

# A Note on the Generalized Sum-Capture Problem for Rings

Ashwin Jha

Ruhr-Universität Bochum  
Bochum, Germany

[letterstoashwin@gmail.com](mailto:letterstoashwin@gmail.com)

July 12, 2024

## Abstract

The sum-capture problem for abelian groups is generalized over any arbitrary finite ring, for an arbitrary number of sets, and in presence of an arbitrary multiplicative mask.

## 1 The problem

Let  $R$  be a finite ring and fix positive integers  $p, q < |R| = N$ . Let  $A = (A_i)_{1 \leq i \leq q}$  be a random sequence (or equivalently, an ordered multiset) over  $R$ . For any  $k \geq 2$ , any  $\alpha \in R^k$  with at least 2 non-zero coordinates, and any  $B_1, B_2, \dots, B_k \subseteq R$ , we define

$$\mu_\alpha(A, B_1, B_2, \dots, B_k) = \left| \left\{ (a, b_1, b_2, \dots, b_k) \in A \times B_1 \times B_2 \times \dots \times B_k : a = \sum_{i=1}^k \alpha_i \cdot b_i \right\} \right|.$$

For any  $p$ , one can define

$$\mu_\alpha(A; p) = \max_{\substack{B_1, \dots, B_k \subseteq R \\ |B_1| = |B_2| = \dots = |B_k| = p}} \mu(A, B_1, B_2, \dots, B_k).$$

Note that,  $\mu_\alpha(A, B_1, B_2, \dots, B_k)$  is equal to  $\frac{|A| \times |B_{i_1}| \times \dots \times |B_{i_j}|}{|R|}$  in expectation when the sets  $A, B_{i_1}, \dots, B_{i_k}$  are chosen at random, where  $\{i_1, \dots, i_j\}$  denotes the set of non-zero coordinate indices in  $\alpha$ . Let

$$\#\alpha := |\{i \in \{1, 2, \dots, k\} : \alpha_i \neq 0\}|.$$

Then, the main problem we consider is to upper bound the deviation of  $\mu_\alpha(A; p)$  from  $qp^{\#\alpha}/N$  that holds with high probability over the random choice of  $A$ . For  $k = 2$ , Babai-Hayes [Bab02, Hay03] (and later Steinberger [Ste13]) proved the following result:

**Theorem 1** ([Bab02, Ste13]). *Let  $R$  be a finite ring, and let  $0 \leq q \leq N/2$ . Fix  $\alpha = (1, 1)$ . For any without replacement sample  $A = (A_i)_{1 \leq i \leq q}$  over  $R$ , we have*

$$\Pr \left( \left| \mu_\alpha(A; p) - \frac{qp^2}{N} \right| \geq 4p\sqrt{\ln(N)q} \right) \leq \frac{2}{N}.$$

In this short note, for  $k \geq 2$ , we prove the following two results:

**Theorem 2.** Let  $R$  be a finite ring, and let  $0 \leq q \leq N/2$ . Fix some  $\alpha \in R^k$  such that  $\#\alpha \geq 2$ . For any positive real  $\epsilon$  and any with replacement sample  $A = (A_i)_{1 \leq i \leq q}$  over  $R$ , we have

$$\Pr \left( \left| \mu_\alpha(A; p) - \frac{qp^{\#\alpha}}{N} \right| \geq p^{\#\alpha-1} \sqrt{2(1+\epsilon) \ln(N)q} \right) \leq \frac{4}{N^\epsilon}.$$

**Theorem 3.** Let  $R$  be a finite ring, and let  $0 \leq q \leq N/2$ . Fix some  $\alpha \in R^k$  such that  $\#\alpha \geq 2$ . For any positive real  $\epsilon$  and any without replacement sample  $A = (A_i)_{1 \leq i \leq q}$  over  $R$ , we have

$$\Pr \left( \left| \mu_\alpha(A; p) - \frac{qp^{\#\alpha}}{N} \right| \geq 2p^{\#\alpha-1} \sqrt{2(1+\epsilon) \ln(N)q} \right) \leq \frac{2e^2}{N^\epsilon}.$$

Let  $\{i_1, i_2, \dots, i_{\#\alpha}\} \subseteq \{1, 2, \dots, k\}$  be the set of non-zero coordinate indices of  $\alpha$ . Then, one can equivalently study  $\mu_{\alpha'}(A, B'_{i_1}, B'_{i_2}, \dots, B'_{i_{\#\alpha}})$  where  $\alpha' = (1, 1, \dots, 1) \in R^{\#\alpha}$  and  $B'_{i_l} = \alpha_{i_l} \cdot B_{i_l}$ . Without loss of generality, we assume this form and drop  $\alpha'$  from the subscript.

Then, it is also clear that the (non-)commutativity of  $R$  does not play any role vis a vis the sum-capture problem. Indeed one can define  $\mu_\alpha(A; p)$  equivalently using right multiplication.

As a side-effect of the aforementioned simplification *we completely ignore the multiplicative aspect of  $R$ , and simply view it as an additive abelian group of order  $N$* . Henceforth, we assume  $\#\alpha = k$ . The case of  $2 \leq \#\alpha \leq k-1$  can be proved analogously.

## 2 A proof

A proof of both the theorems largely extends the Babai-Steinberger approach, delving into basic Fourier analysis, with a brief foray into probabilistic tail inequalities towards the end. We reproduce Steinberger's excellent introductions [Bab02, Ste13] to Fourier analysis (almost verbatim) for the uninitiated, while simultaneously working towards a proof of Theorems 2-3 — the main technical results of this note.

A *character* of  $R$  is a homomorphism  $\chi : R \rightarrow \mathbb{C}^\times$ , where  $\mathbb{C}^\times$  denotes the multiplicative group of complex numbers. Thus,

$$\chi(x)^N = \chi(Nx) = \chi(0) = 1,$$

which means that the elements in the image of  $\chi$  are the  $N^{\text{th}}$  roots of unity, and thus  $\chi(-x) = \chi(x)^{-1} = \overline{\chi(x)}$ . The *principal character*  $\chi_0$  of  $R$  is defined as the constant function that maps all  $x \in R$  to 1. Thus,  $\sum_{x \in R} \chi_0(x) = N$ , and for any non-principal character  $\chi$  and any non-zero  $y \in R$ ,

$$\chi(y) \sum_{x \in R} \chi(x) = \sum_{x \in R} \chi(x+y) = \sum_{x \in R} \chi(x),$$

whence  $\sum_{x \in R} \chi(x) = 0$ . Then, for distinct characters  $\chi$  and  $\xi$

$$\sum_{x \in R} \xi(x) \overline{\chi(x)} = 0,$$

follows from the fact that  $\xi \overline{\chi}$  is a non-principal character of  $R$ .

Let  $\hat{R}$  denote the set of characters of  $R$ . Then, it is easy to see that  $\hat{R}$  forms an abelian group under pointwise multiplication.  $\hat{R}$  is called the *dual group* of  $R$ , and  $R \cong \hat{\hat{R}}$ .

Every function  $f : R \rightarrow \mathbb{C}$  can be seen as an element of  $\mathbb{C}^{|R|}$ . This is an  $N$ -dimensional space over  $\mathbb{C}$ . For every  $f : R \rightarrow \mathbb{C}$ , define

$$E_x[f(x)] = \frac{1}{N} \sum_{x \in R} f(x),$$

which gives a natural definition of inner product over  $\mathbb{C}^{|R|}$ , namely  $\langle f, g \rangle = E[f\bar{g}]$ . Then, for any  $\chi, \xi \in \hat{R}$ , we have

$$E[\xi\bar{\chi}] = 0, \quad \xi \neq \chi$$

More precisely,

$$E[\xi\bar{\chi}] = \begin{cases} 1 & \text{if } \xi = \chi, \\ 0 & \text{if } \xi \neq \chi. \end{cases}$$

or equivalently,

$$E[\chi] = \begin{cases} 1 & \text{if } \chi = \chi_0, \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

Since  $\hat{R}$  is a set of  $N$  orthogonal functions in  $\mathbb{C}^{|R|}$ , they form a basis of  $\mathbb{C}^{|R|}$ , i.e., for every function  $f : R \rightarrow \mathbb{C}$  there exist complex numbers  $\alpha_\chi$  for every  $\chi \in \hat{R}$  such that

$$f = \sum_{\chi \in \hat{R}} \alpha_\chi \chi.$$

The coefficients  $\alpha_\chi$  are called the *fourier coefficients* of  $f$  and are typically written  $\hat{f}(\chi) := \alpha_\chi$ . In particular,  $\hat{f}(\chi_0)$  is called the *principal* fourier coefficient and all other coefficients are referred as non-principal. Thus,

$$f = \sum_{\chi \in \hat{R}} \hat{f}(\chi) \chi$$

for any  $f : R \rightarrow \mathbb{C}$ . One has

$$\hat{f}(\chi) = E[f\bar{\chi}].$$

More precisely, this can be verified from the fact that

$$E[f\bar{\chi}] = E\left[\left(\sum_{\xi \in \hat{R}} \alpha_\xi \xi\right) \bar{\chi}\right] = E[\alpha_\chi \chi \bar{\chi}] = \alpha_\chi$$

using orthogonality. For any  $f, g : R \rightarrow \mathbb{C}$ , we have

$$E[fg] = E\left[\left(\sum_{\chi \in \hat{R}} \hat{f}(\chi) \chi\right) \left(\sum_{\xi \in \hat{R}} \hat{g}(\xi) \xi\right)\right] = \sum_{\chi, \xi \in \hat{R}} \hat{f}(\chi) \hat{g}(\xi) E[\chi \xi] = \sum_{\chi \in \hat{R}} \hat{f}(\chi) \hat{g}(\bar{\chi}).$$

and similarly  $E[f\bar{g}] = \sum_{\chi \in \hat{R}} \hat{f}(\chi) \hat{g}(\chi)$ . In particular  $E[|f|^2] = \sum_{\chi \in \hat{R}} |\hat{f}(\chi)|^2$  and if  $f : R \rightarrow \{-1, 1\}$  then

$$\sum_{\chi \in \hat{R}} \hat{f}(\chi)^2 = 1$$

since  $E[f^2] = 1$ . Moreover if  $f : R \rightarrow \{0, 1\}$  then  $(-1)^f : R \rightarrow \{-1, 1\}$  and  $(-1)^f = 1 - 2f$  so

$$\begin{aligned} 1 &= \sum_{\chi \in \hat{R}} \widehat{(-1)^f}(\chi)^2 \\ &= \sum_{\chi \in \hat{R}} \widehat{1 - 2f}(\chi)^2 \\ &= \sum_{\chi \in \hat{R}} (\hat{1}(\chi) - 2\hat{f}(\chi))^2 \\ &= \sum_{\chi \in \hat{R}} \hat{1}(\chi)^2 - 4\hat{1}(\chi)\hat{f}(\chi) + 4\hat{f}(\chi)^2 \\ &= 1 - 4\hat{f}(\chi_0) + 4 \sum_{\chi \in \hat{R}} \hat{f}(\chi)^2 \end{aligned}$$

from which we deduce:

$$\hat{f}(\chi_0) = \sum_{\chi \in \hat{R}} \hat{f}(\chi)^2, \quad (\text{whenever } f : R \rightarrow \{0, 1\}). \quad (1)$$

Define convolution of  $f_1, f_2 : R \rightarrow \mathbb{C}$  as

$$(f_1 * f_2)(x) = \sum_{y \in R} f_1(y)g(x-y) = N E_y[f(y)g(x-y)].$$

Using the fact that  $\chi(x-y) = \chi(x)\overline{\chi(y)}$  for all  $\chi \in \hat{R}$ ,  $x, y$  we find

$$\begin{aligned} \widehat{f_1 * f_2}(\chi) &= E_x \left[ (f_1 * f_2)(x) \overline{\chi(x)} \right] \\ &= E_x \left[ \sum_y f_1(y) f_2(x-y) \overline{\chi(x)} \right] \\ &= \frac{1}{N} \sum_y f_1(y) \sum_x f_2(x-y) \overline{\chi(x)} \\ &= \frac{1}{N} \sum_y f_1(y) \sum_x f_2(x) \overline{\chi(x+y)} \\ &= N \left( \frac{1}{N} \sum_y f_1(y) \overline{\chi(y)} \right) \left( \frac{1}{N} \sum_x f_2(x) \overline{\chi(x)} \right) \\ &= N \hat{f}_1(\chi) \hat{f}_2(\chi). \end{aligned} \quad (2)$$

In fact, by virtue of associativity one may define a convolution  $f_{(1*k)} := f_1 * f_2 * \dots * f_k$  of any  $f_1, f_2, \dots, f_k$  and for any  $k \geq 2$ , in which case (2) has a natural generalization, namely

$$\hat{f}_{(1*k)}(\chi) = N^{k-1} \hat{f}_1(\chi) \hat{f}_2(\chi) \dots \hat{f}_k(\chi). \quad (3)$$

For any (multi)set  $Z$  with elements from  $R$ , define  $1_Z : R \rightarrow \mathbb{C}$  by the mapping

$$x \longmapsto |\{y \in Z : y = x\}|,$$

i.e.,  $1_Z(x)$  denotes the multiplicity of  $x$  in  $Z$ . Then, using (3), for any sets  $B_1, B_2, \dots, B_k \subseteq R$ , we have

$$\begin{aligned} \mu(A, B_1, B_2, \dots, B_k) &= \sum_{x \in R} 1_A(x) 1_{B_{(1*k)}}(x) \\ &= N E[1_A 1_{B_{(1*k)}}] \\ &= N \sum_{\chi \in \hat{R}} \hat{1}_A(\chi) \hat{1}_{B_{(1*k)}}(\bar{\chi}) \\ &= N^k \sum_{\chi \in \hat{R}} \hat{1}_A(\chi) \hat{1}_{B_1}(\bar{\chi}) \hat{1}_{B_2}(\bar{\chi}) \dots \hat{1}_{B_k}(\bar{\chi}) \\ &= N^k \left( \frac{|A||B_1||B_2| \dots |B_k|}{N^{k+1}} + \sum_{\chi \neq \chi_0} \hat{1}_A(\chi) \hat{1}_{B_1}(\bar{\chi}) \hat{1}_{B_2}(\bar{\chi}) \dots \hat{1}_{B_k}(\bar{\chi}) \right), \end{aligned}$$

and, by rearranging terms

$$\mu(A, B_1, B_2, \dots, B_k) - \frac{|A||B_1||B_2| \dots |B_k|}{N} = N^k \sum_{\chi \neq \chi_0} \hat{1}_A(\chi) \hat{1}_{B_1}(\bar{\chi}) \hat{1}_{B_2}(\bar{\chi}) \dots \hat{1}_{B_k}(\bar{\chi}).$$

It follows that

$$\left| \mu(A, B_1, B_2, \dots, B_k) - \frac{|A||B_1||B_2| \dots |B_k|}{N} \right| \leq N^k \sum_{\chi \neq \chi_0} |\hat{1}_A(\chi)| |\hat{1}_{B_1}(\bar{\chi})| |\hat{1}_{B_2}(\bar{\chi})| \dots |\hat{1}_{B_k}(\bar{\chi})|.$$

Define  $|\hat{1}_A| := \max_{\chi \neq \chi_0} |\hat{1}_A(\chi)|$ . Then, letting  $B_{>2} = B_3 \times \dots \times B_k$ , we have

$$\begin{aligned} \left| \mu(A, B_1, B_2, \dots, B_k) - \frac{|A||B_1||B_2| \dots |B_k|}{N} \right| &\leq N^k \cdot |\hat{1}_A| \sum_{\chi \neq \chi_0} |\hat{1}_{B_1}(\chi)| |\hat{1}_{B_2}(\chi)| \dots |\hat{1}_{B_k}(\chi)| \\ &\leq N^2 \cdot |\hat{1}_A| \cdot |B_{>2}| \cdot \sum_{\chi \in \hat{R}} |\hat{1}_{B_1}(\chi)| |\hat{1}_{B_2}(\chi)|, \end{aligned}$$

where the second inequality follows from the fact that  $|\hat{1}_X(\chi)| \leq |\hat{1}_X(\chi_0)| = |X|/N$  for any  $X \subseteq R$  and any  $\chi \neq \chi_0$ . By Cauchy-Schwarz inequality and (1), we have

$$\begin{aligned} \left| \mu(A, B_1, B_2, \dots, B_k) - \frac{|A||B_1||B_2| \dots |B_k|}{N} \right| &\leq N^2 \cdot |\hat{1}_A| \cdot |B_{>2}| \cdot \sqrt{\sum_{\chi \in \hat{R}} \hat{1}_{B_1}(\chi)^2} \sqrt{\sum_{\chi \in \hat{R}} \hat{1}_{B_2}(\chi)^2} \\ &= N^2 \cdot |\hat{1}_A| \cdot |B_{>2}| \cdot \sqrt{\hat{1}_{B_1}(\chi_0)} \sqrt{\hat{1}_{B_2}(\chi_0)} \\ &\leq N \cdot |\hat{1}_A| \cdot |B_{>2}| \cdot \sqrt{|B_1||B_2|} \end{aligned} \quad (4)$$

Then, for all sets  $B_1, B_2, \dots, B_k \subseteq R$ ,  $|B_1| = |B_2| = \dots = |B_k| = p$ , we have

$$\left| \mu(A, B_1, B_2, \dots, B_k) - \frac{|A||B_1||B_2| \dots |B_k|}{N} \right| \leq p^{k-1} \cdot N \cdot |\hat{1}_A|. \quad (5)$$

All that remains is to show that  $N \cdot |\hat{1}_A| \in O(\ln(N)q)$  with overwhelmingly high probability. At this point the proofs for Theorem 2 and 3 diverge depending upon the tail inequality in play.

## 2.1 Proof of Theorem 2

This case adheres to the well-known Chernoff bound, as also observed previously in [Bab02, Ste13, CS18]. In particular, for any  $\chi \neq \chi_0$  and an arbitrary ordering  $(A_1, \dots, A_q)$  of  $A$ , we have

$$\begin{aligned} N \cdot |\hat{1}_A(\chi)| &= \left| \sum_x 1_A(x) \chi(x) \right| \\ &= \left| \sum_x \sum_{i=1}^q 1_{\{A_i\}}(x) \chi(x) \right| \\ &= \left| \sum_{i=1}^q \chi(A_i) \right|. \end{aligned}$$

Writing  $\chi(A_i) = \phi(A_i) + \iota\psi(A_i)$  and splitting the corresponding sums, we have

$$\begin{aligned} N \cdot |\hat{1}_A(\chi)| &= \left| \sum_{i=1}^q \chi(A_i) \right| \\ &= \left| \sum_{i=1}^q \phi(A_i) + \iota \sum_{i=1}^q \psi(A_i) \right|, \end{aligned}$$

where  $\phi(A_i), \psi(A_i)$  are real-valued random variables with  $|\phi(A_i)|, |\psi(A_i)| \leq 1$  and  $E_{A_i}[\phi(A_i)] = E_{A_i}[\psi(A_i)] = 0$ . Furthermore,  $\phi(A_i)$  are all independent, and similarly  $\psi(A_i)$  are all independent. Then, for any  $a \geq 0$ , we have

$$\begin{aligned} \Pr(N \cdot |\hat{1}_A(\chi)| \geq a) &\leq \Pr\left(\left|\sum_{i=1}^q \phi(A_i)\right| \geq a\right) + \Pr\left(\left|\sum_{i=1}^q \psi(A_i)\right| \geq a\right) \\ &\leq 4e^{-a^2/2q}, \end{aligned}$$

where the second inequality is a consequence of Chernoff bound. Finally, union bound gives

$$\Pr(N \cdot |\hat{1}_A| \geq a) \leq \sum_{\chi \neq \chi_0} \Pr(N \cdot |\hat{1}_A(\chi)| \geq a) \leq 4(N-1)e^{-a^2/2q}. \quad (6)$$

By setting  $a = \sqrt{2(1+\epsilon)\ln(N)q}$  for  $\epsilon > 0$

$$\left| \mu(A, B_1, B_2, \dots, B_k) - \frac{qp^k}{N} \right| \leq p^{k-1} \sqrt{2(1+\epsilon)\ln(N)q}, \quad (7)$$

for all sets  $B_1, B_2, \dots, B_k \subseteq R$ ,  $|B_1| = \dots = |B_k| = p$  with at least  $1 - 4/N^\epsilon$  probability.

## 2.2 Proof of Theorem 3

Hayes [Hay03] proved the following result.

**Theorem 4** (Hayes, [Hay03] Lemma 6.3). *Let  $\epsilon > 0$ . Let  $R$  be a finite abelian group of order  $N$ , and let  $\chi$  be a non-principal character of  $R$ . Let  $q \leq N$  and  $q' = \min\{q, N - q\}$ . For any  $a \geq 0$ , any without replacement sample  $A = (A_i)_{1 \leq i \leq q}$  we have*

$$\Pr\left(N \cdot |\hat{1}_A(\chi)| \geq a\sqrt{q'}\right) \leq 2e^2 e^{-a^2/8}.$$

Then, the result follows by using  $q \leq N/2$  and choosing  $a = 2\sqrt{2(1+\epsilon)\ln(N)}$ .

## References

- [Bab02] László Babai. The fourier transform and equations over finite abelian groups: An introduction to the method of trigonometric sums. Online Lecture Notes (Version 1.3), 2002. <http://people.cs.uchicago.edu/laci/reu02/fourier.pdf> (last accessed: 7th March, 2024).
- [CS18] Benoît Cogliati and Yannick Seurin. Analysis of the single-permutation encrypted davies-meyer construction. *Des. Codes Cryptogr.*, 86(12):2703–2723, 2018.
- [Hay03] Thomas P. Hayes. A large-deviation inequality for vector-valued martingales. Online, 2003. <https://www.cs.unm.edu/hayes/papers/VectorAzuma/VectorAzuma20030207.pdf> (last accessed: 7th March, 2024).
- [Ste13] John P. Steinberger. Counting solutions to additive equations in random sets. *CoRR*, abs/1309.5582, 2013. <http://arxiv.org/abs/1309.5582> (last accessed: 7th March, 2024).