# IMPROVED LOWER BOUND FOR DIFFERENCE BASES

ANTON BERNSHTEYN AND MICHAEL TAIT

Abstract. A difference basis with respect to $n$ is a subset $A \subseteq \mathbb{Z}$ such that $A - A \supseteq \{1, \ldots, n\}$. Rédei and Rényi showed that the minimum size of a difference basis with respect to $n$ is $(c + o(1))\sqrt{n}$ for some positive constant $c$. The best previously known lower bound on $c$ is $c \geqslant 1.5602\ldots$, which was obtained by Leech using a version of an earlier argument due to Rédei and Rényi. In this note we use Fourier-analytic tools to show that the Leech–Rédei–Rényi lower bound is not sharp.

## 1. Introduction

We use $\mathbb{N}$ (resp. $\mathbb{N}^+$) to denote the set of all nonnegative (resp. positive) integers. For $n \in \mathbb{N}^+$, let $[n] := \{1, \ldots, n\}$ and $[-n] := \{-n, \ldots, -1\}$. Given $A \subseteq \mathbb{Z}$, we write $A - A := \{a - b \,:\, a, b \in A\}$.

A set $A \subseteq \mathbb{Z}$ is called a **difference basis with respect to** $n$ if $A - A \supseteq [n]$. In this note we address the following problem, first raised by Rédei and Rényi [RR49]:

**Problem 1.1.** For given $n \in \mathbb{N}^+$, what is the minimum size of a difference basis with respect to $n$?

Problem 1.1, while it is a natural combinatorial number theory question in its own right, also has applications to graceful labelings of graphs [Gol72b; GS80], to symmetric intersecting families of sets [EKN17], and to signal processing [Hay+92; LST93; Mof68].

Let $\mathsf{D}(n)$ denote the smallest size of a difference basis with respect to $n$. In their seminal paper [RR49], Rédei and Rényi showed that the limit

$$\mathsf{d}^* := \lim_{n \to \infty} \frac{\mathsf{D}(n)^2}{n}$$

exists. Clearly, if $[n] \subseteq A - A$, then $n \leqslant \binom{|A|}{2}$, and hence $\mathsf{d}^* \geqslant 2$. On the other hand, it is not hard to give a construction that shows $\mathsf{d}^* \leqslant 4$. It turns out that both these bounds can be improved. In particular, Rédei and Rényi [RR49] showed that

$$2.4244\ldots = 2 + \frac{4}{3\pi} \leqslant \mathsf{d}^* \leqslant \frac{8}{3} = 2.6666\ldots.$$

Leech [Lee56] found a way to improve the Rédei–Rényi construction to derive the upper bound $\mathsf{d}^* \leqslant 2.6646\ldots$. This was further improved by Golay [Gol72a] to $\mathsf{d}^* \leqslant 2.6458\ldots$.

In this note we are interested in lower bounds on $\mathsf{d}^*$. Here, again, the result of Rédei and Rényi was improved by Leech [Lee56], who noticed that the argument from [RR49] depends on a certain parameter $\vartheta$ (taken by Rédei and Rényi to be $\vartheta = 3\pi/2$) and that making the optimal choice for $\vartheta$ gives the following:

**Theorem 1.2** (Leech–Rédei–Rényi [Lee56])**.** *We have*

$$\mathsf{d}^* \geqslant 2 - 2 \inf_{\vartheta \neq 0} \frac{\sin(\vartheta)}{\vartheta} = 2.4344\ldots.$$

The contribution of this paper is to show that the bound in Theorem 1.2 is not sharp:

Department of Mathematical Sciences, Carnegie Mellon University, Pittsburgh, PA, 15213, USA

*E-mail addresses*: abernsht@math.cmu.edu, mtait@cmu.edu.

Research of the second author is supported in part by NSF grant DMS-1606350.

**Theorem 1.3.** *There exists $\varepsilon > 0$ such that*

$$\mathsf{d}^* \;\geqslant\; \varepsilon + 2 - 2\inf_{\vartheta \neq 0} \frac{\sin(\vartheta)}{\vartheta}.$$

Our numerical computations suggest that $\varepsilon$ in Theorem 1.3 can be taken to be around $10^{-3}$. However, we did not make an effort to optimize $\varepsilon$, since it is unclear how close the best lower bound that our methods can give is to the correct value of $\mathsf{d}^*$.

Our proof techniques are Fourier-analytic. The original approach of Rédei and Rényi can be formulated in terms of looking at the first Fourier coefficient of a certain probability measure on the unit circle. Essentially, we show that taking into account higher Fourier coefficients leads to better lower bounds on $\mathsf{d}^*$.

## 2. Preliminaries

**Measures.** For a nonempty finite set $A$, $\mathsf{uni}(A)$ denotes the uniform probability measure on $A$. For a function $\varphi\colon X \to Y$ and a measure $\mu$ on $X$, the pushforward of $\mu$ by $\varphi$ is denoted by $\varphi_*(\mu)$.

**The space of measures.** Let $X$ be a compact metric space. We use $\mathrm{Prob}(X)$ to denote the space of all probability Borel measures on $X$ equipped with the usual weak-$*$ topology (see, e.g., [Kec95, §17.E]). Note that the space $\mathrm{Prob}(X)$ is compact and metrizable [Kec95, Theorem 17.22].

**Measures on the unit circle.** Let $\mathbb{T} \coloneqq \{z \in \mathbb{C} \,:\, |z| = 1\}$ be the unit circle in the complex plane, viewed as a compact Abelian group. Given a measure $\mu \in \mathrm{Prob}(\mathbb{T})$, we use $\overline{\mu}$ to denote the pushforward of $\mu$ by the conjugation map $\mathbb{T} \to \mathbb{T}\colon z \mapsto \overline{z}$. The **Fourier transform** of a measure $\mu \in \mathrm{Prob}(\mathbb{T})$ is the function $\widehat{\mu}\colon \mathbb{Z} \to \mathbb{C}$ defined by the formula

$$\widehat{\mu}(k) \;\coloneqq\; \int_{\mathbb{T}} z^k \,\mathrm{d}\mu(z).$$

The values $\widehat{\mu}(k)$ are referred to as the **Fourier coefficients** of $\mu$. We shall make use of the following basic observation:

**Lemma 2.1.** *Let $\mu$ be a probability measure on $\mathbb{T}$ and let $A$ be the $n$-by-$n$ matrix with entries*

$$A(i,j) \coloneqq \widehat{\mu}(j-i), \qquad \text{for all } 1 \leqslant i,\, j \leqslant n.$$

*Then $A$ is Hermitian and positive semidefinite.*

Proof. That $A$ is Hermitian is clear. To show that $A$ is positive semidefinite, take any $w \in \mathbb{C}^n$. Viewing $w$ as a column vector, we compute

$$\begin{aligned}\langle Aw, w\rangle \;&=\; \sum_{i=1}^n \sum_{j=1}^n A(i,j)\overline{w_i}w_j \;=\; \sum_{i=1}^n \sum_{j=1}^n \widehat{\mu}(j-i)\overline{w_i}w_j \;=\; \sum_{i=1}^n \sum_{j=1}^n \int_{\mathbb{T}} z^{j-i}\,\mathrm{d}\mu(z)\overline{w_i}w_j \\ &=\; \int_{\mathbb{T}} \sum_{i=1}^n \sum_{j=1}^n \overline{(w_i z^i)}(w_j z^j)\,\mathrm{d}\mu(z) \;=\; \int_{\mathbb{T}} \left|\sum_{i=1}^n w_i z^i\right|^2 \mathrm{d}\mu(z) \;\geqslant\; 0. \qquad \blacksquare\end{aligned}$$

It will be useful to remember that if a Hermitian matrix $A$ is positive-semidefinite, then so is the real symmetric matrix whose entries are the real parts of the corresponding entries of $A$.

For completeness, we record here the converse of Lemma 2.1 (although we will not need it):

**Theorem 2.2** (Bochner–Herglotz [Rud90, §1.4.3])**.** *Let $f\colon \mathbb{Z} \to \mathbb{C}$ be a function such that $f(0) = 1$, $f(-k) = \overline{f(k)}$ for all $k \in \mathbb{Z}$, and for each $n \in \mathbb{N}^+$, the $n$-by-$n$ matrix $A$ with entries $A(i,j) \coloneqq f(j-i)$ is positive semidefinite. Then there exists a unique probability measure $\mu \in \mathrm{Prob}(\mathbb{T})$ with $f = \widehat{\mu}$.*

**Convolutions of measures.** Given two probability measures $\mu$, $\nu$ on $\mathbb{T}$, their **convolution** is the probability measure $\mu * \nu$ on $\mathbb{T}$ given by

$$\int_{\mathbb{T}} f(z)\,\mathrm{d}(\mu * \nu)(z) \;:=\; \int_{\mathbb{T}\times\mathbb{T}} f(xy)\,\mathrm{d}(\mu \times \nu)(x,y) \;=\; \int_{\mathbb{T}}\int_{\mathbb{T}} f(xy)\,\mathrm{d}\mu(x)\,\mathrm{d}\nu(y).$$

Notice that the Fourier transform turns convolution into multiplication, in the sense that

$$\widehat{\mu * \nu}(k) \;=\; \widehat{\mu}(k)\widehat{\nu}(k) \qquad \text{for all } k \in \mathbb{Z}.$$

## 3. Proof of Theorem 1.3

In this section we prove Theorem 1.3, without making any attempt to compute an exact value for $\varepsilon$. Let $\vartheta = 4.4934\ldots$ be the value for which $\sin(\vartheta)/\vartheta$ is minimized (so $\sin(\vartheta)/\vartheta = -0.2172\ldots$). Suppose, towards a contradiction, that there is an infinite set of "bad" integers $B \subseteq \mathbb{N}^+$ and a way to assign to every $n \in B$ a difference basis $A_n \subset \mathbb{Z}$ with respect to $n$ so that

$$|A_n|^2 \;\leqslant\; \left(2 - \frac{2\sin(\vartheta)}{\vartheta} + o(1)\right) n \;=\; (2.4344\ldots + o(1))n. \tag{3.1}$$

Take any $n \in B$ and let $\alpha_n := |A_n|^2/n - 2$, so $|A_n|^2 = (2+\alpha_n)n$. Let $\varphi_n \colon \mathbb{Z} \to \mathbb{T}$ be the function given by $\varphi_n(k) := \exp(\vartheta i k/n)$, and define the following two measures on $\mathbb{T}$:

$$\mu_n := (\varphi_n)_*(\mathsf{uni}(A_n)) \qquad \text{and} \qquad \nu_n := (\varphi_n)_*(\mathsf{uni}([-n] \cup [n])).$$

Notice that $A_n - A_n \supseteq [-n] \cup [n]$, and hence we can express the convolution $\mu_n * \overline{\mu_n}$ as follows:

$$\mu_n * \overline{\mu_n} \;=\; \frac{2}{2+\alpha_n}\nu_n + \frac{\alpha_n}{2+\alpha_n}\zeta_n, \tag{3.2}$$

for some $\zeta_n \in \mathrm{Prob}(\mathbb{T})$. Now we pass to the limit as $n$ tends to infinity. Let $\varphi \colon [-1;1] \to \mathbb{T}$ be the map given by $\varphi(a) := \exp(\vartheta i a)$, and let

$$\nu := \varphi_*(\lambda),$$

where $\lambda$ is the uniform probability measure on the interval $[-1;1]$. It is then clear that

$$\nu = \lim_{n\in B} \nu_n.$$

Upon replacing $B$ by a subset if necessary, we may also assume that the following limits exist:

$$\alpha := \lim_{n\in B}\alpha_n, \qquad \mu := \lim_{n\in B}\mu_n, \qquad \text{and} \qquad \zeta := \lim_{n\in B}\zeta_n.$$

By (3.1), we have $\alpha \leqslant -2\sin(\vartheta)/\vartheta = 0.4344\ldots$, while from (3.2), we conclude that

$$\mu * \overline{\mu} \;=\; \frac{2}{2+\alpha}\nu + \frac{\alpha}{2+\alpha}\zeta. \tag{3.3}$$

**Lemma 3.4.** *The Fourier coefficients of $\nu$ are $\widehat{\nu}(0) = 1$ and $\widehat{\nu}(k) = \sin(k\vartheta)/(k\vartheta)$ for all $k \neq 0$.*

Proof. A straightforward direct computation. ■

Let $\delta_1$ denote the Dirac probability measure concentrated at $1 \in \mathbb{T}$.

**Corollary 3.5.** *The following statements are valid:*

$$\alpha = -2\sin(\vartheta)/\vartheta; \qquad \widehat{\mu}(1) = 0; \qquad \textit{and} \qquad \zeta = \delta_1.$$

Proof. From (3.3) and Lemma 3.4, we obtain

$$\begin{aligned} 0 \;\leqslant\; |\widehat{\mu}(1)|^2 \;=\; \widehat{\mu * \overline{\mu}}(1) \;&=\; \frac{2}{2+\alpha}\widehat{\nu}(1) + \frac{\alpha}{2+\alpha}\widehat{\zeta}(1) \\ &=\; \frac{2}{2+\alpha}\cdot\frac{\sin(\vartheta)}{\vartheta} + \frac{\alpha}{2+\alpha}\widehat{\zeta}(1) \;\leqslant\; \frac{2}{2+\alpha}\cdot\frac{\sin(\vartheta)}{\vartheta} + \frac{\alpha}{2+\alpha}, \end{aligned} \tag{3.6}$$

and therefore $\alpha \geqslant -2\sin(\vartheta)/\vartheta$ (this is essentially the Leech–Rédei–Rényi's proof of Theorem 1.2). Since $\alpha \leqslant -2\sin(\vartheta)/\vartheta$ by assumption, we conclude that $\alpha = -2\sin(\vartheta)/\vartheta$ and neither of the two inequalities in (3.6) can be strict, which means that

$$\widehat{\mu}(1) = 0 \qquad \text{and} \qquad \widehat{\zeta}(1) = 1.$$

Since $\delta_1$ is the only probability measure on $\mathbb{T}$ whose first Fourier coefficient is 1, we have $\zeta = \delta_1$. ■

Set $\beta \coloneqq \sqrt{\alpha/(2+\alpha)} = 0.4224\ldots$. Using Corollary 3.5, we can rewrite (3.3) as

$$\mu * \overline{\mu} \;=\; (1-\beta^2)\nu + \beta^2\delta_1. \tag{3.7}$$

**Lemma 3.8.** *The measure $\mu$ has precisely one atom $z \in \mathbb{T}$, and it satisfies $\mu(\{z\}) = \beta$.*

Proof. From (3.7), it follows that $\mu * \overline{\mu}$ has a unique atom, namely 1, and $(\mu * \overline{\mu})(\{1\}) = \beta^2$. If $\mu$ were atomless, then so would be $\mu * \overline{\mu}$, so $\mu$ must have at least one atom. On the other hand, if $\mu$ had two distinct atoms, say $x$ and $y$, then we would have $(\mu * \overline{\mu})(\{xy^{-1}\}) \geqslant \mu(\{x\})\mu(\{y\}) > 0$, which is impossible as $xy^{-1} \neq 1$. Therefore, $\mu$ has a unique atom $z$, and furthermore

$$\mu(\{z\})^2 \;=\; (\mu * \overline{\mu})(\{1\}) \;=\; \beta^2,$$

i.e., $\mu(\{z\}) = \beta$, as desired. ■

If necessary, we may rotate $\mu$ so that its unique atom is $1 \in \mathbb{T}$. Then $\mu$ can be decomposed as

$$\mu \;=\; (1-\beta)\eta + \beta\delta_1, \tag{3.9}$$

for some $\eta \in \mathrm{Prob}(\mathbb{T})$. Form (3.9), we obtain

$$\mu * \overline{\mu} \;=\; (1-\beta)^2(\eta * \overline{\eta}) + (1-\beta)\beta(\eta + \overline{\eta}) + \beta^2\delta_1.$$

Combined with (3.7), this yields

$$(1-\beta)(\eta * \overline{\eta}) + \beta(\eta + \overline{\eta}) = (1+\beta)\nu. \tag{3.10}$$

**Lemma 3.11.** *We have $\widehat{\eta}(0) = 1$ and $\widehat{\eta}(1) = -\beta/(1-\beta) = -0.7314\ldots$.*

Proof. We have $\widehat{\eta}(0) = 1$ since $\eta$ is a probability measure. From (3.9) and Corollary 3.5, we have

$$0 \;=\; \widehat{\mu}(1) \;=\; (1-\beta)\widehat{\eta}(1) + \beta,$$

which yields $\widehat{\eta}(1) = -\beta/(1-\beta)$, as desired. ■

For brevity, set $\gamma \coloneqq -\beta/(1-\beta)$.

**Lemma 3.12.** *We have $0 < \mathrm{Re}(\widehat{\eta}(2)) < 0.1$.*

Proof. From (3.10) and Lemma 3.4, we obtain

$$(1-\beta)|\widehat{\eta}(2)|^2 + 2\beta\mathrm{Re}(\widehat{\eta}(2)) - (1+\beta)\frac{\sin(2\vartheta)}{2\vartheta} \;=\; 0.$$

Setting $x \coloneqq \mathrm{Re}(\widehat{\eta}(2))$, we conclude that

$$(1-\beta)x^2 + 2\beta x - (1+\beta)\frac{\sin(2\vartheta)}{2\vartheta} \;\leqslant\; 0.$$

Using the numerical values for $\beta = 0.4224\ldots$ and $\vartheta = 4.4934\ldots$, we deduce that

$$-1.5384\ldots \;\leqslant\; x \;\leqslant\; 0.0755\ldots \;<\; 0.1.$$

To show that $x > 0$, consider the 3-by-3 matrix $A$ with entries $A(i,j) \coloneqq \mathrm{Re}(\widehat{\eta}(j-i))$:

$$A \;=\; \begin{bmatrix} 1 & \gamma & x \\ \gamma & 1 & \gamma \\ x & \gamma & 1 \end{bmatrix}.$$

By Lemma 2.1, the matrix $A$ must be positive semidefinite. In particular,

$$\det(A) \;=\; (x-1)(-x+2\gamma^2-1) \;\geqslant\; 0,$$

which yields $0 < 0.0700\ldots = 2\gamma^2 - 1 \leqslant x \leqslant 1$. ∎

We are now ready for the final step. Set

$$x := \mathrm{Re}(\hat{\eta}(2)) \qquad \text{and} \qquad y := \mathrm{Re}(\hat{\eta}(3)),$$

and let $M$ be the 4-by-4 matrix with entries $M(i,j) := \mathrm{Re}(\hat{\eta}(j-i))$:

$$M \;=\; \begin{bmatrix} 1 & \gamma & x & y \\ \gamma & 1 & \gamma & x \\ x & \gamma & 1 & \gamma \\ y & x & \gamma & 1 \end{bmatrix}.$$

By Lemma 2.1, the matrix $M$ must be positive semidefinite. In particular,

$$\begin{aligned}\det M \;=\; &\big((-1-\gamma)\,y + x^2 + 2\gamma x + \gamma^2 - \gamma - 1\big)\\ &\cdot\;\big((1-\gamma)\,y + x^2 - 2\gamma x + \gamma^2 + \gamma - 1\big) \;\geqslant\; 0.\end{aligned}$$

This means that $y$ is located in the interval between

$$y_1 := \frac{x^2 + 2\gamma x + \gamma^2 - \gamma - 1}{\gamma + 1} \qquad \text{and} \qquad y_2 := \frac{x^2 - 2\gamma x + \gamma^2 + \gamma - 1}{\gamma - 1}.$$

As a function of $x$, $y_1$ attains its minimum at the point $-\gamma = 0.7314\ldots$. This means that on the interval $[0; 0.1]$ it is decreasing, and hence, since $0 < x < 0.1$ by Lemma 3.12, we conclude that

$$y_1 \;\geqslant\; \frac{0.01 + 0.2\gamma + \gamma^2 - \gamma - 1}{\gamma + 1} \;=\; 0.4848\ldots \;>\; 0.4.$$

Similarly, $y_2$, viewed as a function of $x$, attains its maximum at the point $\gamma = -0.7314\ldots$. Hence, it is decreasing on the interval $[0; 0.1]$, and thus

$$y_2 \;\geqslant\; \frac{0.01 - 0.2\gamma + \gamma^2 + \gamma - 1}{\gamma - 1} \;=\; 0.6007\ldots \;>\; 0.4.$$

Therefore, we conclude that $y > 0.4$. On the other hand, from (3.10) and Lemma 3.4, we obtain

$$(1-\beta)|\hat{\eta}(3)|^2 + 2\beta \mathrm{Re}(\hat{\eta}(3)) - (1+\beta)\frac{\sin(3\vartheta)}{3\vartheta} \;=\; 0,$$

which yields

$$(1-\beta)y^2 + 2\beta y - (1+\beta)\frac{\sin(3\vartheta)}{3\vartheta} \;\leqslant\; 0.$$

Using the numerical values for $\beta = 0.4224\ldots$ and $\vartheta = 4.4934\ldots$, we obtain

$$-1.5559\ldots \;\leqslant\; y \;\leqslant\; 0.0929\ldots \;<\; 0.1.$$

This contradiction completes the proof of Theorem 1.3.

## Concluding remarks and acknowledgments

Even though our proof, as presented in Section 3, does not give an explicit lower bound on $\varepsilon$, it is clear how one could obtain such an explicit lower bound by introducing small margins of error throughout the argument. However, determining the optimal value of $\varepsilon$ in Theorem 1.3 appears technically challenging. One difficulty is that is is necessary to quantify how "close" the measure $\zeta$ is to the Dirac measure in Corollary 3.5; the outcome of this step then propagates through the rest of the proof. It seems unlikely that our methods could yield the exact value of $\mathsf{d}^*$. Golay felt that the correct value "will, undoubtedly, never be expressed in closed form" [Gol72a]. Nevertheless, we do not know the answer to the following question:

**Question 3.13.** Let $a$ denote the infimum of all real numbers $\alpha > 0$ such that there exist probability measures $\mu, \zeta \in \mathrm{Prob}(\mathbb{T})$ satisfying (3.3). We know that $\mathsf{d}^* \geqslant 2+a$. Is it true that, in fact, $\mathsf{d}^* = 2+a$?

The second author would like to thank Craig Timmons for introducing him to the problem.

## References


[EKN17] D. Ellis, G. Kalai, and B. Narayanan. *On symmetric intersecting families*, `https://arxiv.org/abs/1702.02607` (preprint), 2017

[Gol72a] M.J.E. Golay. *Notes on the representation of* 1, 2, ..., $N$ *by differences*, J. London Math. Soc., **2** (4) (1972), 729–734

[Gol72b] S.W. Golomb. "How to number a graph". *Graph theory and computing.* Elsevier, 1972, 23–37

[GS80] R.L. Graham and N.J.A. Sloane. *On additive bases and harmonious graphs*, SIAM J. Alg. Disc. Methods, **1** (4) (1980), 382–404

[Hay+92] S. Haykin, J.P. Reilly, V. Kezys, and E. Vertatschitsch. "Some aspects of array signal processing". *IEEE Proceedings F-Radar and Signal Processing.* Vol. 139. 1. IET. 1992, 1–26

[Kec95] A.S. Kechris. *Classical Descriptive Set Theory.* New York: Springer-Verlag, 1995

[Lee56] J. Leech. *On the representation of* 1, 2, ..., $n$ *by differences*, J. London Math. Soc., **31** (2) (1956), 160–169

[LST93] D.A. Linebarger, I.H. Sudborough, and I.G. Tollis. *Difference bases and sparse sensor arrays*, IEEE Transactions on information theory, **39** (2) (1993), 716–721

[Mof68] A. Moffet. *Minimum-redundancy linear arrays*, IEEE Transactions on antennas and propagation, **16** (2) (1968), 172–175

[RR49] L. Rédei and A. Rényi. О представлении чисел 1, 2, ..., $N$ посредством разностей (Russian) [On the representation of 1, 2, ..., $N$ by differences], Mat. Sb., **66** (3) (1949), 385–389

[Rud90] W. Rudin. *Fourier Analysis on Groups.* Wiley, 1990