP}_r \) has a sharp threshold (see Definition 4) whereas in [4], the sharp threshold can be shown for an adversarially restricted version of this problem. We believe that the generality of techniques in this paper could find use elsewhere (for example, such as that in Section 5).

1.1 Results on sharp threshold for \( \text{AP}_c \)

For a \( p \in (0, 1) \), let \( X_1, X_2, \ldots \) denote independent \( \text{Ber}(p) \) random variables. For a family of Boolean functions \( f : \{0, 1\}^n \rightarrow \{0, 1\} \), we use \( f^{(n)}(p) \) to denote the random variable \( f(X_1, \ldots, X_n) \).

▶ Definition 4 (Sharp threshold). For a family of monotone functions \( f \), we say that \( f \) has a sharp threshold at a \( p \) if for every \( \epsilon > 0 \), there is an \( n_0 \) such that for every \( n > n_0 \), we have that \( \mathbb{P}(f^{(n)}(p(1 - \epsilon)) = 0) \geq 0.99 \), and \( \mathbb{P}(f^{(n)}(p(1 + \epsilon)) = 1) \geq 0.99 \).

Henceforth, we shall assume that \( q \) is a very large prime power. So, all the high probability events and asymptotics are as \( q \) grows. Where there is no ambiguity, we also just use \( f(p) \) to mean \( f^{(n)}(p) \) and \( n \) growing.

One limitation of \( \text{AC}^0[\oplus] \) that is exploited when proving lower bounds (including in [8]) for monotone functions is that \( \text{AC}^0[\oplus] \) cannot compute functions with “very” sharp thresholds. For a quantitative discussion, let us call the smallest \( \epsilon \) in the definition above the threshold interval. It is known that \( \text{AC}^0 \) (and therefore, \( \text{AC}^0[\oplus] \)) can compute (some) functions with threshold interval of \( O\left(\frac{1}{\log n}\right) \), for example, consider the following function on Boolean inputs \( z_1, \ldots, z_n \). Let \( Z_1 \sqcup \cdots \sqcup Z_{\ell} \) be an equipartition of \([n]\), such that each \( |Z_i| \approx \log n - \log \log n \). Consider the function given by

\[
f(z_1, \ldots, z_n) = \bigvee_{i \in [\ell]} \left( \bigwedge_{j \in Z_i} z_j \right).
\]

This is commonly known as the tribes function and is known to have a threshold interval of \( O\left(\frac{1}{\log n}\right) \). This is clearly computable by an \( \text{AC}^0 \) circuit. A construction from [12] gives an \( \text{AC}^0 \) circuit (in \( n \) inputs) of size \( n^\Theta(h) \) and depth \( h \) that has a threshold interval \( \tilde{O}\left(\frac{1}{(\log n)^{h-1}}\right) \). A remarkable result from [12] and [6] (Theorem 13 from [6] plus Lemma 3.2 in [1]) says that this is in some sense, tight. Formally,

▶ Theorem 5 ([12, 6]). Let \( n \) be any integer and \( f : \{0, 1\}^n \rightarrow \{0, 1\} \) be a function with threshold interval \( \delta \) at \( \frac{1}{2} \). Any depth \( h \) circuit with \( \wedge, \vee, \neg, \) and \( \oplus \) gates that computes \( f \) must have size at least \( \exp\left(\Omega\left(h (1/\delta)^{\frac{1}{h-1}}\right)\right) \).

This improves upon previous lower bounds by Shaltiel and Viola [14] who show a size lower bound of \( \exp\left(\left(1/\delta\right)^{\frac{1}{2-h}}\right) \). In [12], this was studied as the Coin Problem, which we will also define in Section 4. Given the above theorem, a natural strategy suggests itself. If we could execute the following two steps, then we would be done:
1. Establish Theorem 5 for functions with thresholds at points other than \( \frac{1}{2} \).
2. Show that \( \text{AP}_r \) has a sharp threshold at \( q^{-r} \) with a suitably small threshold interval, i.e.,
\[
\frac{1}{\text{poly} q^{\frac{1}{r}}}
\]
The first fact essentially reduces to approximating \( p \)-biased coins by unbiased coins in constant depth. Understanding the second part, naturally leads us to study \( \text{AP}_r^{p} \) for some \( p = p(q) \). Let \( A_1, \ldots, A_q \subset \mathbb{F}_q \) be independently chosen random subsets where each element is included in \( A_i \) with probability \( p \). Let \( C \) be the \( \text{RS}[q, rq] \) code. We have \( |C| = q^{rq} + 1 \). Let us denote
\[
X := |(A_1 \times \cdots \times A_q) \cap C|.
\]
For \( w \in C \), let \( X_w \) denote the indicator random variable for the event \( \{w \in A_1 \times \cdots \times A_q\} \).
Clearly, \( X = \sum_{w \in C} X_w \), and for every \( w \in C \), we have \( \mathbb{P}(X_w = 1) = p^{\frac{1}{r}} \). We first note that for \( \epsilon = \omega\left(\frac{\log q}{q}\right) \), and \( p = q^{-r}(1 - \epsilon) \), we have, using linearity of expectation,
\[
\mathbb{E}[X] = \sum_{w \in C} \mathbb{E}[X_w] = |C| \cdot \left(q^{-r}(1 - \epsilon)^q\right) = q^{rq+1} \left(q^{-r}(1 - \epsilon)^q\right) = q \cdot (1 - \epsilon)^q \leq q \cdot e^{-\epsilon q} = o(1).
\]
When \( p = q^{-r}(1 + \epsilon) \), using a similar calculation as above, we have
\[
\mathbb{E}[X] = q \cdot (1 + \epsilon)^q \geq q.
\]
To summarize, for \( \epsilon = \omega\left(\frac{\log q}{q}\right) \), and \( p = q^{-r}(1 - \epsilon) \), \( \mathbb{E}[X] \to 0 \), and for \( p = q^{-r}(1 + \epsilon) \), \( \mathbb{E}[X] \to \infty \).

\textbf{Lemma 6.} For \( \epsilon = \omega\left(\frac{\log q}{q}\right) \), we have
\[
\mathbb{P}(\text{AP}_{r}^{p}(q^{-r}(1 - \epsilon)) = 1) \leq \exp\left(-\Omega(\epsilon q)\right).
\]
\textbf{Proof.} This is just Markov’s inequality. We have \( \mathbb{P}(\text{AP}_{r}(p(1 - \epsilon)) = 0) = \mathbb{P}(X \geq 1) \leq \mathbb{E}[X] \leq q \cdot e^{-\epsilon q} = \exp\left(-\Omega(\epsilon q)\right) \).

This counts for half the proof of the sharp threshold for \( \text{AP}_r \). The other half forms the main technical contribution of this work. We show the following:

\textbf{Theorem 7.} Let \( q \) be a prime power, \( r = r(q) \) and \( \epsilon = \epsilon(q) \) be real numbers such that
\[
q^{-r} \geq \frac{\log q}{q} \quad \text{and} \quad \epsilon = \omega\left(\max\left\{q^{-r}, \sqrt{q^{-1} \log (q^{1-r})}\right\}\right).
\]
Let \( A_1, \ldots, A_q \) be independently chosen random subsets of \( \mathbb{F}_q \) with each point picked independently with probability \( q^{-r}(1 + \epsilon) \). Then
\[
\mathbb{P}((A_1 \times \cdots \times A_q) \cap \text{RS}[q, rq] = \emptyset) = o(1).
\]
First, we observe is that when $r$ is bounded away from 0 and 1, then $\epsilon = \frac{1}{\text{poly}(q)}$ suffices. The condition to focus on here is that $q^{-r} \geq \frac{\log q}{q}$. Indeed, one can see that this condition is necessary to ensure that w.h.p, all the $A_i$'s are nonempty. So, for example, if the dimension of $C$ is $q-1$, then setting $p = q^{-1}(1+\epsilon)$ is enough for $E[X] = \omega(1)$ but this does not translate to there almost surely being a codeword in $A_1 \times \cdots \times A_q$.

Lemma 6 and Theorem 7 together give us that AP$_r$ has a sharp threshold at
\[
\max\left\{q^{-r}, \frac{\log q}{q}\right\}
\]
whenever $1 - \frac{1}{q} \geq r \gg \frac{1}{\log p}$. For the sake of completeness one could ask if AP$_r$ has a threshold for all feasible values of $r$, and we show that the answer is yes. More formally,

▶ Theorem 8 (Sharp threshold for list recovery). For every $r = r(q)$, there is a critical $p = p(r,q)$ such that for every $\epsilon > 0$,
1. $\mathbb{P}(\text{AP}_r(p(1-\epsilon)) = 1) = o(1)$.
2. $\mathbb{P}(\text{AP}_r(p(1+\epsilon)) = 1) = 1 - o(1)$.

The case that is not handled by Theorem 7 is when $r = O(\frac{1}{\log q})$ (since in this case, Theorem 7 requires $\epsilon = \Omega(1))$. This corresponds to the case where $q^{-r}$ is a number bounded away from 0 and 1.

1.2 Results on random list recovery with errors

Given a random subset of points in $S \subseteq \mathbb{F}_q^2$, what is the largest fraction of any degree $d = \Theta(q)$ polynomial that is contained in this set? Using the Union Bound, it is easy to see that no polynomial of degree $d$ has more than $d \log \frac{1}{p} q + o(q)$ points contained in $S$ (formal details are given in Section 5). We show that perhaps unsurprisingly, this is the truth. Formally,

▶ Corollary 9. Let $S$ be a randomly chosen subset of $\mathbb{F}_q^2$ where each point is picked independently with probability $p$. Then with probability $1 - o(1)$,
\[
\max_{w \in \text{RS}[q,d]} |w \cap S| = d \log \frac{1}{p} q - O\left(\frac{q}{\log \left(\frac{1}{p}\right)}\right).
\]

We restrict our attention to the case when $d = \Theta(q)$, where the above statement is nontrivial. This is the content of Section 5. However, we believe that the statement should hold for all rates, and error (in general) better than $O\left(\frac{q}{\log q}\right)$.

2 Preliminaries

2.1 Properties of Reed-Solomon codes

We will state some basic facts about Reed-Solomon codes that will be used in the proof. The first one is that the dual vector space of a Reed-Solomon code is also a Reed-Solomon code.

▶ Fact 10. Let $C$ be a RS[q,d] code. Then $C^\perp = \text{RS}[q, q - d - 1]$.

For $t \neq 0$, let $W_t$ be the number of codewords of weight $t$ in RS[q,d]. We have the following simple bound.

▶ Proposition 11. We have $W_{q-i} \leq \frac{q^{i+1}}{i!}$. 
Proof. We have that $\mathcal{C}$ is a $d+1$-dimensional subspace of $\mathbb{F}^q$. Add $i$ extra constraints by choosing some set of $i$ coordinates and restricting them to 0. As long as $i < d$, these new constraints strictly reduce the dimension of $\mathcal{C}$. There are exactly $\binom{q}{i}$ ways to choose the coordinates, and the resulting space has dimension $d+1-i$. Therefore, the number of codewords of weight at most $q-i$ is at most $q^{d+1-i} \cdot \binom{q}{i} \leq \frac{q^{d+1-i}}{i!}$.

\[ \square \]

2.1.1 Punctured Reed-Solomon codes

All of the statements above when instead of Reed-Solomon codes, one considers punctured Reed-Solomon codes. For a $w = (w_1, \ldots, w_n) \in \mathbb{F}_q^n$, and a set $S \subset [n']$, let us define

$$w|_S = (w_i)_{i \in S}.$$ 

For a subset $C \subset \mathbb{F}_q^n$, let us define

$$C|_S := \{w |_S \mid w \in C\}.$$ 

We call $\text{RS}[q,d]|_S$ the $S$-punctured $\text{RS}[q,d]$ code. Let $C$ denote the $\text{RS}[q,d]|_n$ code. Since the properties we will care about are independent of the specific set $S$, let us just parametrize this by $|S| =: n$. The following properties hold

1. $C^\perp = \text{RS}[q,q-d-1]|_n$.
2. Let $W_i$ be the number of codewords in $C$ code of weight $i$. Then we have

$$W_{n-i} \leq q^{d+1-n} \cdot \frac{1}{i!}.$$ 

Both facts can be easily checked.

2.2 Basic probability inequalities

We will use the standard (multiplicative) Chernoff bound for sums of i.i.d. Bernoulli random variables. Let $X_1, \ldots, X_n$ be independent $\text{Ber}(p)$ random variables. Let $X := \sum_{i \in [n]} X_i$ and denote $\mu = E[X] = np$. Then for any $\epsilon \in (0,1)$, we have:

$$\mathbb{P}(|X - \mu| \geq \epsilon \mu) \leq e^{-\frac{\epsilon^2 \mu}{2}}. \quad (1)$$

We also have (a special case of) the Paley-Zygmund inequality, which states that for a nonnegative random variable $X$,

$$\mathbb{P}(X > 0) \geq \frac{E[X^2]}{E[X]^2}. \quad (2)$$

2.3 Fourier analysis over $\mathbb{F}_q$

For functions $u, v : \mathbb{F}_q^n \rightarrow \mathbb{C}$, we have a normalized inner product $\langle u, v \rangle := \frac{1}{q^n} \sum_{s \in \mathbb{F}_q^n} u(s)v(s)$. Consider any symmetric, non-degenerate bi-linear map $\chi : \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow \mathbb{R}/\mathbb{Z}$ (such a map exists). For an $\alpha \in \mathbb{F}_q^n$, the character function associated with $\alpha$, denoted by $\chi_\alpha : \mathbb{F}_q^n \rightarrow \mathbb{C}$ is given by $\chi_\alpha(x) = e^{-2\pi i \langle \alpha, x \rangle}$.

We have that for all distinct $\alpha, \beta \in \mathbb{F}_q$, we have that $\langle \chi_\alpha, \chi_\beta \rangle = 0$, and every function $f : \mathbb{F}_q \rightarrow \mathbb{C}$ can be written in a unique way as $f(x) = \sum_{\alpha \in \mathbb{F}_q} \hat{f}(\alpha) \chi_\alpha(x)$. Here the $\hat{f}(\alpha)$’s are called the Fourier coefficients, given by

$$\hat{f}(\alpha) = \langle f, \chi_\alpha \rangle.$$
We will state some facts that we will use in the proof of Theorem 7. The interested reader is referred to the excellent book of Tao and Vu [15] (chapter 4) for further details.

Fact 12 (Plancherel's Theorem). For functions \( f, g : \mathbb{F}_q^n \to \mathbb{C} \), we have
\[
(f, g) = \sum_{\alpha} \hat{f}(\alpha) \hat{g}(\alpha).
\]

Fact 13. Suppose \( g : \mathbb{F}_q^n \to \mathbb{C} \) can be written as a product \( g(x) = \prod_{i \in [t]} g_i(x) \), then we have the Fourier coefficients of \( g \) given by:
\[
\hat{g}(\alpha) = (\hat{g}_1 \cdots \hat{g}_t)(\alpha) = \sum_{\beta_1, \ldots, \beta_{t-1}} \hat{g}_1(\beta_1) \cdots \hat{g}_{t-1}(\beta_{t-1}) \hat{g}_t(\alpha - \sum_{i \in [t-1]} \beta_i).
\]

Fact 14. If \( g : \mathbb{F}_q^n \to \mathbb{C} \) is the indicator of a linear space \( C \), we have:
\[
\hat{g}(\alpha) = \begin{cases} \frac{|C|}{|\mathbb{F}_q|^n}, & \text{if } \alpha \in C^\perp \\ 0, & \text{otherwise.} \end{cases}
\]

2.4 Hypercontractivity and sharp thresholds

Here we state some tools from the analysis of Boolean function that we will use:

Definition 15. We say that a function \( f : \{0, 1\}^n \to \{0, 1\} \) is transitive-symmetric if for every \( i, j \in [n] \), there is a permutation \( \sigma \in S_n \) such that:
1. \( \sigma(i) = j \)
2. \( f(x_{\sigma(i)}, \ldots, x_{\sigma(n)}) = f(x) \) for all \( x \in \{0, 1\}^n \).

Let \( f : \{0, 1\} \to \{0, 1\} \) be a monotone function. We will state an important theorem by Friedgut and Kalai, as stated in the excellent reference [13], regarding sharp thresholds for balanced symmetric monotone Boolean functions. This will be another important tool that we will use.

Theorem 16 ([7]). Let \( f : \{0, 1\}^n \to \{0, 1\} \) be a nonconstant, monotone, transitive-symmetric function and let \( F : [0, 1] \to [0, 1] \) be the strictly increasing function defined by \( F(p) = P(f(p) = 1) \). Let \( p_{\text{crit}} \) be the critical probability such that \( F(p_{\text{crit}}) = 1/2 \) and assume without loss of generality that \( p_{\text{crit}} \leq 1/2 \). Fix \( 0 < \epsilon < 1/4 \) and let
\[
\eta = B \log(1/\epsilon) \cdot \frac{\log(1/p_{\text{crit}})}{\log n},
\]
where \( B > 0 \) is a universal constant. Then assuming \( \eta \leq 1/2 \),
\[
F(p_{\text{crit}} : (1 - \eta)) \leq \epsilon, \quad F(p_{\text{crit}} : (1 + \eta)) \geq 1 - \epsilon.
\]

We will use an immediate corollary of the above theorem.

Corollary 17. Let \( f : \{0, 1\}^n \to \{0, 1\} \) be a nonconstant, monotone, transitive-symmetric function. Let \( F : [0, 1] \to [0, 1] \) be the strictly increasing function defined by \( F(p) = Pr(f(p) = 1) \). Let \( p \) be such that \( F(p) \geq \epsilon \), and let \( \eta = B \log(1/\epsilon) \cdot \frac{\log(1/p)}{\log n} \). Then \( F(p(1 + 2\eta)) \geq 1 - \epsilon \).

In particular, in the above corollary, if for some \( \epsilon \in (0, 1) \) we have that \( F^{-1}(\epsilon) \in (0, 1) \), then the function \( f \) has a sharp threshold.

One easy observation that will allow us to use Theorem 16 is the following:

Proposition 18. The Boolean function \( AP_r : \{0, 1\}^{q \times n} \to \{0, 1\} \) is transitive-symmetric.

Proof. For a pair of coordinates indexed by \((i_1, j_1)\) and \((i_2, j_2)\), it is easy to see that the map \((x, y) \mapsto (x + i_2 - i_1, y + j_2 - j_1)\) gives us what we need since the set of polynomials is invariant under these operations.
3 Proof ideas of Theorem 7 and Theorem 8

Here, we sketch the proofs of the Theorem 7 and Theorem 8, which can be considered the two main technical contributions of this work. Due to space constraints, we do not reproduce the full proof. However, all the essential ideas are contained in Section 3.2 and Sec 3.3. First, we describe why some obvious approaches do not work.

3.1 What doesn’t work, and why

One obvious attempt to prove Theorem 7 is to consider the second moment of $X = |C \cap (A_1 \times \cdots \times A_q)|$ and hope that $E[X^2] = (1 + o(1))E[X]$. Unfortunately, $E[X^2]$ is too large. Through a very careful calculation using the weight distribution of Reed Solomon codes which we do not attempt to reproduce here, we have $E[X^2] = \Omega(e^{\frac{r}{2}}E^2[X])$. So in the regime where, for example, $p = q^{-\Omega(1)}$, this approach is unviable.

To understand this (without the aforementioned involved calculation) in an informal manner, let us fix $p = q^{-r}$ for some fixed constant $r$. Let us identify the tuple of sets $(A_1, \ldots, A_q)$ with the single set $S = \cup_{i \in [q]} \{(a_i, z) \mid z \in A_i\}$. So, we are choosing a random subset $S \subset \mathbb{F}_q^2$ of size $q^{2-r}$. On the other hand, the objects we are looking for, i.e., codewords, have size $q$. This is much larger than the standard deviation of $|S|$, which is of the order of $q^{1-(r/2)}$. Thus, conditioning on the existence of some codeword $w \subset \mathbb{F}_q^2$, the distribution of $S$ changes significantly. One way to see this is the following: Using standard Chernoff bounds, one can check that the size of $S$ is almost surely $q^{2-r} \pm O\left(q^{1-(r/2)} \log q\right)$. However, conditioned on $w \in A_1 \times \cdots \times A_q$, the size of $S$ is almost surely $q + q^{-r}(q^2 - q) \pm O\left(q^{1-(r/2)} \log q\right)$ (the additional $q$ comes from the points that make up $w$). This is much larger than before when $r$ is relatively large. On the other hand, the main point behind (successful) applications of the second moment method is that the distribution does not significantly change after such a conditioning.

One possible way to circumvent the above problem is to pick a uniformly random set $S \subset \mathbb{F}_q^2$ of size $q^{2-r}$, instead of every point independently with probability $q^{-r}$. This is a closely related distribution, and it is often the case that Theorems in this model are also true in the above “i.i.d.” model. This fact can be also be made formal (see, for example [10] Corollary 1.16). Here, when one conditions on the existence of some codeword $w$, at least $|S|$ does not change. Thus the second moment method is not ruled out right at the start. However, it seems to be much more technically involved and it is unclear if it is possible to obtain the relatively small threshold interval that is required for Theorem 3 in this way.

3.2 Proof sketch of Theorem 7

The key idea in the proof of this theorem is to count the number of polynomials in the “Fourier basis”. Let us consider $f : \mathbb{F}_q^2 \to \{0, 1\}$ to be the indicator of $C$. For $i \in [q]$, let $g_i : \mathbb{F}_q \to \{0, 1\}$ denote the indicator of $A_i$.

For an extremely brief and informal discussion, what we want is essentially $\langle f, \prod_{i \in [q]} g_i \rangle$, which, by Plancharell’s identity (see Fact 12) is $\sum_{\alpha} \hat{f} \cdot \prod_i g_i(\alpha)$. Since $C$ is a vector space, we have that $\hat{f}$ is supported on $C^\perp$. Moreover, $\hat{g}_i(\alpha)$ is much larger when $\alpha_i = 0$ than when $\alpha_i \neq 0$ if $A_i$ is random. This combined with the fact that most points in $C^\perp$ have large weight, and a bit more Fourier analysis means that the inner product, $\langle f, \prod_{i \in [q]} g_i \rangle$, is dominated by $f(0) \prod_{i \in [q]} \hat{g}_i(0)$ which is the expected number of codewords in $A_1 \times \cdots \times A_q$. 
Now we give a slightly less informal sketch.

**Proof sketch of Theorem 7.** What we are trying to estimate is exactly

\[ X = |C \cap (A_1 \times \cdots \times A_q)| = \sum_{x_1, \ldots, x_q} f(x) \left( \prod_{i \in [q]} g_i(x_i) \right). \]

Using Fourier analysis over \( F_q \), one can show that

\[ \frac{q^q}{|C|} \cdot X = \sum_{(\alpha_1, \ldots, \alpha_q) \in C^+} \prod_{i \in [q]} \hat{g}_i(\alpha_i) \]

\[ \geq \prod_{i \in [q]} \hat{g}_i(0) - \sum_{(\alpha_1, \ldots, \alpha_q) \in C^+ \setminus \{0\}} \left( \prod_{i \in [q]} \hat{g}_i(\alpha_i) \right). \]  

(3)

Using the fact that \( C \) is an RS\([q, rq]\) code, one has (see Fact 10) that \( C^\perp \) is an RS\([q, q-rq-1]\) code. What will eventually help in the proof is that the weight distribution of Reed Solomon codes (and so in particular, \( C^\perp \)) is well understood.

Now clearly, it suffices to understand the term \( \sum_{(\alpha_1, \ldots, \alpha_q) \in C^+} \left( \prod_{i \in [q]} \hat{g}_i(\alpha_i) \right) =: R \). One way to control \( |R| \) is to control \( |R|^2 = R \overline{R} \). Here, one can use the fact that the \( A_i \)'s are randomly and independently chosen to establish cancellation in many terms of \( E[|R|^2] \). More precisely, one can prove that

\[ E[|R|^2] = \sum_{(\alpha_1, \ldots, \alpha_q) \in C^+ \setminus \{0\}} E[|\hat{g}_i(\alpha_i)|^2]. \]  

(4)

It is a more or less standard fact that if \( A_i \) is a uniformly random set where every element is included with probability \( p \) independently, then

\[ E[|\hat{g}_i(0)|^2] = p^2 + \frac{p(1-p)}{q} \]  

(5)

and

\[ E[|\hat{g}_i(\alpha_i)|^2] = \frac{p(1-p)}{q} \]  

for \( \alpha_i \neq 0 \).  

(6)

This difference, will be the reason why \( |R| \) is typically much smaller than \( \prod_{i \in [q]} \hat{g}_i(0) \).

To continue, let us rewrite (4) using (5) and (6) as

\[ E[|R|^2] \leq \sum_{i=0}^{n-1} \sum_{\alpha \in C^+ \setminus \{0\}, \text{wt}(\alpha) = n-i} \left( p^2 + \frac{p(1-p)}{q} \right)^{i} \left( \frac{p(1-p)}{q} \right)^{n-i} \]

\[ \leq \sum_{i=0}^{n-1} q^{q-rq} \left( p^2 + \frac{p(1-p)}{q} \right)^{i} \left( \frac{p(1-p)}{q} \right)^{n-i} \]

The last inequality is using the fact that \( C^\perp \) is a RS\([q, q-rq-1]\) code (Fact 10) and thus we understand its weight distribution (Proposition 11). This quantity can be shown to be at most \( e \cdot (1-p)^q \cdot q^{q-rq} \left( \frac{p}{q} \right)^q e^{\left( \frac{r q^2}{p} \right)} \) and so Markov’s inequality gives that with probability at least \( 1 - \frac{1}{q} \), one has that

\[ |R| \leq \left( e q \cdot (1-p)^q \cdot q^{q-rq} \left( \frac{p}{q} \right)^q e^{\left( \frac{r q^2}{p} \right)} \right)^{\frac{1}{2}}. \]  

(7)

On the other hand, using standard large deviation inequalities (1), we have the following:
Claim 19. For $q, c$ as given above, let $\epsilon = \omega\left(\sqrt{q^{c-1}\log(q^{1-r})}\right)$, and $p = q^{-r}(1 + \epsilon)$. Then with probability $1 - o(1)$, we have:

$$\prod_{i \in [q]} \widehat{g}_i(0) \geq q^{-rq}(1 + 0.9\epsilon)^{0.9q}.$$  \hspace{1cm} (8)

What remains to be checked is that for the given range of parameters, plugging in the estimates from (8) and (7) inside (3) gives us that $X > 0$, which completes the proof. ◀

### 3.3 Proof sketch of Theorem 8

The starting point of Theorem 8 is noticing that the only case not covered by Theorem 7 is $p \in (0, 1)$ is some fixed constant, or equivalently $r = O\left(\frac{1}{\log q}\right)$.

**Proof sketch of Theorem 8.** Here we have a somewhat crude weight distribution result for Reed Solomon codes (Proposition 11) to compute the second moment. We first show that $E[X^2] = O\left(e^p E[X^2]\right)$. Using, for example the Paley-Zygmund Inequality (2), this means that $\mathbb{P}(X > 0) \geq \Omega(e^{-\frac{1}{p}})$. Thus we have that $\{X > 0\}$ with at least some (possibly small) constant probability. But what we need is that $\mathbb{P}(X > 0) \geq 0.99$. For this, we now use the fact that $\text{AP}_r$ is monotone and transitive-symmetric. So Corollary 17) gives that for $p' = p + O\left(\frac{1}{\log q}\right)$, we have that $\mathbb{P}(\text{AP}_r(p') = 1) \geq 0.99$. ◀

### 4 AC$^0[⊕]$ lower bound for $\text{AP}_r$

We prove the lower bound by showing that $\text{AP}_r$ solves a biased version of the *Coin Problem*, and use the lower bounds known for such kinds of functions, obtained by [12], [6].

**Definition 20 ($p, \epsilon$-coin problem).** We say that a circuit $C = C^n$ on $n$ inputs solves the $(p, \epsilon)$-coin problem if

- For $X_1, \ldots, X_n \sim \text{Ber}(p(1 - \epsilon))$,
  $$\mathbb{P}(C(X_1, \ldots, X_n) = 0) \geq 0.99$$
- For $X_1, \ldots, X_n \sim \text{Ber}(p(1 + \epsilon))$,
  $$\mathbb{P}(C(X_1, \ldots, X_n) = 1) \geq 0.99$$

The $(\frac{1}{2}, \epsilon)$-Coin Problem was explicitly introduced in [5]. We shall abbreviate the $(p, \epsilon)$-Coin Problem on $n$ variables as $\text{CP}^n(p, \epsilon)$. We observe that a function $f : \{0, 1\}^n \rightarrow \{0, 1\}$ solves $\text{CP}^n(p, \epsilon)$ if it has a sharp threshold at $p$ with threshold interval at most $\epsilon$. The one obstacle we have to overcome in using Theorem 5 is that $\text{AP}_r$ has a sharp threshold at $p^{-c} \ll \frac{1}{2}$. However, we will show how to simulate biased Bernoulli r.v.’s from almost unbiased ones. Let $C(s, d)$ to denote the class of functions on $n$ variables which have circuits of size $O(s) = O(s(n))$ and depth $d = d(n)$ using $\land, \lor, \neg$, and $\oplus$ gates. Here, we make the following simple observation about the power of AC$^0[⊕]$ circuits to solve biased and unbiased $\epsilon$-coin problem. First, we observe that it is possible to simulate a biased coin using an unbiased one.
\textbf{Lemma 21.} Let $s$ be such that $\frac{1}{2^s} \leq p \in (0,1)$, and $\epsilon \leq \frac{1}{2s^2}$ for a large constant $K$. Then, there is a CNF $F_p$ on $t \leq s^2$-variables such that for inputs $X_1, \ldots, X_t \in \text{Ber} \left( \frac{1}{2} + \epsilon \right)$,
\[
\mathbb{P}(F_p(X_1, \ldots, X_t) = 1) = p(1 + \Omega(\epsilon L))
\]
and for inputs $X_1, \ldots, X_t \in \text{Ber} \left( \frac{1}{2} - \epsilon \right)$,
\[
\mathbb{P}(F_p(X_1, \ldots, X_t) = 1) = p \left( 1 + \frac{1}{2^{2n(\sqrt{n})}} - \Omega(\epsilon L) \right)
\]
where $L = \lceil \log_2(1/p) \rceil$.

The idea is essentially that the AND of $k$ unbiased coin is a $2^{-k}$-biased coin. However, some extra work has to be done if we want other biases (say, $(0.15) \cdot 2^k$). We give a sketch of the proof.

\textbf{Proof Sketch.} Consider the sequence of integers $\{k_i\}_{i \in \mathbb{N}}$ such that for every $i$, $k_i$ is the largest such that
\[
\prod_{j=1}^i \left( 1 - \frac{1}{2^j} \right)^{k_j} \geq p.
\]
We make a basic observation:

\textbf{Observation 22.} We have that $k_1 = \lceil \log_2(1/p) \rceil \leq s$ and for all $j \geq 2$, we have that $k_j \leq 3$.

Let $\ell$ be the largest such that $k_\ell > 0$ and $\sum_{i \in [\ell]} i \cdot k_i < s^2$. Let $t = \sum_{i \in [\ell]} i \cdot k_i$. Consider the CNF given by
\[
C_p = \bigwedge_{j \in [\ell]} \left( \bigwedge_{i \in k_j} \bigwedge_{j \in \mathbb{N}} C^j_i \right)
\]
where the clause $C^j_i$ is an $\bigvee$ of $j$ independent variables. It remains to check that $C_p$ satisfies the required properties.

This lemma now gives us the following:

\textbf{Lemma 23.} Let $z \in (0,1)$ be a fixed constant. If $CP^n \left( \frac{1}{z^3}, o(\epsilon \log n) \right) \in C^z(s,h)$, then there is a $t \leq \log^2 n$ such that $CP^{nt} \left( \frac{1}{2}, \epsilon \right) \in C^{nt}(z \epsilon \log n, h + 2)$.

\textbf{Proof.} Let $C$ be a circuit for $CP^n \left( \frac{1}{z^3}, \delta \right)$-coin problem. Replace each input variable with the CNF $F_\left( \frac{1}{16} \right)$ from Lemma 21 on $t = O(\log^4 n)$ independent variables. Call this circuit $C'$, on $tn$ variables. If the bias of each of these input variables is $\frac{1}{2} + \epsilon$, then the guarantee of Lemma 21 is that output of the and gate is $1$ with probability at least $\frac{1}{2^t}(1 + \Omega(\epsilon \log n))$.

A similar computation gives that if the bias of the inputs are $\left( \frac{1}{2} - \epsilon \right)$, then the bias of the output is at most $\frac{1}{2^t}(1 - \Omega(\epsilon \log n))$. Therefore, $C'$ solves $CP^{nt} \left( \frac{1}{2}, \epsilon \right)$, and has size at most $s \log n$, and depth $h + 2$.

Theorem 7 and Lemma 6, together, now give us the following corollary:

\textbf{Corollary 24.} Let $q$ be a large enough prime power. Then $AP_r$ on $q^2$ inputs solves the $(q^{-r}, \epsilon)$ coin problem, for $\epsilon = \omega \left( \max \left\{ q^{-r}, q^{-\frac{r+2}{2}} \right\} \right)$.
As a result, Theorem 5, and Lemma 21, and Lemma 23 together, give us the following bounded depth circuit lower bound for \( AP_r \):

**Theorem 3 (Restated).** For any \( r \in (0,1) \), and \( h \in \mathbb{N} \), we have that

\[
AP_r \not\subseteq C \left( \exp \left\{ \Omega \left( h q^{\frac{2}{q^d}} \right) \right\}, h \right).
\]

## 5 Random list recovery with errors

In this section, we shall again consider Reed-Solomon codes \( RS[q, rq] \) where \( r \) is some constant between 0 and 1. Let us slightly abuse notation, as before, and think of a codeword \( w \in RS[q, rq] \) corresponding to a polynomial \( p(X) \) as the set of all the zeroes of the polynomial \( Y = p(X) \). That is, for a codeword \( w = (w_1, \ldots, w_q) \) associated with polynomial \( p \), we think of \( w \) as a subset \( \{ (a_i, p(a_i)) \mid i \in [q] \} \) (recall that \( F = \{a_1, \ldots, a_q\} \)). For a set of points \( S \subset F_q^2 \) and a codeword \( w \) we say the agreement between \( w \) and \( S \) to denote the quantity \( |w \cap S| \). For a code \( C \), we say that the agreement between \( C \) and \( S \) to denote \( \max_{w \in C} |m \cap S| \).

We are interested in the following question: For a set \( S \subset F_q^2 \). What is the smallest \( \ell \) such that there exists a \( w \in RS[q, rq] \) such that \( |w \cap S| \geq q - \ell \)? In other words, what is the largest agreement between \( RS[q, rq] \) and \( S \)? This is (very close to) the list recovery problem for codes with errors. Naturally, we seek to answer this question when \( S \) is chosen randomly in an i.i.d. fashion with probability \( p \). Theorem 7 gives asymptotically tight bounds in a relatively straightforward way for constant error rate.

One can observe that the only properties about Reed-Solomon codes that was used in Theorem 7 was the weight distribution in the dual space of codewords. However, (see Section 2.1.1) these are also true for punctured Reed-Solomon codes. So, an analogous theorem also holds for punctured Reed-Salom codes. Formally,

**Theorem 25.** Let \( q, n, d \) be integers such that \( q \) is a prime power and \( n = \omega(\log q) \), and \( q^{-\frac{d}{q}} \geq \frac{\log n}{q} \) and let \( \epsilon = \omega \left( \max \left\{ q^{-\frac{d}{q}}, q^{1-\frac{d}{q}} \right\} \log \left( q^{1-\frac{d}{q}} \right) \right) \). Let \( C \) be an \( RS[q, d] |_{n} \) code.

Let \( A_1, \ldots, A_{\ell} \) be independently chosen random subsets of \( F_q \) with each point picked independently with probability \( q^{-\frac{d}{q}} (1 + \epsilon) \). Then

\[
P( (A_1 \times \cdots \times A_{\ell}) \cap C = \emptyset ) = o(1).
\]

We do not repeat the proof but is it the exact same as that of Theorem 7. Let \( E_a \) denote the event that the agreement between \( S \) and \( RS[q, rq] \) is \( a \). Union bound gives us that

\[
P( E_{q-\ell} ) \leq \binom{q}{\ell} q^{r q + 1} p^{q - \ell}.
\]

So if \( \ell \) is such that the RHS of 9 is \( o(1) \). Then the agreement is almost surely less than \( q - \ell \).

For the other direction, we have the following corollary:

**Corollary 26.** Let \( \epsilon \geq \max \left\{ 10q^{-\frac{d}{q}}, \sqrt{q^{-\frac{d}{q}} \cdot \log q} \right\} \). Let \( S \) be a randomly chosen subset of \( F_q^2 \) with each point picked independently with probability at least \( q^{-\frac{d}{q}} (1 + \epsilon) \), then with probability at least \( 1-o(1) \), the agreement between \( S \) and \( RS[q, d] \) is at least \( q - \ell \).
**Proof.** For $i \in [q - \ell]$, let us denote $S_i := \{j \mid (i, j) \in S\}$.

Let us use $S' := S_1 \times \cdots \times S_{q-\ell}$. Let us denote $\mathcal{C} = \text{RS}[q, d]|_{q-\ell}$. Formally, for a codeword $w \in \text{RS}[q, d]$, denote $p_w$ to be the polynomial corresponding to $m$. We have

$$\mathcal{C} = \{(i, p_w(i)) \mid i \in [q - \ell]\}$$

We observe that the conditions in Theorem 7 hold, so

$$\mathbb{P}(C' \cap S' = \emptyset) = o(1)$$

as desired.

**Corollary 9 (Restated).** Given a random subset $S \subseteq \mathbb{F}_q^2$ where each point is picked with probability $p$, then with probability at least $1 - o(1)$, the largest agreement $\text{RS}[q, d]$ with $S$ is $d \log \frac{q}{p} q = O\left(\frac{q}{\log(\frac{1}{p})}\right)$.

**Proof.** Let $a$ be an integer that denotes the maximum agreement between $S$ and $\text{RS}(q, d)$. Suppose that $a \leq d \log \frac{q}{p} q$, then setting $\ell = q - a$, and noting that the conditions for Corollary 26 are satisfied, we get that with probability at least $1 - o(1)$, there is a polynomial that agrees with the set $S$ in the first $q - \ell$ coordinates. On the other hand, if $a \geq d \log \frac{q}{p} q + 4 \frac{q}{\log(\frac{1}{p})}$, again, setting $\ell = q - a$, Union Bound gives us:

$$\mathbb{P}(E_{q-\ell}) \leq \sum_{w \in \mathcal{C}} \sum_{P \subseteq \mathbb{F}_q \mid |P| = q - \ell} \mathbb{P}(w \mid P \subseteq S)$$

$$= \binom{q}{\ell} q^{d+1} p^{q-r}$$

$$\ll \frac{1}{q}.$$

And so we have that with probability at least $1 - o(1)$, the agreement of $\text{RS}(q, d)$ with $S$ is $d \log \frac{q}{p} q = O\left(\frac{q}{\log(\frac{1}{p})}\right)$.

**6 Conclusion**

We started off by attempting to prove a bounded depth circuit lower bound for Andreev’s Problem. This led us into (the decision version of the) random List Recovery of Reed-Solomon codes. Here we show a sharp threshold for a wide range of parameters, with nontrivial threshold intervals in some cases. However, one of the unsatisfactory aspects about Theorem 8 is that it is proved in a relatively “hands-off” way possibly resulting in a suboptimal guarantee on $\epsilon$. The obvious open problem that is the following:

**Open Problem.** Is Theorem 8 true with a better bound on $\epsilon$?

If it is true with a much smaller $\epsilon$, it would extend in a straightforward way to the $\text{AC}^0[\oplus]$ lower bound as well. Another point we would like to make is that the only thing stopping us from proving Theorem 8 for general MDS codes is the lack of Proposition 18.
On the $\text{AC}^0[⊕]$ Complexity of Andreev’s Problem

References