Deconstructing Arsovski's Proof of Snevily's Conjecture

Deepanshu Kush
Integrated MSc Student,
Department of Mathematics,
Indian Institute of Technology,
Bombay, Powai, Mumbai
Maharashtra 400 076, India.
Email:deepkush@iitb.ac.in

The combinatorial problem discussed in this article is very simple to state but needs the algebraic machinery of characters of abelian groups.

1. Introduction

In a 1999 article [1] of the *American Mathematical Monthly*, Hunter Snevily posed the following:

Conjecture. *For any positive integer k and any two k-element subsets $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_k\}$ of a finite abelian group of odd order, there exists a permutation $\pi \in S_k$ such that all sums $a_i + b_{\pi(i)}$, where $i \in [k]$, are pairwise distinct.*

Shortly after the conjecture was formulated, Noga Alon [2] found a proof in the case where the group is cyclic of prime order. The proof is algebraic in nature and is a fairly straightforward application of the *Combinatorial Nullstellensatz*. Almost immediately after Alon published the proof, Dasgupta, Karolyi, Serra and Szegedy [3] modified it to prove the conjecture for all cyclic groups of odd order.

Our focus in this discussion is to try to analyze Bodan Arsovski's complete resolution of this conjecture [4], which was published in 2011. We shall attempt to motivate every step along the way.

2. What Do We Know?

Let us turn back the clock to 2002; Snevily's conjecture has just been proved for all cyclic groups of odd order by Dasgupta *et al*. and our aim now is to resolve the general case. An immediate observation after reading the two successive resolutions is that in both proofs, the cyclic group in question is embedded in an appropriate field, specifically in the multiplicative group of

Keywords
Snevily's conjecture, abelian groups, cyclic groups, homomorphism, Cayley table, permutation-constraints, linear characters into finite fields.

Cyclic groups can be realized in the multiplicative groups of finite fields which in fact is useful in tackling Snevily's conjecture in these cases.

an appropriate finite field, and then algebraic results are used to prove the claim. This technique however, clearly cannot be used for general abelian groups as they cannot, in general, be realised as subgroups of cyclic groups.

What can we do then? In order to apply the algebraic machinery available to us, we need to both preserve the group structure and work over a field. That's where group characters come in. Indeed, a character is a group homomorphism from a group G to the non-zero elements (*i.e.*, the multiplicative group) of a field $\mathbb{F}$. Further, it is known that

Theorem 1. *Suppose G is finite abelian of order m and m divides $|\mathbb{F}^\times|$. If V is the vector space of all $\mathbb{F}$-valued functions on G, then* $\mathrm{Hom}(G, \mathbb{F}^\times)$ *forms a basis for V.*

In order to not distract ourselves with technicalities, we shall defer the proof to the appendix.

Let us now turn our attention to the statement of the conjecture. Assuming the contrary, it follows that for every permutation $\pi \in S_k$, there exist distinct indices $i = i(\pi), j = j(\pi)$ such that $a_i + b_{\pi(i)} = a_j + b_{\pi(j)}$. Or in other words, the vector

$$[a_1 + b_{\pi(1)}, a_2 + b_{\pi(2)}, \ldots, a_k + b_{\pi(k)}]$$

has two of its entries equal. Staring at this hypothesis, we observe two things: first, that we have a bunch of constraints corresponding to the space of permutations S_k, and second, that it talks about two entries in a vector being equal. We are supposed to somehow use a combination of these *permutation-constraints* to arrive at a contradiction. What is the most natural such combination that we know of? Yes, the determinant! Further, the second observation alludes to us that the fact that the determinant of a matrix with two identical columns is zero must be lying somewhere in the background!

Now for the determinant to make sense, we need to work over a field. Also, we need to construct a square matrix out of the given vector. This motivates us to recast the hypothesis as the following:

Observation 1. *Let $\mathbb{F}$ be a field and suppose $f_1, \ldots, f_k$ be $\mathbb{F}$-valued functions on G. Then given $\pi \in S_k$, if*

$$A = \begin{bmatrix} f_1(a_1 + b_{\pi(1)}) & f_1(a_2 + b_{\pi(2)}) & \ldots & f_1(a_k + b_{\pi(k)}) \\ f_2(a_1 + b_{\pi(1)}) & f_2(a_2 + b_{\pi(2)}) & \ldots & f_2(a_k + b_{\pi(k)}) \\ \vdots & \vdots & & \vdots \\ f_k(a_1 + b_{\pi(1)}) & f_k(a_2 + b_{\pi(2)}) & \ldots & f_k(a_k + b_{\pi(k)}) \end{bmatrix},$$

then $\det A = 0$.

Let $\det \|a_{ij}\|$ denote the determinant of the $k \times k$ matrix in $M_k(\mathbb{F})$ whose $(i, j)^{\text{th}}$ entry is a_{ij}. Then observation 1 implies that for every permutation $\tau \in S_k$, $\det \|f_i(a_j + b_{\tau(j)})\| = 0$. The most natural thing to do next is to add all these determinants. Also, recall that the determinant itself is defined as the signed summation of certain products over all permutations. For ease of writing, let us work over a field of characteristic 2 so that the determinant becomes the permanent *i.e.*, the signs can be ignored. So we have that the following double summation is zero:

$$0 = \sum_{\tau \in S_k} \det \|f_i(a_j + b_{\tau(j)})\| = \sum_{\tau \in S_k} \sum_{\pi \in S_k} \prod_{i \in [k]} f_i(a_{\pi(i)} + b_{\tau(\pi(i))})$$

What happens when we switch the summations?

$$\sum_{\tau \in S_k} \sum_{\pi \in S_k} \prod_{i \in [k]} f_i(a_{\pi(i)} + b_{\tau(\pi(i))}) = \sum_{\pi \in S_k} \sum_{\tau \in S_k} \prod_{i \in [k]} f_i(a_{\pi(i)} + b_{\tau(\pi(i))})$$

Carry out the transformation $(i \longmapsto \pi^{-1}(i))$:

$$= \sum_{\pi^{-1} \in S_k} \sum_{\tau \in S_k} \prod_{i \in [k]} f_{\pi^{-1}(i)}(a_i + b_{\tau(i)})$$

$(\pi^{-1} \longmapsto \pi)$ yields:

$$= \sum_{\pi \in S_k} \sum_{\tau \in S_k} \prod_{i \in [k]} f_{\pi(i)}(a_i + b_{\tau(i)})$$

$$= \sum_{\pi \in S_k} \det \|f_{\pi(i)}(a_i + b_j)\|$$

This is the first non-trivial result we have arrived at! Let us record it as,

Observation 2. *Suppose $f_1, \ldots, f_k$ are $\mathbb{F}$-valued functions on G. Then under the assumption of falsity of Snevily's conjecture,*

$$\sum_{\pi \in S_k} \det\| f_{\pi(i)}(a_i + b_j)\| = 0.$$

3. Searching in History Books

To solve an open problem, it is always fruitful to look back at the theory in context and try to determine how the theory can be applied. In our case, let us first look at the language Snevily posed his conjecture in. We will need a couple of definitions first.

Definition 1. *If $(G, +)$ is an abelian group of order m with elements $g_1, \ldots, g_m$, then its Cayley table is defined as the $m \times m$ array A_G whose $(i, j)^{\text{th}}$ entry is $g_i + g_j$.*

Definition 2. *A transversal of an $m \times m$ matrix is a collection of m cells, no two of which are in the same row or column. A transversal of a matrix is a latin transversal if no two of its cells contain the same element.*

Snevily's conjecture states that any $k \times k$ submatrix of the Cayley table of an abelian group of odd order has a latin transversal.

Thus, Snevily's conjecture states that any $k \times k$ submatrix of the Cayley table of an abelian group of odd order has a latin transversal. Let us go back and look at Observation 2. It is a statement about the determinant of (a function of) a $k \times k$ submatrix of the Cayley table. This motivates us to look up existing literature about the *determinant of the Cayley table*. Indeed, we have the following well-known result:

Theorem 2. *(Frobenius Determinant) Let a finite group G have elements $g_1, g_2, \ldots, g_n$, and let x_{g_i} be associated with each element of G. Define the matrix X_G with entries $a_{ij} = x_{g_i g_j}$. Then,*

$$\det X_G = \prod_{j=1}^{r} P_j(x_{g_1}, x_{g_2}, \ldots, x_{g_n})^{\deg P_j}$$

for some pairwise non-proportional irreducible polynomials P_js and where r is the number of conjugacy classes of G.

The theory of characters and representations started with the computation of the group determinant by Frobenius as mentioned in the theorem.

A little bit of history about this result. This was a conjecture made in 1896 by the mathematician Richard Dedekind, who wrote a letter to F. G. Frobenius about it, who ultimately proved it. In the process, it became the starting point for creation of the modern field of representation theory!

We are interested in what the theorem implies for abelian groups:

Corollary 3. *Let G be a finite abelian group having elements $g_1, g_2, \ldots, g_m$, and let x_{g_i} be associated with each element of G. Then there is an assignment of these formal variables $\{x_{g_i} = z_i\}$ in the underlying field (say, $\mathbb{C}$) such that* $\det X_G(z_1, \ldots, z_m) \neq 0$.

Proof. We know that since G is abelian, it has precisely m conjugacy classes. Further, since all P_js are irreducible, we must have that $\deg P_j \geq 1$ and that $m = \sum_{i=1}^{m} (\deg P_i)^2$ which forces every P_j to be linear so that $\det X_G = (x_{g_1} - y_1)(x_{g_2} - y_2) \ldots (x_{g_m} - y_m)$ for some $y_j \in \mathbb{C}$. Thus, one can find an assignment $\{z_i\}$ such that each factor is non-zero. □

Remark. *Both theorem 2 and corollary 3 are true in the case when G is of odd order and the underlying field has characteristic 2.*

Although it would turn out later that we don't need this theorem directly for proving Snevily's conjecture, just the statement of the corollary in our context gives us several ideas to progress:

Idea 1: Corollary 3 suggests, at least when $k = m$, that there exists a function $f : G \to \mathbb{F}$, where $\mathbb{F}$ is as chosen before (*i.e.*, of characteristic 2 and such that m divides $|\mathbb{F}^\times|$) such that $\det \|f(a_i + b_j)\| \neq 0$. So the next thing to ask is if it holds for a general $1 \leq k \leq m$.

Idea 2: Suppose that idea 1 works *i.e.*, given k, there is a function corresponding to which the determinant of the $k \times k$ submatrix in question is non-zero. But then to contradict idea 1, it is reasonable

to propose that $\det \|f(a_i + b_j)\| = 0$ for every function f. In fact, since theorem 1 tells us that any function is a linear combination of (m distinct) *characters*, to prove that the determinant is zero, we could start off by applying observation 2 to the characters, taken k at a time.

Henceforth, assume that $\mathbb{F}$ has characteristic 2 and m divides $|\mathbb{F}^\times|$. (It is an easy exercise to prove that all odd numbers divide a number of the form $2^n - 1$.)

4. Finishing Things Off

Let us begin by exploring idea 1. The following proof is by Arsovski [4].

Lemma 1. *Let A be a $k \times k$ matrix, each of whose entries is one of the formal variables $z_1, ..., z_m$, and such that any two entries in the same row or the same column are distinct. Then these formal variables can be assigned values from $\mathbb{F}$ so that* $\det A \neq 0$.

Proof. The proof proceeds by induction by k. The case $k = 1$ is trivial. If k is greater than 1, we may assume without loss of generality that z_1 appears as an entry. The determinant of A is a polynomial in z_1, of degree at most $k < |\mathbb{F}|$, with leading coefficient being the determinant of a submatrix of A. By the induction hypothesis, the formal variables $z_2, ..., z_m$ can be assigned values from $\mathbb{F}$ so that this coefficient is non-zero. The polynomial in z_1, obtained in this way, is not the zero polynomial, and has degree at most $k < |\mathbb{F}|$; therefore, z_1 can be assigned a value from $\mathbb{F}$ so that this polynomial does not vanish. □

The multilinearity property of the determinant map is very useful as we see here.

Lemma 2. *Suppose that φ is any map from G to $\mathbb{F}$. Then*

$$\det \|\varphi(a_i + b_j)\| = 0.$$

Proof. The system of all characters $\varphi_1, ..., \varphi_m : G \to \mathbb{F}^\times$ forms a basis of the vector space of all maps from G to $\mathbb{F}$. Therefore, there are elements $\lambda_1, ..., \lambda_m \in \mathbb{F}$ such that $\varphi = \lambda_1\varphi_1 + \ldots + \lambda_m\varphi_m$.

Substituting, the determinant is,

$$\det \|\varphi(a_i + b_j)\| = \det \| \sum_{s=1}^{m} \lambda_s \varphi_s(a_i + b_j)\|.$$

Observe that the i^{th} row is the linear combination of some m vectors

$$[\varphi_1(a_i + b_1), \ldots, \varphi_1(a_i + b_k)], [\varphi_2(a_i + b_1), \ldots, \varphi_2(a_i + b_k)], \ldots, [\varphi_m(a_i + b_1), \ldots, \varphi_m(a_i + b_k)].$$

So naturally, the next idea is to exploit the multilinearity of the determinant *i.e.*, to choose one such vector for each of the k rows and sum the resulting determinant over all possible choices of vectors. Note that 'choosing a vector for row i' corresponds to picking an index $1 \leq s_i \leq m$ for row i *i.e.*, choosing the vector $[\varphi_{s_i}(a_i + b_1), \ldots, \varphi_{s_i}(a_i + b_k)]$ for row i. Thus, we can write

$$\det \| \sum_{s=1}^{m} \lambda_s \varphi_s(a_i + b_j)\| = \sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i} \right) \det \|\varphi_{s_i}(a_i + b_j)\|. \quad (1)$$

What happens when two of the chosen indices are equal? This is where the homomorphism property of the characters comes in. Suppose, $s_p = s_q$ $(= s, \text{say})$ for some $1 \leq p < q \leq k$. Then we claim that rows p and q are proportional. Indeed, observe that for every $j \in [k]$,

$$\varphi_s(a_q + b_j) = \varphi_s(a_q - a_p)\varphi_s(a_p + b_j),$$

which implies,

$$[\varphi_{s_p}(a_p+b_1), \ldots, \varphi_{s_p}(a_p+b_k)] = \varphi_s(a_q-a_p)[\varphi_{s_q}(a_q+b_1), \ldots, \varphi_{s_q}(a_q+b_k)].$$

Thus, in this case, the resulting determinant vanishes! Therefore, in the right hand side of (1), only the terms corresponding to pairwise distinct s_is survive. These pairwise distinct s_is can be chosen in the following manner. We choose a length k strictly increasing sequence in $[m]$, say $1 \leq t_1 < t_2 < \ldots < t_k \leq m$ and consider all

permutations of this sequence, assigning for a given $\pi \in S_k$ the index $t_{\pi(i)}$ to row i. We thus have,

$$\sum_{s_1,\ldots,s_k=1}^{m} \left(\prod_{i=1}^{k} \lambda_{s_i}\right) \det \|\varphi_{s_i}(a_i + b_j)\| = \sum_{1\le t_1<t_2<\ldots<t_k\le m} \left(\prod_{i=1}^{k} \lambda_{t_i}\right)\left(\sum_{\pi\in S_k} \det \|\varphi_{t_{\pi(i)}}(a_i + b_j)\|\right).$$

But on the right hand side, for any sequence $1 \le t_1 < t_2 < \ldots < t_k \le m$,

$$\sum_{\pi\in S_k} \det \|\varphi_{t_{\pi(i)}}(a_i + b_j)\| = 0,$$

by observation 2, by choosing $f_i = \varphi_{t_i}$. Finally, we can conclude that

$$\det \|\varphi(a_i + b_j)\| = 0.$$

□

Lemma 1 and 2 finally give us the desired contradiction. Indeed, if we associate with every element $g \in G$ a formal variable x_g, then all entries in the same row or in the same column of the matrix $[x_{a_i+b_j}]$ are distinct. By lemma 1, x_g can be assigned a value $\varphi(g)$ such that the determinant of the resulting matrix $[\varphi(a_i+b_j)]$ is non-zero. But this immediately contradicts lemma 2. We have thus proved Snevily's conjecture.

Appendix

As promised, following is the proof of theorem 1.

Claim. *The distinct characters of G are linearly independent as members of V.*

Proof. Assume the contrary. Let $\chi_1, \ldots, \chi_s$ be distinct characters with the dependency relation,

$$a_1\chi_1(x) + \ldots + a_s\chi_s(x) = 0, \qquad (2)$$

for every $x \in G$. Further, assume minimality of s (≥ 2). As $\chi_1 \neq \chi_2$, $\chi_1(g) \neq \chi_2(g)$ for some $g \in G$. Multiply (2) by $\chi_1(g)$, and then subtract $\sum a_i\chi_i(xg) = \sum a_i\chi_i(x)\chi_i(g) = 0$ to get

$$\sum_{j\geq 2} a_j\chi_j(x)(\chi_1(g) - \chi_j(g)) = 0,$$

contradicting minimality of s.

Let $\mathrm{Hom}(G, \mathbb{F}^\times)$, also called the character group of G, be denoted by $\widehat{G}$. We thus need to show that $|G| = |\widehat{G}|$. From the claim, it follows that $|\widehat{G}| \leq \dim V = |G| = m$. It is therefore enough to show that there are m distinct characters of G. Indeed, if G is cyclic *i.e.*, $G = \mathbb{Z}_m$ and $|\mathbb{F}^\times| = mr$ where r is an integer, then identify $\mathbb{F}^\times$ with $\mathbb{Z}_{mr}$ and consider the (distinct) homomorphisms which send $1 \in G$ to sr as $s \in \{0, 1, \ldots, m-1\}$. In fact, it is also easy to see that these characters form a cyclic group generated by the homomorphism which sends $1 \in G$ to r with the group operation being pointwise addition.

This basic property of independence of characters due to Dedekind is very easy to prove and one of the crucial ingredients in many arguments.

If $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$ and $|\mathbb{F}^\times| = mr = np$, then we can send the generators $(1, 0), (0, 1) \in G$ to sr (where $s \in \{0, 1, \ldots, m-1\}$) and tp (where $t \in \{0, 1, \ldots, n-1\}$) respectively, giving rise to mn distinct homomorphisms. Thus, $|\widehat{\mathbb{Z}_m \oplus \mathbb{Z}_n}| = mn$ and further, by similar reasoning one can argue that $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \widehat{\mathbb{Z}_m \oplus \mathbb{Z}_n}$. Finally then for a general finite abelian group G with $|G|$ dividing $|\mathbb{F}^\times|$, $G \cong \widehat{G}$ follows from the structure theorem for finitely generated abelian groups. □

Suggested Reading

[1] **H Snevily, Unsolved Problems: The Cayley Addition Table of $\mathbb{Z}/n\mathbb{Z}$, *American Mathematical Monthly* Vol.106, pp.584–585, 1999.**

[2] **N Alon, Additive Latin Transversals, *Israel Journal of Mathematics*, Vol.117, pp.125–130, 2000.**

[3] **S Dasgupta, Gy. Karolyi, O Serra and B Szegedy, Transversals of Additive Latin Squares, *Israel Journal of Mathematics*, Vol.126, pp.17–28, 2001.**

[4] **B Arsovski, A Proof of Snevily's Conjecture, *Israel Journal of Mathematics*, Vol.182, pp.505–508, 2011.**