Permutations destroying arithmetic progressions in finite cyclic groups

Peter Hegarty
(joint work with Anders Martinsson)

Department of Mathematics, Chalmers/Gothenburg University

Monday, 6 July, 2015

- [H, 2004] P. Hegarty, *Permutations avoiding arithmetic patterns*, Electron. J. Combin. **11** (2004), No. 1, Paper 39, 21pp.
- [JS, 2015] V. Jungic and J. Sahasrabudhe, *Permutations destroying arithmetic structure*, Electron. J. Combin. **22** (2015), No. 2, Paper P2.5, 14pp.
- [HM, 2015] P. Hegarty and A. Martinsson, *Permutations destroying arithmetic progressions in finite cyclic groups*. Preprint available at `http://arxiv.org/abs/1506.05342`

- G an abelian group

- G an abelian group
- S a subset of G

- G an abelian group
- S a subset of G
- $f : S \to S$ a function

- G an abelian group
- S a subset of G
- $f : S \to S$ a function
- f is said to **destroy arithmetic progressions (APs)** if:

- G an abelian group
- S a subset of G
- $f : S \to S$ a function
- f is said to **destroy arithmetic progressions (APs)** if:

  Whenever (a, b, c) is a non-trivial 3-term AP in G, then $(f(a), f(b), f(c))$ is not an AP.

- G an abelian group
- S a subset of G
- $f : S \to S$ a function
- f is said to **destroy arithmetic progressions (APs)** if:

  Whenever (a, b, c) is a non-trivial 3-term AP in G, then $(f(a), f(b), f(c))$ is not an AP.
- Special cases of most interest:

- G an abelian group
- S a subset of G
- $f : S \to S$ a function
- f is said to **destroy arithmetic progressions (APs)** if:

  Whenever (a, b, c) is a non-trivial 3-term AP in G, then $(f(a), f(b), f(c))$ is not an AP.
- Special cases of most interest:
  (i) $G = \mathbb{Z}$, $S = \mathbb{N}$ or $\{1, \dots, n\}$; or

- G an abelian group
- S a subset of G
- $f : S \to S$ a function
- f is said to **destroy arithmetic progressions (APs)** if:

  Whenever (a, b, c) is a non-trivial 3-term AP in G, then $(f(a), f(b), f(c))$ is not an AP.
- Special cases of most interest:
  (i) $G = \mathbb{Z}$, $S = \mathbb{N}$ or $\{1, \ldots, n\}$; or
  $G = S = \mathbb{Z}_n$ for some $n > 0$.

- G an abelian group
- S a subset of G
- $f : S \to S$ a function
- f is said to **destroy arithmetic progressions (APs)** if:

  Whenever (a, b, c) is a non-trivial 3-term AP in G, then $(f(a), f(b), f(c))$ is not an AP.
- Special cases of most interest:
  (i) $G = \mathbb{Z}$, $S = \mathbb{N}$ or $\{1, \ldots, n\}$; or
  $G = S = \mathbb{Z}_n$ for some $n > 0$.
  (ii) f a bijection (permutation).

- Our definition is not to be confused with the notion of a permutation **not containing any (*k*-term) APs** (Davis et al, 1977).

- Our definition is not to be confused with the notion of a permutation **not containing any (*k*-term) APs** (Davis et al, 1977).
- A **Costas array** is a permutation of $\{1, \ldots, n\}$ destroying all non-trivial Sidon quadruples, that is, non-trivial solutions to $a + b = c + d$.

- Our definition is not to be confused with the notion of a permutation **not containing any (*k*-term) APs** (Davis et al, 1977).

- A **Costas array** is a permutation of $\{1, \ldots, n\}$ destroying all non-trivial Sidon quadruples, that is, non-trivial solutions to $a + b = c + d$.

  A 3-term AP is a non-trivial solution to $a - 2b + c = 0$.

- Our definition is not to be confused with the notion of a permutation **not containing any (k-term) APs** (Davis et al, 1977).

- A **Costas array** is a permutation of $\{1, \ldots, n\}$ destroying all non-trivial Sidon quadruples, that is, non-trivial solutions to $a + b = c + d$.

  A 3-term AP is a non-trivial solution to $a - 2b + c = 0$.

  Our basic definition can be immediately extended to any linear equation with integer coefficients.

- Our definition is not to be confused with the notion of a permutation **not containing any (k-term) APs** (Davis et al, 1977).

- A **Costas array** is a permutation of $\{1, \ldots, n\}$ destroying all non-trivial Sidon quadruples, that is, non-trivial solutions to $a + b = c + d$.

  A 3-term AP is a non-trivial solution to $a - 2b + c = 0$.

  Our basic definition can be immediately extended to any linear equation with integer coefficients.

  Indeed, one may consider systems of linear equations, or even non-linear equations. But we will not do so in this talk.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations. Consideration of a random permutation and assuming a "Poisson paradigm" would lead one to expect that $M(n) = e^{-\Theta(n)} n!$.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations. Consideration of a random permutation and assuming a "Poisson paradigm" would lead one to expect that $M(n) = e^{-\Theta(n)} n!$.
- Open problem to make this intuition rigorous. Dependencies between the events of destroying individual APs are subtle.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations. Consideration of a random permutation and assuming a "Poisson paradigm" would lead one to expect that $M(n) = e^{-\Theta(n)} n!$.
- Open problem to make this intuition rigorous. Dependencies between the events of destroying individual APs are subtle.
- Note that in the case of a linear equation with k variables, the corresponding estimate would be $e^{-\Theta(n^{k-2})} n!$.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations. Consideration of a random permutation and assuming a "Poisson paradigm" would lead one to expect that $M(n) = e^{-\Theta(n)} n!$.
- Open problem to make this intuition rigorous. Dependencies between the events of destroying individual APs are subtle.
- Note that in the case of a linear equation with k variables, the corresponding estimate would be $e^{-\Theta(n^{k-2})} n!$.
- Hence, for $k \geq 4$, such permutations may well not exist at all, for most n.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations. Consideration of a random permutation and assuming a "Poisson paradigm" would lead one to expect that $M(n) = e^{-\Theta(n)} n!$.
- Open problem to make this intuition rigorous. Dependencies between the events of destroying individual APs are subtle.
- Note that in the case of a linear equation with k variables, the corresponding estimate would be $e^{-\Theta(n^{k-2})} n!$.
- Hence, for $k \geq 4$, such permutations may well not exist at all, for most n.
- For Costas arrays, it is a well-known problem whether they exist or not for all $n \gg 0$.

- Easy to prove, by an inductive argument, that AP-destroying permutations exist for every n (H, 2004)
- Let $M(n)$ denote the number of such permutations. Consideration of a random permutation and assuming a "Poisson paradigm" would lead one to expect that $M(n) = e^{-\Theta(n)} n!$.
- Open problem to make this intuition rigorous. Dependencies between the events of destroying individual APs are subtle.
- Note that in the case of a linear equation with k variables, the corresponding estimate would be $e^{-\Theta(n^{k-2})} n!$.
- Hence, for $k \geq 4$, such permutations may well not exist at all, for most n.
- For Costas arrays, it is a well-known problem whether they exist or not for all $n \gg 0$. However, there are "algebraic" constructions which work for infinitely many n.

- Can construct an AP-destroying permutation of $\mathbb{N}$ by a **greedy algorithm**:

- Can construct an AP-destroying permutation of $\mathbb{N}$ by a **greedy algorithm**:

$\pi(1) := 1,$

- Can construct an AP-destroying permutation of $\mathbb{N}$ by a **greedy algorithm**:

  $\pi(1) := 1$,
  Having chosen $\pi(1), \ldots, \pi(n-1)$, choose $\pi(n)$ to be the smallest number not yet chosen and which doesn't screw things up !

- Can construct an AP-destroying permutation of $\mathbb{N}$ by a **greedy algorithm**:

  $\pi(1) := 1$,
  Having chosen $\pi(1), \ldots, \pi(n-1)$, choose $\pi(n)$ to be the smallest number not yet chosen and which doesn't screw things up !
- A not-quite-trivial exercise to show that this works and that π is surjective, hence an AP-destroying permutation of $\mathbb{N}$.

- Can construct an AP-destroying permutation of $\mathbb{N}$ by a **greedy algorithm**:

  $\pi(1) := 1$,
  Having chosen $\pi(1), \ldots, \pi(n-1)$, choose $\pi(n)$ to be the smallest number not yet chosen and which doesn't screw things up !
- A not-quite-trivial exercise to show that this works and that π is surjective, hence an AP-destroying permutation of $\mathbb{N}$.
- Simulations suggest that $\pi(n)/n \to 1$ as $n \to \infty$, though slowly and "chaotically".

- Can construct an AP-destroying permutation of $\mathbb{N}$ by a **greedy algorithm**:

  $\pi(1) := 1$,
  Having chosen $\pi(1), \ldots, \pi(n-1)$, choose $\pi(n)$ to be the smallest number not yet chosen and which doesn't screw things up !
- A not-quite-trivial exercise to show that this works and that π is surjective, hence an AP-destroying permutation of $\mathbb{N}$.
- Simulations suggest that $\pi(n)/n \to 1$ as $n \to \infty$, though slowly and "chaotically". All that has been proven so far (H, 2004) is that, for all n,

$$\frac{3}{8} \leq \frac{\pi(n)}{n} \leq \frac{3}{2}.$$

- This "greedy algorithm" can be used to construct AP-destroying permutations of countably infinite abelian groups in general.

- This "greedy algorithm" can be used to construct AP-destroying permutations of countably infinite abelian groups in general.

Theorem (H, 2004) *Let G be a countable infinite abelian group. Then there exists an AP-destroying permutation of G if and only if the quotient group $G/\Omega_2(G)$ is infinite.*

- This "greedy algorithm" can be used to construct AP-destroying permutations of countably infinite abelian groups in general.

  Theorem (H, 2004) *Let G be a countable infinite abelian group. Then there exists an AP-destroying permutation of G if and only if the quotient group $G/\Omega_2(G)$ is infinite.*
- Generalisation given in [JS, 2015] to arbitrary linear equations.

- This "greedy algorithm" can be used to construct AP-destroying permutations of countably infinite abelian groups in general.

  Theorem (H, 2004) *Let G be a countable infinite abelian group. Then there exists an AP-destroying permutation of G if and only if the quotient group $G/\Omega_2(G)$ is infinite.*

- Generalisation given in [JS, 2015] to arbitrary linear equations.
- Note, in particular, for $k \geq 4$ variables, the difference to the finite case, where it's not expected that such permutations exist in general.

- An alternative AP-destroying permutation of $\mathbb{N}$ is given explicitly by (Sidorenko, 1988)

$$f\left(\sum a_i 4^i\right) = \sum \pi(a_i) 4^i,$$

- An alternative AP-destroying permutation of $\mathbb{N}$ is given explicitly by (Sidorenko, 1988)

$$f\left(\sum a_i 4^i\right) = \sum \pi(a_i) 4^i,$$

where π is the permutation of $\{0, 1, 2, 3\}$ given by

$$\pi(0) = 0, \quad \pi(1) = 2, \quad \pi(2) = 1, \quad \pi(3) = 3.$$

- An alternative AP-destroying permutation of $\mathbb{N}$ is given explicitly by (Sidorenko, 1988)

$$f\left(\sum a_i 4^i\right) = \sum \pi(a_i) 4^i,$$

where π is the permutation of $\{0, 1, 2, 3\}$ given by

$$\pi(0) = 0, \quad \pi(1) = 2, \quad \pi(2) = 1, \quad \pi(3) = 3.$$

- The point is that π has the stronger property of destroying APs modulo 4, i.e.: it is an AP-destroying permutation of the abelian group $G = \mathbb{Z}_4$.

- An alternative AP-destroying permutation of $\mathbb{N}$ is given explicitly by (Sidorenko, 1988)

$$f\left(\sum a_i 4^i\right) = \sum \pi(a_i) 4^i,$$

where π is the permutation of $\{0, 1, 2, 3\}$ given by

$$\pi(0) = 0, \quad \pi(1) = 2, \quad \pi(2) = 1, \quad \pi(3) = 3.$$

- The point is that π has the stronger property of destroying APs modulo 4, i.e.: it is an AP-destroying permutation of the abelian group $G = \mathbb{Z}_4$.
  In the same way, any AP-destroying permutation of $\mathbb{Z}_n$ can be lifted to an AP-destroying permutation of $\mathbb{N}$.

- An alternative AP-destroying permutation of $\mathbb{N}$ is given explicitly by (Sidorenko, 1988)

$$f\left(\sum a_i 4^i\right) = \sum \pi(a_i) 4^i,$$

where π is the permutation of $\{0, 1, 2, 3\}$ given by

$$\pi(0) = 0, \quad \pi(1) = 2, \quad \pi(2) = 1, \quad \pi(3) = 3.$$

- The point is that π has the stronger property of destroying APs modulo 4, i.e.: it is an AP-destroying permutation of the abelian group $G = \mathbb{Z}_4$.
  In the same way, any AP-destroying permutation of $\mathbb{Z}_n$ can be lifted to an AP-destroying permutation of $\mathbb{N}$.
  This leads us to our main topic ...

- Conderation of a random permutation would still lead one to expect that the number of AP-destroying permutations of $\mathbb{Z}_n$ behaves as $e^{-\Theta(n)} n!$.

- Conderation of a random permutation would still lead one to expect that the number of AP-destroying permutations of $\mathbb{Z}_n$ behaves as $e^{-\Theta(n)} n!$.
- In particular, one expects such permutations to exist, at least for all $n \gg 0$.

- Conderation of a random permutation would still lead one to expect that the number of AP-destroying permutations of $\mathbb{Z}_n$ behaves as $e^{-\Theta(n)} n!$.
- In particular, one expects such permutations to exist, at least for all $n \gg 0$.
- However, in contrast to the case of $S = \{1, \ldots, n\}$, it seems non-trivial to find such permutations at all in $\mathbb{Z}_n$.

- Conderation of a random permutation would still lead one to expect that the number of AP-destroying permutations of $\mathbb{Z}_n$ behaves as $e^{-\Theta(n)}n!$.
- In particular, one expects such permutations to exist, at least for all $n \gg 0$.
- However, in contrast to the case of $S = \{1, \ldots, n\}$, it seems non-trivial to find such permutations at all in $\mathbb{Z}_n$. Indeed, none exist for $n \in \{2, 3, 5, 7\}$.

- Conderation of a random permutation would still lead one to expect that the number of AP-destroying permutations of $\mathbb{Z}_n$ behaves as $e^{-\Theta(n)}n!$.
- In particular, one expects such permutations to exist, at least for all $n \gg 0$.
- However, in contrast to the case of $S = \{1, \ldots, n\}$, it seems non-trivial to find such permutations at all in $\mathbb{Z}_n$. Indeed, none exist for $n \in \{2, 3, 5, 7\}$.
- In [H, 2004] I conjectured that there exists an AP-destroying permutation of $\mathbb{Z}_n$ if and only if $n \notin \{2, 3, 5, 7\}$. This I regard as the main open problem from that initial paper.

Here is what we currently know:

Here is what we currently know:

R1 (H, 2004): If there exist AP-destroying permutations of both $\mathbb{Z}_m$ and $\mathbb{Z}_n$, then there exists one of $\mathbb{Z}_{mn}$.

Here is what we currently know:

R1 (H, 2004): If there exist AP-destroying permutations of both $\mathbb{Z}_m$ and $\mathbb{Z}_n$, then there exists one of $\mathbb{Z}_{mn}$.

R2 (HM, 2015): Let p be a prime such that $p > 3$ and $p \equiv 3 \pmod 8$. Then there exists an AP-destroying permutation of $\mathbb{Z}_p$.

Here is what we currently know:

R1 (H, 2004): If there exist AP-destroying permutations of both $\mathbb{Z}_m$ and $\mathbb{Z}_n$, then there exists one of $\mathbb{Z}_{mn}$.

R2 (HM, 2015): Let p be a prime such that $p > 3$ and $p \equiv 3 \pmod 8$. Then there exists an AP-destroying permutation of $\mathbb{Z}_p$.

R3 (HM, 2015): There exists an AP-destroying permutation of $\mathbb{Z}_n$ for all $n \geq n_0$, where

$$n_0 = (9 \times 11 \times 16 \times 17 \times 19 \times 23)^2 \approx 1.4 \times 10^{14}.$$

Proof of R1:

Proof of R1: This is an application of the following more general fact:

Proof of R1: This is an application of the following more general fact:
Let G be an abelian group and H a subgroup.

Proof of R1: This is an application of the following more general fact:
Let G be an abelian group and H a subgroup. Let π_1 and π_2 be AP-destroying permutations of H and G/H respectively.

Proof of R1: This is an application of the following more general fact:
Let G be an abelian group and H a subgroup. Let π_1 and π_2 be AP-destroying permutations of H and G/H respectively. Choose a coset decomposition

$$G = \bigsqcup_i Hg_i.$$

Proof of R1: This is an application of the following more general fact:
Let G be an abelian group and H a subgroup. Let π_1 and π_2 be AP-destroying permutations of H and G/H respectively. Choose a coset decomposition

$$G = \bigsqcup_i Hg_i.$$

Then the function $\pi : G \to G$ given by

$$\pi(hg_i) = \pi_1(h)g_{\pi_2(i)}$$

is an AP-destroying permutation of G.

Proof of R2:

Proof of R2:
Let $\xi \in \{0, 1, \ldots, p-1\}$ be such that both ξ and $\xi - 1$ are quadratic non-residues modulo p.

Proof of R2:
Let $\xi \in \{0, 1, \ldots, p-1\}$ be such that both ξ and $\xi - 1$ are quadratic non-residues modulo p.
Define $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by

$$f(x) = \begin{cases} x^2, & \text{if } x \in \{0, 2, \ldots, p-1\}, \\ \xi x^2, & \text{if } x \in \{1, 3, \ldots, p-2\}. \end{cases}$$

Proof of R2:

Let $\xi \in \{0, 1, \ldots, p-1\}$ be such that both ξ and $\xi - 1$ are quadratic non-residues modulo p.

Define $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by

$$f(x) = \begin{cases} x^2, & \text{if } x \in \{0, 2, \ldots, p-1\}, \\ \xi x^2, & \text{if } x \in \{1, 3, \ldots, p-2\}. \end{cases}$$

Magic, it works ! But only if $p \equiv 3 \pmod 8$.

Proof of R2:
Let $\xi \in \{0, 1, \ldots, p-1\}$ be such that both ξ and $\xi - 1$ are quadratic non-residues modulo p.
Define $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by

$$f(x) = \begin{cases} x^2, & \text{if } x \in \{0, 2, \ldots, p-1\}, \\ \xi x^2, & \text{if } x \in \{1, 3, \ldots, p-2\}. \end{cases}$$

Magic, it works ! But only if $p \equiv 3 \pmod 8$.
Curiously, we have not been able to find any modification of this construction which works for other primes.

Proof of R3:

Proof of R3:

- Imagine the numbers $0, 1, \ldots, n-1$ placed round a circle and divided into k blocks, each of size M or $M+1$, where $M = \lfloor n/k \rfloor$.

Proof of R3:

- Imagine the numbers $0, 1, \ldots, n-1$ placed round a circle and divided into k blocks, each of size M or $M+1$, where $M = \lfloor n/k \rfloor$.
- We think of k as being fixed and M as variable.

Proof of R3:

- Imagine the numbers $0, 1, \ldots, n-1$ placed round a circle and divided into k blocks, each of size M or $M+1$, where $M = \lfloor n/k \rfloor$.
- We think of k as being fixed and M as variable.
- We permute the blocks according to some permutation π_1 of $\mathbb{Z}_k$ and permute within each block according to some permutations π_2, π_2' of $\mathbb{Z}_M$ or $\mathbb{Z}_{M+1}$, as appropriate.

Proof of R3:

- Imagine the numbers $0, 1, \ldots, n-1$ placed round a circle and divided into k blocks, each of size M or $M+1$, where $M = \lfloor n/k \rfloor$.
- We think of k as being fixed and M as variable.
- We permute the blocks according to some permutation π_1 of $\mathbb{Z}_k$ and permute within each block according to some permutations π_2, π_2' of $\mathbb{Z}_M$ or $\mathbb{Z}_{M+1}$, as appropriate.
- It suffices for π_2 to destroy APs as a permutation of $\{1, 2, \ldots, M\}$, and we know such permutations exist for all M.

Proof of R3:

- Imagine the numbers $0, 1, \ldots, n-1$ placed round a circle and divided into k blocks, each of size M or $M+1$, where $M = \lfloor n/k \rfloor$.
- We think of k as being fixed and M as variable.
- We permute the blocks according to some permutation π_1 of $\mathbb{Z}_k$ and permute within each block according to some permutations π_2, π_2' of $\mathbb{Z}_M$ or $\mathbb{Z}_{M+1}$, as appropriate.
- It suffices for π_2 to destroy APs as a permutation of $\{1, 2, \ldots, M\}$, and we know such permutations exist for all M.
- π_1 will need to destroy APs modulo k, that is, considered as a permutation of $\mathbb{Z}_k$. However, that is not quite enough, which is where the subtlety lies ...

- Let $\beta(x) \in [0, k)$ denote the number of the block containing $x \in [0, n)$.

- Let $\beta(x) \in [0, k)$ denote the number of the block containing $x \in [0, n)$.
- If (a, b, c) is an AP modulo n, then $(\beta(a), \beta(b), \beta(c))$ need not quite be an AP modulo k.

- Let $\beta(x) \in [0, k)$ denote the number of the block containing $x \in [0, n)$.
- If (a, b, c) is an AP modulo n, then $(\beta(a), \beta(b), \beta(c))$ need not quite be an AP modulo k. However, if $M \geq k$, then

$$|\beta(a) - 2\beta(b) + \beta(c)| \leq 2 \pmod{k}. \tag{1}$$

- Let $\beta(x) \in [0, k)$ denote the number of the block containing $x \in [0, n)$.
- If (a, b, c) is an AP modulo n, then $(\beta(a), \beta(b), \beta(c))$ need not quite be an AP modulo k. However, if $M \geq k$, then

$$|\beta(a) - 2\beta(b) + \beta(c)| \leq 2 \pmod{k}. \tag{1}$$

- **Definition:** A permutation π of $\mathbb{Z}_k$ is said to *destroy the pattern* $s \mapsto t$ if there is no triple (a, b, c) satisfying
(i) a, b, c not all equal and $a - 2b + c \equiv s \pmod{k}$,
(ii) $\pi(a) - 2\pi(b) + \pi(c) \equiv t \pmod{k}$.

- Let $\beta(x) \in [0, k)$ denote the number of the block containing $x \in [0, n)$.
- If (a, b, c) is an AP modulo n, then $(\beta(a), \beta(b), \beta(c))$ need not quite be an AP modulo k. However, if $M \geq k$, then

$$|\beta(a) - 2\beta(b) + \beta(c)| \leq 2 \pmod{k}. \qquad (1)$$

- **Definition:** A permutation π of $\mathbb{Z}_k$ is said to *destroy the pattern* $s \mapsto t$ if there is no triple (a, b, c) satisfying
(i) a, b, c not all equal and $a - 2b + c \equiv s \pmod{k}$,
(ii) $\pi(a) - 2\pi(b) + \pi(c) \equiv t \pmod{k}$.
- **Definition:** A permutation π of $\mathbb{Z}_k$ is said to *destroy* (s, t)*-almost APs* if it destroys the patterns $s' \mapsto t'$ for all $s' \in [-s, s]$ and $t' \in [-t, t]$.

- Let $\beta(x) \in [0, k)$ denote the number of the block containing $x \in [0, n)$.
- If (a, b, c) is an AP modulo n, then $(\beta(a), \beta(b), \beta(c))$ need not quite be an AP modulo k. However, if $M \geq k$, then

$$|\beta(a) - 2\beta(b) + \beta(c)| \leq 2 \pmod{k}. \tag{1}$$

- **Definition:** A permutation π of $\mathbb{Z}_k$ is said to *destroy the pattern* $s \mapsto t$ if there is no triple (a, b, c) satisfying
(i) a, b, c not all equal and $a - 2b + c \equiv s \pmod{k}$,
(ii) $\pi(a) - 2\pi(b) + \pi(c) \equiv t \pmod{k}$.
- **Definition:** A permutation π of $\mathbb{Z}_k$ is said to *destroy* (s, t)*-almost APs* if it destroys the patterns $s' \mapsto t'$ for all $s' \in [-s, s]$ and $t' \in [-t, t]$.
- By (1), it suffices to find a $(2, 2)$-almost AP-destroying permutation of $\mathbb{Z}_k$, for **any single** k.

- This basically reduces the problem to a computer search.

- This basically reduces the problem to a computer search.
- However, by considering a random permutation, one easily convinces oneself that $(2, 2)$-almost AP-destroying permutations are far too sparse to be found directly.

- This basically reduces the problem to a computer search.
- However, by considering a random permutation, one easily convinces oneself that $(2,2)$-almost AP-destroying permutations are far too sparse to be found directly.
- Instead, we break down the $(2,2)$ property into its 24 constituent patterns, along with $0 \mapsto 0$.

- This basically reduces the problem to a computer search.
- However, by considering a random permutation, one easily convinces oneself that $(2, 2)$-almost AP-destroying permutations are far too sparse to be found directly.
- Instead, we break down the $(2, 2)$ property into its 24 constituent patterns, along with $0 \mapsto 0$.
- We locate (via computer search) permutations of $\mathbb{Z}_{k_1}, \mathbb{Z}_{k_2}, \ldots, \mathbb{Z}_{k_r}$, $r \leq 24$, which destroy different subsets of these patterns, each subset including $0 \mapsto 0$.

- This basically reduces the problem to a computer search.
- However, by considering a random permutation, one easily convinces oneself that $(2,2)$-almost AP-destroying permutations are far too sparse to be found directly.
- Instead, we break down the $(2,2)$ property into its 24 constituent patterns, along with $0 \mapsto 0$.
- We locate (via computer search) permutations of $\mathbb{Z}_{k_1}, \mathbb{Z}_{k_2}, \ldots, \mathbb{Z}_{k_r}$, $r \leq 24$, which destroy different subsets of these patterns, each subset including $0 \mapsto 0$.
- If the k_i are pairwise relatively prime, then a clever application of the Chinese Remainder Theorem yields a $(2,2)$-almost AP-avoiding permutation of $\mathbb{Z}_k$, where $k = \prod_{j=1}^{r} k_j$.

- This basically reduces the problem to a computer search.
- However, by considering a random permutation, one easily convinces oneself that $(2, 2)$-almost AP-destroying permutations are far too sparse to be found directly.
- Instead, we break down the $(2, 2)$ property into its 24 constituent patterns, along with $0 \mapsto 0$.
- We locate (via computer search) permutations of $\mathbb{Z}_{k_1}, \mathbb{Z}_{k_2}, \ldots, \mathbb{Z}_{k_r}$, $r \leq 24$, which destroy different subsets of these patterns, each subset including $0 \mapsto 0$.
- If the k_i are pairwise relatively prime, then a clever application of the Chinese Remainder Theorem yields a $(2, 2)$-almost AP-avoiding permutation of $\mathbb{Z}_k$, where $k = \prod_{j=1}^{r} k_j$.
- This leads to a larger value of n_0 than stated in **R3**. However, by choosing the block decomposition carefully at the outset, it suffices to find a $(1, 2)$-almost AP-destroying permutation.

Question:

Question: Let $\mathcal{L}(x_1, \ldots, x_k) = a_0 + \sum_{i=1}^{k} a_i x_i = 0$, $a_i, \in \mathbb{Z}$, $a_i \neq 0 \; \forall \, i > 0$, be a linear equation. Is it true that the following statements are equivalent:

Question: Let $\mathcal{L}(x_1, \ldots, x_k) = a_0 + \sum_{i=1}^{k} a_i x_i = 0$, $a_i, \in \mathbb{Z}$, $a_i \neq 0 \, \forall \, i > 0$, be a linear equation. Is it true that the following statements are equivalent:

(i) There is an $n_0 = n_0(\mathcal{L})$ such that, for every $n \geq n_0$, there exists a permutation π of $\mathbb{Z}_n$ destroying all non-trivial solutions of $\mathcal{L} = 0$.

Question: Let $\mathcal{L}(x_1, \ldots, x_k) = a_0 + \sum_{i=1}^{k} a_i x_i = 0$, $a_i, \in \mathbb{Z}$, $a_i \neq 0 \; \forall \; i > 0$, be a linear equation. Is it true that the following statements are equivalent:
(i) There is an $n_0 = n_0(\mathcal{L})$ such that, for every $n \geq n_0$, there exists a permutation π of $\mathbb{Z}_n$ destroying all non-trivial solutions of $\mathcal{L} = 0$.
(ii) Either the equation $\mathcal{L} = 0$ is variant, or it is invariant and $k \in \{2, 3\}$?

Question: Let $\mathcal{L}(x_1, \ldots, x_k) = a_0 + \sum_{i=1}^{k} a_i x_i = 0$, $a_i, \in \mathbb{Z}$, $a_i \neq 0 \; \forall \, i > 0$, be a linear equation. Is it true that the following statements are equivalent:

(i) There is an $n_0 = n_0(\mathcal{L})$ such that, for every $n \geq n_0$, there exists a permutation π of $\mathbb{Z}_n$ destroying all non-trivial solutions of $\mathcal{L} = 0$.

(ii) Either the equation $\mathcal{L} = 0$ is variant, or it is invariant and $k \in \{2, 3\}$?

- A simple affine transformation will work if the equation is variant.

Question: Let $\mathcal{L}(x_1, \ldots, x_k) = a_0 + \sum_{i=1}^{k} a_i x_i = 0$, $a_i, \in \mathbb{Z}$, $a_i \neq 0 \; \forall \, i > 0$, be a linear equation. Is it true that the following statements are equivalent:
(i) There is an $n_0 = n_0(\mathcal{L})$ such that, for every $n \geq n_0$, there exists a permutation π of $\mathbb{Z}_n$ destroying all non-trivial solutions of $\mathcal{L} = 0$.
(ii) Either the equation $\mathcal{L} = 0$ is variant, or it is invariant and $k \in \{2, 3\}$?

- A simple affine transformation will work if the equation is variant.
- In [H, 2004] we proved that no permutation of any finite abelian group can destroy all non-trivial solutions to the Sidon equation $a + b - c - d = 0$. However, we do not see at this point how to modify that argument for equations in four or more variables in general.