A Note on the Generalized Sum-Capture Problem for Finite Fields

Ashwin Jha

Ruhr-Universität Bochum

letterstoashwin@gmail.com

July 12, 2024

Abstract

The sum-capture problem for abelian groups is generalized to study the sum-capture over any arbitrary number of sets and in presence of a multiplicative mask.

1 The problem

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

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

Suppose, $\{i_1,i_2,\dots,i_j\}\subseteq\{1,2,\dots,k\}$ be the set of non-zero coordinate indices of α, and $H(\alpha)$ denote the size of this set. Then, one can equivalently study $\mu_{\alpha'}(A,B'_{i_1},B'_{i_2},\dots,B'_{i_j})$ where $\alpha'=(1,1,\dots,1)$ and $B'_{i_l}=\alpha_{i_l}\cdot B_{i_l}$. Henceforth, without loss of generality, we assume this form and drop α' from the subscript. As a side-effect of this simplification we can also ignore the multiplicative aspect of F, and simply view it as an abelian group of order N.

For any p, one can define

$$\mu_k(A;p)=\max_{\substack{B_1,\dots,B_k\subseteq F\\ |B_1|=|B_2|=\cdots=|B_k|=p}}\mu(A,B_1,B_2,\dots,B_k).$$

Note that, $\mu(A,B_1,B_2,\dots,B_k)$ is equal to $\dfrac{|A|\times|B_1|\times|B_2|\times\cdots\times|B_k|}{|F|}$ in expectation when the sets $A,B_1,B_2,\dots,B_k$ are chosen at random. Then, the main problem we consider is to upper bound the deviation of $\mu_\alpha(A;p)$ from qp^k/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 F be a finite field, and let $0\le q\le N/2$. For any without replacement sample $A=(A_i)_{1\le i\le q}$ over F, we have*

$$\Pr\left(\left|\mu_2(A;p)-\frac{qp^2}{N}\right|\ge 4p\sqrt{\ln(N)q}\right)\le\frac{2}{2^n}.$$

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

Theorem 2. *Let F be a finite field, and let $0 \leq q \leq N/2$. For any with replacement sample $A = (A_i)_{1\leq i\leq q}$ over F, we have*

$$\Pr\left(\left|\mu_k(A;p) - \frac{qp^k}{N}\right| \geq 2p^{k-1}\sqrt{\ln(N)q}\right) \leq \frac{2}{N}.$$

Theorem 3. *Let F be a finite field, and let $0 \leq q \leq N/2$. For any without replacement sample $A = (A_i)_{1\leq i\leq q}$ over F, we have*

$$\Pr\left(\left|\mu_k(A;p) - \frac{qp^k}{N}\right| \geq 4p^{k-1}\sqrt{\ln(N)q}\right) \leq \frac{2e^2}{N}.$$

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 F is a homomorphism $\chi : F \to \mathbb{C}^\times$, 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 χ are the N^{th} roots of unity, and thus $\chi(-x) = \chi(x)^{-1} = \overline{\chi(x)}$. The *principal character* χ_0 of F is defined as the constant function that maps all $x \in F$ to 1. Thus, $\sum_{x\in F}\chi_0(x) = N$, and for any non-principal character χ and $y \neq 1 \in F$,

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

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

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

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

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

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

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

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

$$E[\xi\overline{\chi}] = 0, \qquad \xi \neq \chi$$

More precisely,

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

or equivalently,

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

Since $\hat{F}$ is a set of $|F|$ orthogonal functions in $\mathbb{C}^{|F|}$, they form a basis of $\mathbb{C}^{|F|}$. I.e., for every function $f: F \to \mathbb{C}$ there exist complex numbers α_χ for every $\chi \in \hat{F}$ such that

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

The coefficients α_χ 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,

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

for any $f: F \to \mathbb{C}$. One has

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

More precisely, this can be verified from the fact that

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

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

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

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

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

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

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

from which we deduce:

$$\hat{f}(\chi_0) = \sum_{\chi \in \hat{F}} \hat{f}(\chi)^2, \qquad (\textbf{whenever } f: F \to \{0, 1\}). \tag{1}$$

Define convolution of $f_1, f_2: F \to \mathbb{C}$ as

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

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

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

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

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

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

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

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

$$\begin{aligned}
\mu(A,B_1,B_2,\ldots,B_k) &= \sum_{x\in F}1_A(x)1_{B_{(1*k)}}(x) \\
&= NE[1_A1_{B_{(1*k)}}] \\
&= N\sum_{\chi\in\hat{F}}\hat{1}_A(\chi)\hat{1}_{B_{(1*k)}}(\overline{\chi}) \\
&= N^k\sum_{\chi\in\hat{F}}\hat{1}_A(\chi)\hat{1}_{B_1}(\overline{\chi})\hat{1}_{B_2}(\overline{\chi})\ldots\hat{1}_{B_k}(\overline{\chi}) \\
&= N^k\left(\frac{|A||B_1||B_2|\ldots|B_k|}{N^{k+1}}+\sum_{\chi\neq\chi_0}\hat{1}_A(\chi)\hat{1}_{B_1}(\overline{\chi})\hat{1}_{B_2}(\overline{\chi})\ldots\hat{1}_{B_k}(\overline{\chi})\right),
\end{aligned}$$

and, by rearranging terms

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

It follows that

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

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

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

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

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

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

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

All that remains is to show that $N \cdot |\hat{1}_A| \in O(\ln(N)q)$. 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's bound, as also observed previously in [Bab02, Ste13, CS18]. Following [CS18] and using Chernoff's bound, we have

$$\Pr(N|\hat{1}_A| \geq \sqrt{4\ln(N)q}) \leq 2(N-1)e^{-2\ln(N)} \leq 2/N, \qquad (6)$$

which immediately gives

$$\mu(A,B_1,B_2,\dots,B_k) \leq \frac{qp^k}{N} + p^{k-1}\sqrt{4\ln(N)q}, \qquad (7)$$

for all sets $B_1, B_2, \dots, B_k \subseteq F$, $|B_1| = \dots = |B_k| = p$ with at least $1-2/N$ probability. This completes the proof.

2.2 Proof of Theorem 3

Hayes [Hay03] proved the following upper bound on the magnitude of the non-principal Fourier coefficients of 1_A:

Theorem 4 (Hayes, [Hay03] Theorem 1.13). *Let $\varepsilon > 0$. Let G be a finite abelian group, and let $0 \leq q \leq N$. For all but an $O(N^{-\varepsilon})$ fraction of subsets $A \subseteq G$ such that $|A| = q$, we have $N \cdot |\hat{1}_A| \leq 2\sqrt{2(1+\varepsilon)\ln(N)q'}$, where $q' = \min(q, N-q)$.*

Assuming such an A, using Hayes's Theorem with $\varepsilon = 1$ and $q \leq N/2$ in (5), we have

$$\left|\mu(A,B_1,B_2,\dots,B_k) - \frac{qp^k}{N}\right| \leq 4p^{k-1}\sqrt{\ln(N)q}, \qquad (8)$$

for all sets $B_1, B_2, \dots, B_k \subseteq G$, $|B_1| = \dots = |B_k| = p$ with at least $1 - 2e^2/N$ probability. This completes the proof.

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).