Some new computations regarding Alspach's Conjecture

Sarah Rovner-Frydman

May 1, 2020

1 Alspach's Conjecture and the polynomial method

Alspach's Conjecture is an open problem in combinatorics. To state it, we'll need the following definition: Given an abelian group A and a finite subset $S \subseteq G$, a *sequencing* of S is an enumeration $a_1, \ldots, a_n$ of S such that the sequence of partial sums $0, a_1, a_1 + a_2, \ldots, \sum_i a_i$ contains no duplicates. If $0 \in S$, then S has no sequencing, because then any enumeration must place 0 as one of the terms, and then two adjacent partial sums will be the same; and if the sum of the elements of S is 0, then S has no sequencing, because 0 occurs as the first and last term of any enumeration's partial sums. Are these the only possible barriers to the existence of a sequencing? Alspach's Conjecture is that this is the case, at least in cyclic groups: that any $S \subseteq \mathbb{Z}_n$ which does not contain 0 or sum to 0 admits a sequencing. It is further conjectured that this is true in any other finite abelian group as well.

[wikipedia voice] by whom?

?

In the prime-order case, however, we have an extra tool: the structure of an integral domain! Over integral domains, many statements can be turned into ones about polynomials, and have just such luck in this case. Consider a fixed integral domain R and a subset $S \subseteq R$; write n for $|S|$. We can formulate "S has a sequencing" as follows:

$$\overbrace{\exists a_1 \in S, \ldots, a_n \in S.}^{\text{an enumeration of } S} \left(\bigwedge_{1 \le i < j \le n} a_i \neq a_j \right) \wedge \overbrace{\left(\bigwedge_{0 \le i < j \le n} \sum_{k=1}^{i} a_k \neq \sum_{k=1}^{j} a_k \right)}^{\text{whose partial sums are distinct}}.$$

If S satisfies the side conditions described above, then there is some redundancy in this formula. In particular, the conjuncts of the form $\sum_{k=1}^{i} a_k \neq \sum_{k=1}^{j} a_k$ automatically follow in this case for $i = 0, j = n$ and $j = i + 1$. So we can weaken the formula to

$$\exists a_1 \in S, \ldots, a_n \in S. \left(\bigwedge_{1 \le i < j \le n} a_i \neq a_j \right) \wedge \left(\bigwedge_{\substack{0 \le i < j \le n \\ j \neq i+1 \\ (i,j) \neq (0,n)}} \sum_{k=1}^{i} a_k \neq \sum_{k=1}^{j} a_k \right).$$

We can then apply de Morgan's laws to transform this into

$$\exists a_1 \in S, \ldots, a_n \in S.\ \neg \left(\left(\bigvee_{1 \le i < j \le n} a_i = a_j \right) \vee \left(\bigvee_{\substack{0 \le i < j \le n \\ j \neq i+1 \\ (i,j) \neq (0,n)}} \sum_{k=1}^{i} a_k = \sum_{k=1}^{j} a_k \right) \right).$$

This is where the integral domain structure becomes relevant: the negated formula is a disjunction of equations that are polynomial in the a_is, and any disjunction of such equations in an integral domain can be transformed into a single polynomial equation. If we define

$$p(x_1, \ldots, x_n) = \left(\prod_{1 \le i < j \le n} x_i - x_j \right) \left(\prod_{\substack{0 \le i < j \le n \\ j \neq i+1 \\ (i,j) \neq (0,n)}} \sum_{k=1}^{i} x_k - \sum_{k=1}^{j} x_k \right), \quad (1)$$

then for side-condition-satisfying S, "S has a sequencing" reduces to

$$\exists a_1 \in S, \ldots, a_n \in S.\ p(a_1, \ldots, a_n) \neq 0.$$

In other words, "does p have a non-root in S^n?"

At this point, we may not appear to have saved ourselves much work; a brute-force search through S^n for a non-root of p is essentially the same computational task as a brute-force search through S^n for a sequencing. However, there is another key trick: we use the *non-vanishing corollary to the combinatorial Nullstellensatz* [1]:

Theorem 1. *Let R be an integral domain and let p be a polynomial over R in k variables. Let $A_1, \ldots, A_k \subseteq R$. If p includes a monomial of maximal degree $x_1^{t_1} \ldots x_k^{t_k}$ such that $t_i < |A_i|$ for each i, then it follows that there is a non-root of p in $A_1 \times \cdots \times A_k$.*

This citation only states this theorem for a field, even though it's true in an integral domain!

Turn off numbering here maybe?

In particular, let $k = n$ and $A_i = S$; then a sufficient (but unfortunately not necessary!) condition for p to have a non-root in S^n is for it to have a monomial of maximal degree all of whose exponents are less than n. This is far more computationally tractable to check than a brute-force search for non-roots, but it has an additional huge bonus: the definition given for p depended on S only by way of its cardinality n, so any other side-condition-satisfying S' of the same size will also have a sequencing iff p has a non-root in S'^n. Hence, if p has a monomial whose presence implies a sequencing for S by the above reasoning, it also implies a sequencing for all other side-condition-satisfying subsets of R of the same size! So we have one prospective path to verifying that a large number of cases of Alspach's conjecture hold much more efficiently: given some integral domain R and cardinality for subsets of it, we compute the terms of

the associated polynomial. If we find one of maximal degree[1] whose exponents are all strictly bounded by the cardinality in question, then we will be able to conclude that every side-condition-satisfying subset of R of this size can be sequenced.

But we can do even better. For any commutative ring R, define p_n^R to be the polynomial in n variables over R given by (1). As matters stand, we may be able to prove something about many subsets of a given integral domain R at once by examining p_n^R. But if we switch to considering $p_n^{\mathbb{Z}}$ in particular, we can use the fact that $\mathbb{Z}$ is the initial commutative ring to conclude something about *all* p_n^R at once. In particular: For any R, we have a unique homomorphism $f : \mathbb{Z} \to R$, whose kernel is $(\operatorname{char} R)\mathbb{Z}$. This extends to a homomorphism $\hat{f} : \mathbb{Z}[x_1, \ldots, x_n] \to R[x_1, \ldots, x_n]$ which applies f to the coefficients of a polynomial. Then, it is easy to show that $p_n^R = \hat{f}(p_n^{\mathbb{Z}})$, so the monomials of p_n^R will be exactly the monomials of $p_n^{\mathbb{Z}}$ whose coefficients are not sent to 0 by f—i.e., those whose coefficients in $p_n^{\mathbb{Z}}$ are not divisible by $\operatorname{char} R$. Altogether, the presence of a leading term of $p_n^{\mathbb{Z}}$ with coefficient k implies that Alspach's conjecture holds for sets of size n in the additive group of every integral domain whose characteristic does not divide k—infinitely many cases at once!

Thus, in order to find numerical evidence for Alspach's conjecture, one approach is to examine the terms of $p_n^{\mathbb{Z}}$. However, $p_n^{\mathbb{Z}}$ is an enormous polynomial whose number of terms grows roughly exponentially in n—even $p_6^{\mathbb{Z}}$ has around $10,000$ terms! Hence, for this to be practical, we need to be smart about it.

factorially?

2 New Results

I have developed a Haskell library for doing computations with multivariate polynomials of the kind necessary for finding useful coefficients in $p_n^{\mathbb{Z}}$. It improves performance primarily by discarding unnecessary information—note that we really only care about very particular terms of $p_n^{\mathbb{Z}}$. Technical details can be found in this repository in `computation/`, in the Haddock for the `Math.Polynomial` module.

Using this library, we have been able to establish Alspach's conjecture for subsets of size $|S| = 11$ in prime fields, the best result of this kind known to us. We have also been able to verify prior such computations more efficiently.

The library is sufficiently general-purpose as to be potentially applicable to similar uses of polynomials in combinatorics, or at very least, related Alspach-type problems. One possible use case that we began to investigate is the application to Alspach for composite-order groups.

[1] Actually, the polynomial is homogeneous, so all terms have equal and hence maximal degree.

References

[1] Noga Alon. “Combinatorial Nullstellensatz”. In: *Combinatorics, Probability and Computing* 8.1-2 (1999), pp. 7–29.