Discrete Fourier Analysis I

Gautami Bhowmik

Discrete Fourier Analysis I

Gautami Bhowmik

Definition 1. Consider the circle group $S^1 = \{z \in \mathbb{C}, |z| = 1\}$ and let $(G, +)$ be an abelian group . A *character* χ on G is a group homomorphism i.e. $\chi : (G, +) \to (S^1, \times)$ where χ satisfies the property $\chi(t - u) = \chi(t)\chi(u)^{-1} \forall\ t, u \in G$

Example 1. Let G be the additive group of integers, generated by 1. Let $\chi(n) = \chi(1)^n$ for every integer n.Then there exists a real number α such that $\chi(1) = e^{2\pi i\alpha}$. The function $x \in \mathbb{R} \mapsto e^{2\pi ix} \in S^1$ is 1-periodic and is determined up to an integer. So there is a bijection between the characters on $\mathbb{Z}$ and the quotient group $\mathbb{R}/\mathbb{Z}$, often denoted by $\mathbb{T}$ the 1-dimensional torus.

Example 2. Let $G = (\mathbb{Z}/N\mathbb{Z}, +)$ for a positive integer N. The characters of $\mathbb{Z}/N\mathbb{Z}$ are exactly the characters of $\mathbb{Z}$ satisfying the condition $\chi(MN) = 1 \forall M \in \mathbb{Z}$. Thus $\chi(N) = 1$ which implies that $e^{2\pi i\alpha N} = 1$ for some real α. Thus there exists an integer ℓ such that $\alpha = \ell/N$ and the characters of $\mathbb{Z}/N\mathbb{Z}$ are in bijection with the N-th roots of unity.

Notation 1. For every $j \in \mathbb{Z}_N$, the character is denoted by $e_j(k) := \omega^{jk}$ where ω is a primitive N-th root of unity,

Definition 2. The *Pontryagin Dual* of a group G is the topological group $\hat{G}$ given by the set of characters on G which obey the product law $(\chi, \chi') \mapsto \chi.\chi'$.

Example 3.

1. Finite abelian groups are self-dual.
2. The dual group of $\mathbb{Z}$ is S^1.

Exercise 1.

1. Prove the above .
2. Show that an isomorphism between G and $\hat{G}$ is not canonical.
3. Prove directly that $\widehat{\hat{G}} \cong G$.

4. Show that $\widehat{G \times H} \cong \hat{G} \times \hat{H}$.

Let N be a positive integer . Consider V, the $\mathbb{C}$ vector space of functions $f : \mathbb{Z}_N \to \mathbb{C}$.

Definition 3. The hermitian scalar product of $f, g \in V$ is defined by

$$\langle f, g \rangle_V := \frac{1}{N} \sum_{n \in \mathbb{Z}_N} f(n)\overline{g(n)}$$

where $\bar{z}$ is the complex conjugate of z.

We may simply write $\langle f, g \rangle$ where V is understood from the context. Clearly, $\langle f, f \rangle \geq 0$ and $\overline{\langle f, g \rangle} = \langle g, f \rangle$.

Remark 1. In the la language of probability used in ergodic theory, where for a finite set A with cardinality $|A|$ and a complex-valued function $f : A \to \mathbb{C}$, the *mean* or *expectation* $\mathbb{E}(f)$ of f is defined as

$$\mathbb{E}_A(f) = \mathbb{E}_{n \in A} f(n) := \frac{1}{|A|} \sum_{n \in A} f(n),$$

the scalar product is nothing but $\mathbb{E}_{Z_N}(f\bar{g})$.

Remark 2. The $\{e_j\}$ form an orthonormal basis of V, since

$$\langle e_j, e_k \rangle = \frac{1}{N} \sum_{n \in \mathbb{Z}_N} e_k(n)\overline{e_j(n)} = \sum_{n \in \mathbb{Z}_N} \omega^{(j-k)n} = \begin{cases} 1 & \text{if } j = k \\ \frac{\omega^{(j-k)N}-1}{\omega^{j-k}-1} = 0 & \text{otherwise.} \end{cases}$$

Since

$$\langle e_j, e_k \rangle = \delta_{jk} \tag{1}$$

and V has dimension N, the $\{e_j\}_{j \in \mathbb{Z}_N}$ form a complete orthonormal base of V .

We can now define the Fourier transform.

Definition 4. The discrete Fourier transform $\hat{f}$ of $f \in V$ is defined by

$$\hat{f}(k) := \langle f, e_k \rangle = \frac{1}{N} \sum_{s=0}^{N-1} f(s)\omega^{-ks},$$

where $\omega = e^{2\pi i/N}$.

In particular, $\hat{e}_j(k) = \delta_{kj}$ and $\hat{1}(k) = \delta_k$.

Remark 3. The above definition could be seen as the discrete version of

$$\hat{f}(k) = \int f(x)e^{-2\pi ikx}dx$$

though this is not at all the only motivation for this study. There are many many applications in and out of mathematics some of which we will see in this and other courses (many interesting examples of applications can be found in [8]).

We will use the following identities :

Lemma 1. *For $f \in V$ we have :*

$$\text{(Inversion)} \qquad f = \sum_{k\in\mathbb{Z}_N} \hat{f}(k)e_k \tag{2}$$

$$\text{(Plancherel)} \qquad \langle \hat{f}, \hat{g}\rangle = \frac{1}{N}\langle f, g\rangle \tag{3}$$

$$\text{(Parseval)} \qquad (\sum_{k\in\mathbb{Z}_N} |\hat{f}(k)|^2)^{1/2} = (\frac{1}{N}\sum_{x\in\mathbb{Z}_N} |f(x)|^2)^{1/2}. \tag{4}$$

Proof. The Fourier transform can be written as

$$\sum_{k\in\mathbb{Z}_N} \hat{f}(k)e_k(x) = \sum_k e_k(x)\frac{1}{N}\sum_y f(y)e_k(-y) = \frac{1}{N}\sum_k\sum_y f(y)\omega^{(x-y)k}.$$

But $\sum_{k\in\mathbb{Z}_N} \omega^{zk} = N\delta_z$, which yield (2).
Similarly,

$$\langle \hat{f}, \hat{g}\rangle = \frac{1}{N}\sum_{k\in\mathbb{Z}_N} \hat{f}(k)\overline{\hat{g}(k)} = \frac{1}{N}(\sum_{x\in\mathbb{Z}_N} f(x)e_k(-x))(\sum_{y\in\mathbb{Z}_N} \hat{g}(y)e_k(-y))$$

$$= \frac{1}{N^3}\sum_x\sum_y f(x)\overline{g(y)}\sum_k e_k(y-x) = \frac{1}{N^2}\sum_x f(x)\overline{g(x)} = \frac{1}{N}\langle f, g\rangle.$$

Finally, Parseval's identity is a proved as

$$\sum_{k\in\mathbb{Z}_N} |\hat{f}(k)|^2 = \sum_{k\in\mathbb{Z}_N} \hat{f}(k)\overline{\hat{f}(k)} = N\langle \hat{f}, \hat{f}\rangle = \langle f, f\rangle = \frac{1}{N}\sum_x |f(x)|^2.$$

□

Remark 4. The Fourier transform is a linear isomorphism from V to V by considering the linear map $T : V \to V$ defined by $T(f) = \hat{f}$ and two functions are equal if and only if their Fourier transforms are equal.

With respect to the basis e_k, the matrix of T is of the form

$$[T] = \frac{1}{N}(\omega^{-ij})_{1\leq i,j\leq N}. \tag{5}$$

Since $\hat{e}_k(x) = \frac{1}{N}\sum_s e_s(k-x)$, $\hat{e}_k = \frac{1}{N}\sum_s e_s(k)e_s = \frac{1}{N}\sum_s \omega^{-ks}e_s$.

Now that we have a Vandermonde matrix, the determinant of T is non-zero and we can consider the inverse application . By (2), $T^{-1}(f) = \sum f(k)e_k$ and thus $T^{-1}(e_k) = \sum \omega^{-ks}e_s$. This leads to $[T^{-1}] = N[T]^\star$, which gives $\|\det T\| = N^{-N/2}$. Note that $\sqrt{N}T$ is an unitary matrix.

We now introduce the idea of a convolution in V.

Definition 5. let $f, g \in V$. Their convolution $f * g$ is defined as follows

$$f * g(x) := \frac{1}{N}\sum_{n\in\mathbb{Z}_N} f(n)g(x-n).$$

The following identity is rather useful.

$$\widehat{(f*g)} = \hat{f}.\hat{g} \tag{6}$$

Proof. From definitions,

$$\widehat{(f*g)}(k) = \frac{1}{N}\sum_s f*g(s)\omega^{-ks} = \frac{1}{N^2}\sum_x\sum_y f(y)g(x-y)\omega^{-yk}\omega^{-(x-y)k}.$$

By taking $z = x - y$, the above becomes

$$= \frac{1}{N}\sum_y f(y)\omega^{-yk}.\frac{1}{N}\sum_z g(z)\omega^{-zk} = \hat{f}(k)\hat{g}(k).$$

□

We will also come across norms in the context of finite groupes G.

Definition 6. The $L^p(G)$ norm of a function $f : G \to \mathbb{C}$ for $0 < p < \infty$ is defined as

$$||f||_{L^p(G)} := (\mathbb{E}_{x\in G}|f(x)|^p)^{1/p}$$

and the L^∞ as

$$\|f\|_{L^\infty(G)} := \sup_{x\in G}|f(x)|.$$

Similarly the $l^p(G)$ norm for $0 < p < \infty$ is defined to be

$$||f\|_{l^p(G)} := (\sum |f(x)|^p)^{1/p}.$$

while

$$\|f||_{l^\infty(G)} := ||f||_{L^\infty(G)}.$$

Remark 5. For any finite abelian group G and a function $f : G \to \mathbb{C}$ the Fourier transform $\hat{f} : \hat{G} \to \mathbb{C}$ can be seen as

$$\hat{f}(\chi) = \langle f, \chi \rangle_G = \frac{1}{|G|} \sum_{g \in G} f(g)\overline{\chi(g)}.$$

Remark 6. Norms can serve as a useful language. Thus, for example, we see that the L^2 norm of f is simply the magnitude of hilbert space, i.e. $\langle f, f \rangle^{1/2}$. while Parseval's identity can be written as

$$\| f \|_{L^2} = \| \hat{f} \|_{l^2} .$$

Exercise 2. Prove a Parseval identity for any finite abelian group.

1 Arithmetic Progressions

We encounter the use of finite Fourier analysis in the context of arithmetic progressions.

Definition 7. An *arithmetic progression of length* k in an additive group G is a finite sub-set A of cardinality k ($1 \leq k <$ order of G) of the form

$$A = \{a_0, a_0 + d, \ldots, a_0 + (k-1)d\} = a_0 + \{0, d, \ldots, (k-1)d\}$$

with $a_0, d \in G$. To make sure that the progression is *non-trivial* we assume that d is non-zero.

We also need to know the density of a set.

Definition 8. For a set A of positive integers, its *upper density* δ is defined by

$$\delta := \limsup_{N \to \infty} \frac{|A \cap [1, N]|}{N}.$$

One of the most impressive results in this direction is the following.

Theorem 2. *(Szemerédi) Every subset of integers with positive upper density contains arbitrarily long arithmetic progressions .*

This result was proved by Roth [2] by Fourier analytic methods for arithmetic progressions of length three and by Szemerédi (1975) for arbitrary lengths. Other than its original combinatorial proof there are many other surprising ways of treating Szemerédi's theorem for example by higher order fourier analytic methods (Gowers 2001 [3], [4]), by ergodic theory (Furstenberg 1977) or by hypergraphs Nagle-Rödl-Schacht-Skokan (2006).

Notation 2. Let $n_k(N)$ be the smallest integer t such that every sub-set of t elements of the interval $[1, N]$ contains an arithmetic progression of length k.

Roth (1953) proved that $n_3(N) = o(N)$ for every N. More precisely, the quantitative version of the theorem is :

Theorem 3. *(Roth) Let $\delta \in \mathbb{R}^+$. Then there exists an absolute constant $C > 0$ such that if $N \geq exp\ exp\ (C/\delta)$, every sub-set A of $[1, N] \cap \mathbb{N}$ with δN elements contains at least one non-trivial arithmetic progression of length three.*

Roth's theorem and some of its improvements will be proved in the third course on discrete fourier analysis.

Remark 7. Notice that the set of prime numbers have upper density zero and do not fall under the cases just mentioned. Using Fourier analytic methods, van der Corput proved in 1939 that the set of primes contain infinitely many arithmetic progressions of length 3 while the existence of progressions of arbitrary length in primes is the famous Green-Tao theorem of 2004, a particular case (as is Szemerédi's theorem) of the Erdős-Turán conjecture of 1936 that every set of positive integers A verifying $\sum_{a \in A} \frac{1}{a} = \infty$ contains arbitrarily long arithmetic progressions.

2 Uncertainty

As another application we shall consider the uncertainty principle for a finite group.

Definition 9. The support of a function f is defined as supp $(f) := \{x \ : f(x) \neq 0\}$.

We have supp $(f \star g) \subset$ supp $f +$ supp g. In particular, if f and g are the indicator fonctions of the sets A and B, we have the equality supp $(1_A \star 1_B) = A + B$.

Theorem 4. *(Uncertainty Principle) Let G be a finite group and let f be a non-zero function of $G \to \mathbb{C}$. Then we have*

$$|supp\ (f)|.|supp\ (\hat{f})| \geq |G|. \tag{7}$$

Proof. Consider the $l^\infty(G)$ norm of the Fourier transform of f. We can trivially bound this by the $l^1(G)$ norm of f. Thus,

$$||\hat{f}||_{l^\infty(G)} = \sup_{\chi\in\hat{G}} |\hat{f}(\chi)| = \sup |\frac{1}{|G|}\sum_{x\in G} f(x)\overline{\chi(x)}| \leq \frac{1}{|G|}\sum_{x\in G}|f(x)|$$

$$= \frac{|\text{supp }(f)|}{|G|}\frac{1}{|\text{supp }(f)|}\sum_{x\in G}|f(x)|.$$

By applying the inequality of Cauchy-Schwartz on $\sum |f(x)|$ we get

$$||\hat{f}||_{l^\infty(G)} \leq \frac{|\text{supp }(f)|}{|G|}(\frac{1}{|\text{supp }(f)|}\sum_{x\in G}|f(x)|^2)^{1/2} = \frac{|\text{supp }(f)|^{1/2}}{|G|^{1/2}}(\frac{1}{|G|}\sum|f(x)|^2)^{1/2},$$

which is, by Parseval 's identity(4),

$$= \frac{|\text{supp }(f)|^{1/2}}{|G|^{1/2}}\sum|\hat{f}(k)|^2)^{1/2}.$$

So we get

$$||\hat{f}||_{l^\infty(G)} \leq \frac{|\text{supp }(f)|^{1/2}}{|G|^{1/2}}|\text{supp }(\hat{f})|^{1/2}\sup_{k\in G}|\hat{f}(k)|$$

and we have obtained (7).

□

Now we shall prove an improvement of this result for the case of $G = \mathbb{Z}_p$ to get a bound for the sum of supports of f and its Fourier transform.

Theorem 5. *Let p be a prime number and let $f : \mathbb{Z}_p \to \mathbb{C}$ be a non-zero function . Then*

$$|supp\ (f)| + |supp\ (\hat{f})| \geq p + 1. \tag{8}$$

Conversely if A and B are two non-empty sub-sets of $\mathbb{Z}_p$ such that $|A|+|B| \geq p+1$, then there exists a function f such that supp $(f) = A$ et supp $(\hat{f}) = B$.

The proof of such a result requires the existence of an inversible linear application on a sub-set of $\mathbb{Z}_p$. So the Vandermonde matrix of (5) is no longer sufficient . We shall instead use a résult of Chebotarëv which was first proved in 1926, but was subsequently re-proved several times. Here we give an elementary proof due to Frenkel.

Lemma 6. *(Chebotarëv) Let p be a prime number and let $A, A' \subseteq \mathbb{Z}_p$ with $|A| = |A'|$. Let ω be a p-th root of unity. Then the matrix $(\omega^{ji})_{j\in A, i\in A'}$ has non-zero determinant .*

We use two auxilliary lemmas.

Lemma 7. *Let ω be a p-th root of unity for a prime number p. Then*

$$\frac{\mathbb{Z}[\omega]}{(1-\omega)} = \mathbb{F}_p. \tag{9}$$

Proof. We shall find a surjective homomorphism of $\mathbb{Z}[\omega]$ to $\mathbb{F}_p$ whose kernel will be the ideal $(1-\omega)$. This homomorphism will be built out of two others. Let Ω be an indeterminate and let $\Phi_p(\Omega) = 1 + \Omega + \cdots + \Omega^{p-1}$ be the minimal polynomial of an algebraic integer ω. Consider the two following ring homomorphisms

$$\psi_1 : \quad \mathbb{Z}[\Omega] \to \mathbb{Z}[\omega] = \frac{\mathbb{Z}[\Omega]}{(\Phi_p(\Omega))}, \qquad \Omega \mapsto \omega, \tag{10}$$

and

$$\psi_2 : \quad \mathbb{Z}[\Omega] \to \mathbb{F}_p = \frac{\mathbb{Z}[\Omega]}{(1-\Omega, p)}, \qquad \Omega \mapsto 1. \tag{11}$$

They are both surjective and since $\Phi_p(\Omega) \equiv \bmod (1-\Omega)$, we have $\ker\psi_1 \subset \ker\psi_2$. Thus there exists a surjective homomorphism ψ_3 de $\mathbb{Z}_\omega$ to $\mathbb{F}_p$ such that $\psi_2 = \psi_1.\psi_3$ with

$$\ker\psi_3 = \frac{(1-\Omega, p)}{(\Phi_p(\Omega))}.$$

But since $p \equiv \Phi_p(\omega) = 0 \bmod (1-\omega)$ we obtain $\ker\psi_3 = (1-\omega)$.

□

Exercise 3. Find another proof of the above lemma.

Let g be a non-zero polynomial with coefficients in a field $\mathbb{F}$. Let us use the notations $m_a(g)$ for the number of times that $a \in \mathbb{F}^*$ is a root of g and $c(g)$ for the number of non-zero coefficients of g.

Lemma 8. *Consider a non-zero polynomial $g \in \mathbb{F}_p[x]$ with degree less than p. Then $m_a(g) < c(g)$ for every $a \in \mathbb{F}_p^*$.*

Proof. We suppose the result to be already true for degrees less than $k \geq 1$, the case of $k = 0$ being obvious. Now let $\deg g(x) = k$.

If $g(0) = 0$, consider $h(x) = g(x)/x$ of degree $k-1$. Then $m_a(g) = m_a(h)$ and $c(g) = c(h)$ By the induction hypothesis $m_a(h) < c(h)$.

If $g(0) \neq 0$, consider the derived polynomial $g'(x)$. Thus we have $m_a(g) - m_a(g') \leq 1$ and $c(g) = c(g') + 1$. Since $g'(x) \neq 0$, and is of degree less than k, the induction hypothesis on g' gives $m_a(g') + 1 < c(g') + 1$, the desired l'inequality .

□

Proof. (of lemma 6) Let $\sum_{j\in A} a_j\omega^{ji} = 0$ for every $i \in A'$. i.e.

$$g(x) = \sum_{j\in A} a_j x^j \in \mathbb{Z}[\omega][x] = 0 \ \forall\ \omega^i, i \in A'. \tag{12}$$

We shall prove that $a_j = 0$ for every $j \in A$. From (12) we get that $g(x)$ is divisible by $\prod_{i\in A'}(x-\omega^i)$. By using the homomorphism $\psi : \mathbb{Z}[\omega] \to \frac{\mathbb{Z}[\omega]}{(1-\omega)}$ and (9) for coefficients of $g(x)$, we obtain a polynomial $\bar{g}(x) \in \mathbb{F}_p(x)$ which is divisible by $(x-1)^{|A'|}$, i.e. $m_1(\bar{g}) \geq |A'|$. However $c(\bar{g}) \leq |A| = |A'|$, which, by Lemma (8) gives $\bar{g} \equiv 0$. So every a_j is divisible by $1-\omega$ and we can continue dividing indefinitely unless every $a_j = 0$.

□

Now we prove the improvement on cyclic groups of prime order.

Proof. (of Theorem 5)

Suppose, if possible, that there exists a non-zero fonction f such that $|\text{supp }(f)| + |\text{supp }(\hat{f})| \leq p$.

Let $A = \text{supp } f$ and let $|A| = p - t$, where t is a non-negative integer. By our assumption, $|\text{supp }(\hat{f})| \leq t$. Therefore there exist at least $p - t$ elements in $\mathbb{Z}_p$ which are not in supp $\hat{f}$. We can choose a set A' of the same cardinality as A among these elements such that $A' \cap \text{supp } \hat{f} = \emptyset$. Thus for every $k \in A'$, we get $\hat{f}(k) = 0$. We can consider f as a non-zero function such that $f(x) = 0, x \notin A$. Hence the linear application $T_A f = \hat{f}|_{A'} = 0$.

However by Chebotarëv,'s Lemma, $T_A = \frac{1}{|A|}(\omega^{-ji})_{j\in A, i\in A'}$ has non-zero determinant and hence T_A is inversible, which is a contradiction.

Conversely suppose that there exist two sub-sets A, B of $\mathbb{Z}_p$. It suffices to prove the result for the case $|A| + |B| = p + 1$ since the case $|A| + |B| > p + 1$ would then follow by considering sub-sets A_1, B_1 of A, B such that $|A_1| + |B_1| = p + 1$.

We can choose A' with the same cardinality as A in $\mathbb{Z}_p$. As before, by the use of Lemma (6), the linear application T_A such that $T_A f = \hat{f}|_{A'}$ for a function f with supp $f \subseteq A$, is invertible. In particuliar, we may choose A' in such a way that $A' \cap B = \{k'\}$ and f which would satisfy the conditions $\hat{f}(k) = 0$ if $k \in A'\backslash\{k'\}$ and $\hat{f}(k') \neq 0$. Since $\mathbb{Z}_p$ is a disjoint union of $A'\backslash\{k'\}$ and B, we obtain that

$$\text{supp } \hat{f} \subseteq B.$$

But we have already proved that $|\text{supp }(f)| + |\text{supp }(\hat{f})| \geq p+1$, which leads us to

$$p + 1 \leq |\text{supp }(f)| + |\text{supp }(\hat{f})| = |A| - |A\backslash\text{supp } f| + |B - |B\backslash\{\text{supp } \hat{f}\}|.$$

And since $|A| + |B| = p + 1$, we obtain $|A \backslash \text{supp } f| = |B \backslash \text{supp } \hat{f}| = 0$. Thus supp $f = A$ et supp $\hat{f} = B$, as desired. □

Exercise 4. Prove that the case $|A| + |B| = p + 1$ proved above is indeed sufficient for Theorem 5.

And now we shall apply the Principle of Uncertainty just obtained on $\mathbb{Z}_p$ to give a new proof of a classical result in the context of *sumsets*.

Definition 10. Let $(G, +)$ be an additive group. let A et B be two non-empty subsets of G. The *sum* de A, B is the sub-set

$$A + B := \{a + b \mid a \in A,\, b \in B\}.$$

The question of finding bounds on sumsets is an active area of research and some of this will be treaed in the second course on DFA.

Below we see one of the oldest theorems in the subject known as the Cauchy (1813)- Davenport (1935) Theorem reproved recently using uncertainty [7].

Corollary 9. *Let p be a prime number and let A and B be two non-empty subsets of $\mathbb{Z}_p$. Then we have*

$$|A + B| \geq \min(|A| + |B| - 1, p).$$

Proof. (Chapman, Tao) Let us first fix A et B. Since they are non-empty, we can find two non-empty sub-sets X and Y of $\mathbb{Z}_p$ such that $|X| = p + 1 - |A|$, $|Y| = p + 1 - |B|$. Now let $|X \cap Y| = \max(|X| + |Y| - p, 1)$. Since $|A| + |X| = p + 1$, we use Theorem (5) to get a function f such that supp $(f) = A$ and supp $(\hat{f}) = X$. By the same theorem there exists a function g such that supp $(g) = B$ and supp $(\hat{g}) = Y$.

Consider the convolution $f \star g$. We then have,

$$\text{supp } (f \star g) \subset \text{supp } (f) + \text{supp } (g) = A + B$$

and

$$\text{supp } \widehat{(f \star g)} = \text{supp } (\hat{f}.\hat{g}) = \text{supp } (\hat{f}) \cap \text{supp } (\hat{g}) = X \cap Y.$$

By using (8) for $f \star g$, a non-zero function , we obtain

$$|A + B| + |X \cap Y| \geq p + 1. \tag{13}$$

Case 1. $|X| + |Y| - p > 1$. Here we get $|X \cap Y| = |X| + |Y| - p$, so that $|A + B| + |X \cap Y| \geq p + 1$ which gives $|A + B| \geq p + 1 - |X \cap Y| = p + 1 - |X| - |Y| + p = |A| + |B| - 1 = \min(|A| + |B| - 1, p)$.

Case 2. $|X| + |Y| - p = 1$. Here we have $|A| + |B| - 1 = p$ and $|X \cap Y| = 1$, which gives $|A + B| \geq p = \min(|A| + |B| - 1, p)$. □

Exercise 5. Find another proof of the Cauchy-Davenport Theorem.

References

[1] N. Alon, M. Dubiner, A lattice point problem and additive number theory, *Combinatorica* **15** (1995), 301–309.

[2] Roth, K. F. On certain sets of integers. *J. London Math. Soc.* **28** (1953), 104–109.

[3] T. Gowers, A new proof of Szemerédis theorem for arithmetic progressions of length four, *GAFA* **8** (1998), 529-551.

[4] T. Gowers, A new proof of Szemerédis theorem, *GAFA* **11** (2001), 465–588.

[5] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.***27** (1975), 299-345.

[6] T. Tao, V. Vu, Additive combinatorics, Cambridge Studies in Advanced Mathematics, 105. Cambridge University Press, Cambridge, 2010.

[7] T.Tao, An uncertainty principle for cyclic groups of prime order. *Math. Res. Lett.* **12** (2005), no. 1, 121-127.

[8] A. Terras, Fourier analysis on finite groups and applications. London Mathematical Society Student Texts, 43. Cambridge University Press, Cambridge, 1999.