Permutations avoiding arithmetic patterns

Peter Hegarty

Department of Mathematics
Chalmers University of Technology, Göteborg, Sweden
hegarty@math.chalmers.se

Submitted: Jun 23, 2003; Accepted: Jun 9, 2004; Published: Jun 16, 2004
MR Subject Classifications: 11B75, 20K99, 05B30

Abstract

A permutation π of an abelian group G (that is, a bijection from G to itself) will be said to avoid arithmetic progressions if there does not exist any triple (a, b, c) of elements of G, not all equal, such that $c - b = b - a$ and $\pi(c) - \pi(b) = \pi(b) - \pi(a)$. The basic question is, which abelian groups possess such a permutation? This and problems of a similar nature will be considered.

1 Notation and Introduction

Given a positive integer n, the set $\{1, ..., n\}$ will be denoted by $[n]$. If G is a group then $\Omega_n(G)$ denotes the subset (subgroup when G is abelian) consisting of all elements of G of order dividing n. The cyclic group of order n will be denoted $\mathbf{Z}_n$. The symmetric group on n letters will be denoted S_n.

In additive and combinatorial number theory, one encounters problems like the following :

Let n, k be positive integers with $k \geq 3$. How large can a subset A of $[n]$ be which does not contain any k numbers in arithmetic progression?

This well-known problem (and a closely related formulation where the set $[n]$ is replaced by the set of all natural numbers $\mathbf{N}$) has a long and distinguished history. For references covering the period up to 1995, see [**GGL**], Chapter 20. To these should be added the more recent work of Gowers [**G1**], [**G2**].

Another much-studied condition is to demand that the set A is a so-called *Sidon set*, that is, for every quadruple (a, b, c, d) of elements of A, whenever $a + b = c + d$ then either $a = c$, $b = d$ or $a = d$, $b = c$. Notice that a Sidon set avoids 3-term arithmetic progressions. Note also that the rather similar notion of a so-called *(perfect) difference set* has been extensively studied in general finite abelian (semi)groups, as these have applications to the construction of combinatorial designs (see [**CD**]).

More ambitiously still, one might demand that A has *distinct subset sums*, that is, given any two distinct subsets of A, the numbers in these two sets have different sums. Here there is the well-known conjecture of Erdős that such a subset of $[n]$ cannot have size greater than $\log_2 n + C$, where C is an absolute constant.

Erdős, among others, has also looked at multiplicative analogues of the above problems. Again, we refer the reader to [**GGL**], Chapter 20, for extensive discussion and references.

Speaking informally, one is looking here at sets of integers (or elements in an abelian (semi)group) which avoid a certain kind of 'arithmetic pattern'. Now in the field of enumerative combinatorics, the notion of 'pattern avoidance' has a much more precise meaning. Recall the basic idea -

Let $n \geq k > 0$ be integers, $\pi \in S_n$, $\sigma \in S_k$. π is said to *avoid* σ if there does not exist any k-tuple $(a_1, ..., a_k)$ of integers such that

$$1 \leq a_1 < a_2 < \cdots < a_k \leq n,$$
$$\pi(a_i) < \pi(a_j) \Leftrightarrow \sigma(i) < \sigma(j).$$

Here, then, one is looking at permutations of sets of integers which avoid a certain 'pattern', in the sense just defined. The basic problem is to count the number of such permutations, as a function of n, for a fixed pattern σ. The seminal paper in this more recent area of research is probably [**SS**].

In this paper we want to combine these two notions of 'pattern avoidance' to pose new problems. Since this obviously sounds pretty vague, in the next section we will state some precise questions which, after a brief review of the rather sparse relevant literature, will then be the object of study of the rest of the paper. We hope that the discussion above will serve as sufficient motivation, and that the reader will also be inspired to think of a multitude of similar questions which one might pose! In this spirit, the paper will include a number of conjectures and open questions which we were unable to resolve, and will be rounded off with some general suggestions for future investigations.

2 Statements of results

Henceforth, the words 'arithmetic progression' will be abbreviated to AP. We begin with a definition :

DEFINITION 2.1 : Let $k \geq 3$ be an integer, $(S, +)$ an abelian semigroup and T a subset of S. A permutation $\pi : T \rightarrow T$ is said to *avoid k-term APs* if there does not exist any

k-tuple $(a_1, ..., a_k)$ of elements of T, not all equal, such that, for $i = 1, ..., k-2$,

$$\begin{aligned} & a_i + a_{i+2} = a_{i+1} + a_{i+1}, \\ \text{and} \quad & \pi(a_i) + \pi(a_{i+2}) = \pi(a_{i+1}) + \pi(a_{i+1}). \end{aligned}$$

On the other hand if such a k-tuple exists, it will be called an *AP of length k for π*. If $k = 3$ and the permutation π satisfies the requirement of Definition 2.1, we simply say that π *avoids APs*.

The basic question we will be concerned with in this paper is : given S, T and k, does there exist a permutation of T avoiding k-term APs? When the set T is finite, one would naturally also like to 'count' the number of such permutations, but this issue will not be taken up here.

Similarly, we define

DEFINITION 2.2 : Let $(S, +)$ be a semigroup and T a subset of S. A permutation $\pi : T \rightarrow T$ is said to be a *Sidon permutation* if, whenver (a, b, c, d) is a quadruple of elements of T such that

$$\begin{aligned} & a + b = c + d, \\ \text{and} \quad & \pi(a) + \pi(b) = \pi(c) + \pi(d), \end{aligned}$$

then either $a = c$, $b = d$ or $a = d$, $b = c$.

It both these definitions, it is most natural to think of S as the set $\mathbf{N}$ of natural numbers and T as either $\mathbf{N}$ itself or the finite subset $[n]$, for some $n > 0$ (indeed, see the survey of the relevant literature below). However, most of our methods below apply in a more general setting (c.f. classical difference sets), hence the more abstract definition.

Our scanning of the literature revealed two relevant sources of known results :

1. Take $S = T = \mathbf{N}$. In [**S**], the author constructs a permutation of $\mathbf{N}$ avoiding APs. It is very simple to describe. Let σ be the following permutation of the set $\{0, 1, 2, 3\}$

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

Write every natural number n in base 4, say

$$n = \sum_{i=0}^{\lfloor log_4 n \rfloor} b_i 4^i, \quad 0 \leq b_i \leq 3.$$

Then the required permutation $\pi : \mathbf{N} \rightarrow \mathbf{N}$ is given by

$$\pi\left(\sum b_i 4^i\right) := \sum \sigma(b_i) 4^i.$$

For future reference, the thing to notice about this construction is that the map σ is, in the sense of Definition 2.1, just an AP-avoiding permutation of the group $\mathbf{Z}_4$.

2. Take $S = \mathbf{N}$, $T = [n]$ for some $n > 0$. Sidon permutations of $[n]$ have been studied. They have applications in electrical engineering and are referred to in the literature as *Costas arrays of order n*. See **[CD]**, Chapter IV.7 for a summary of the known results.

In Section 3 of this paper we shall prove

Theorem A *(i) If G is a countably infinite abelian group, then there exists a Sidon permutation of G if and only if the factor group $G/\Omega_2(G)$ is infinite.*

(ii) Let G be an infinite abelian group. Then there exists an AP-avoiding permutation of G if and only if $G/\Omega_2(G)$ has the same cardinality as G.

The key to the proof of this theorem will be an alternative construction to that in **[S]** of an AP-avoiding permutation of $\mathbf{N}$ (Theorems 3.1 and 3.3), which will then be suitably generalised to countably infinite abelian groups.

This leaves finite groups and it is perhaps not surprising that these should be most interesting. In Section 4, we shall prove the following theorem -

Theorem B *Let n be a positive integer. Then there exists a permutation of $\mathbf{Z}_n$ avoiding 4-term APs if and only if $n \neq 2, 3$*

- and provide numerical evidence for the following

Conjecture C *There exists an AP-avoiding permutation of $\mathbf{Z}_n$ if and only if $n \neq 2, 3, 5, 7$.*

Finally, in Section 5, we make some suggestions for future investigations.

We close this section with a couple of simple, preliminary observations

Proposition 2.3 *(i) For no finite abelian group G does there exist a Sidon permutation of G.*

(ii) If, in Definition 2.1, we take $S = \mathbf{N}$ and $T = [n]$ for any $n > 0$, then there exists an AP-avoiding permutation of T.

PROOF : (i) Let π be a permutation of G. Let $g \neq 0$ be any non-identity element of G and consider the map $\zeta : G \to G$ given by

$$\zeta(h) := \pi(g + h) - \pi(h), \quad \forall\, h \in G.$$

Since $g \neq 0$, if π were a Sidon permutation, then the map ζ would have to be 1-1. But then there would have to be $h \in G$ for which $\zeta(h) = 0$. Since $g \neq 0$, this would contradict the fact that π itself is 1-1.

(ii) Let $P(n)$ be the proposition that there exists an AP-avoiding permutation of $[n]$. Trivially $P(1)$ holds. We will establish that

(i) $P(n) \Rightarrow P(2n)$,
(ii) $P(n)$ and $P(n+1) \Rightarrow P(2n+1)$,

which will suffice to prove the theorem, by use of induction on n.

For (i), we use the following construction : let π_n be an AP-avoiding permutation of $[n]$. Then the permutation $\pi : [2n] \rightarrow [2n]$ given by

$$\pi(i) := \begin{cases} 2\pi_n(i), & \text{if } k \leq n, \\ 2\pi_n(i-n) - 1, & \text{if } k > n, \end{cases}$$

is easily seen to avoid APs. A similar construction establishes (ii).

3 Proof of Theorem A

In what follows k always denotes a fixed integer greater than or equal to 3.

Given any $n > 1$ for which there exists a permutation of $\mathbf{Z}_n$ avoiding k-term APs we can use it in the manner described in the previous section to construct a permutation of $\mathbf{N}$ also avoiding k-term APs. We now present an alternative method of constructing a permutation π of $\mathbf{N}$ avoiding 3-term APs. π is constructed inductively by means of the following 'greedy algorithm' :

(i) $\pi(1) := 1$,
(ii) suppose $\pi(1), ..., \pi(n-1)$ have been chosen. Then choose $\pi(n)$ to be the least positive integer t which has not already been chosen and such that, for each positive integer $i < n/2$,

$$t - \pi(n-i) \neq \pi(n-i) - \pi(n-2i).$$

The first few terms in the sequence $(\pi(n))_{n>0}$ are

$$1, 2, 4, 3, 5, 6, 8, 7, 10, 9, 13, ...$$

It needs to be proven that -

Theorem 3.1 *The map π is surjective.*

PROOF : First we prove that, for each $n > 0$,

$$\pi(n) < 3n/2. \tag{1}$$

The procedure for choosing $\pi(n)$ implies that, for each positive integer $m < \pi(n)$ either

(A) $m \in \{\pi(i) : 1 \leq i < n\}$,

or

(B) there exists a positive integer $s \leq \frac{n-1}{2}$ such that

$$m - \pi(n-s) = \pi(n-s) - \pi(n-2s). \tag{2}$$

Since there are exactly $n-1$ numbers m satisfying (A) and at most $\frac{n-1}{2}$ numbers satisfying (B), this establishes (1).

Fix $n > 0$. We now verify that π is surjective by showing that n appears among the elements of the set $X := \{\pi(i) : 1 \leq i \leq 4n\}$. Let X_0 denote the subset of X consisting of those elements which are larger than n. Evidently, $|X_0| \geq 3n+1$. Let $x \in X_0$, say $x = \pi(i_x)$. Since the greedy algorithm did not choose n instead of x, there must be a positive integer $s < i_x/2$ such that

$$n - \pi(i_x - s) = \pi(i_x - s) - \pi(i_x - 2s). \tag{3}$$

Define a map $\tau : X_0 \to \mathbf{N}$ by $\tau(x) := \pi(i_x - 2s)$, where $s > 0$ is the smallest integer for which (3) holds.

The map τ is 1-1 and every element of $\tau(X_0)$ is a positive integer differing from n by an even integer. Since $|X_0| > 3n$, it follows that there exists $x \in X_0$ for which $\tau(x) > 6n$. But this means that there is a positive integer i such that $i \leq 4n$ and $\pi(i) > 6n$. This contradicts (1), and so completes the proof of Theorem 3.1.

The permutation of $\mathbf{N}$ just described will be denoted π_g (g for 'greedy'). The last proof implies that, for all $n > 0$,

$$\frac{1}{4} \leq \frac{\pi_g(n)}{n} < \frac{3}{2}. \tag{4}$$

Conjecture 3.2

$$\lim_{n \to \infty} \frac{\pi_g(n)}{n} = 1.$$

We have no idea how one might prove this - our only real evidence is numerical. The interested reader will find a computer plot of the function $\pi_g(n)/n$, for all $n \leq 560,000$, at http://www.mdstud.chalmers.se/ ~md0larur/HTMLFiles/greedyplot_2.gif.

The best improvement on (4) which we have managed is

Theorem 3.3 *For all $n > 0$ we have*

$$\frac{\pi_g(n)}{n} \geq \frac{3}{8}.$$

PROOF : The basic idea is the same as in the second half of the proof of Theorem 3.1, but with a more careful (and more technical!) analysis.

Fix $n > 0$ and suppose n does not appear among the first $\lfloor 8n/3 \rfloor$ positions $\pi(i)$, $1 \leq i \leq \lfloor 8n/3 \rfloor$. We will derive a contradiction from this.

Let l be the number of these positions containing numbers bigger than n. At the very least, we have

$$l > 5n/3. \tag{5}$$

We can then find l pairs of positions (a_i, b_i) such that

$$2y_i - z_i = n, \tag{6}$$

where

$$y_i = \pi(a_i), \qquad z_i = \pi(b_i).$$

All of the z_i $(i = 1, ..., l)$ are distinct, as are all of the y_i. Let

$$\begin{aligned} Y &:= \{y_i : i = 1, ..., l\}, \\ Z &:= \{z_i : i = 1, ..., l\}, \\ t &:= |Y \cap Z|. \end{aligned}$$

We claim that

$$t > 11n/12. \tag{7}$$

To see this consider the relation

$$|Y \cap Z| = |Y| + |Z| - |Y \cup Z|.$$

On the one hand, $|Y| = |Z| = l > 5n/3$. On the other hand, all the numbers in $Y \cup Z$ appear among the first $\lfloor 8n/3 \rfloor$ positions. However, by (6), none of them can be a number $\leq n/2$ of the same parity as n. The number of such numbers is at least $\lfloor n/4 \rfloor$ and, by Theorem 3.1, all of them appear among the first $\lfloor 8n/3 \rfloor$ positions. Hence,

$$|Y \cup Z| \leq \lfloor 8n/3 \rfloor - \lfloor n/4 \rfloor,$$

from which we can deduce (7). Rearranging indices if necessary, we may assume that

$$Y \cap Z = \{y_1, ..., y_t\}.$$

Then each of the numbers z_i, $i = 1, ..., t$, differs from n by a multiple of 4. By (7), there is thus at least one index j such that

$$z_j > 11n/3.$$

Now consider the following : by (6), every number in the set Z has the same parity as n. Hence by (5), there are strictly less than n among the first $\lfloor 8n/3 \rfloor$ positions which contain a number of opposite parity to n. Call the set of numbers in these positions B. Let

$$C := \{c \in \mathbf{N} : c \leq 11n/3 \text{ and } c \not\equiv n \pmod 2\},$$
$$C_1 := C \backslash B.$$

Then

$$s := |C_1| > 5n/6. \tag{8}$$

Consider the position $b_j = \pi^{-1}(z_j)$. None of the numbers $c_i \in C_1$, $i = 1, ..., s$, was chosen for the position b_j. Thus there must be a collection of s pairs (α_i, β_i) of positions such that

$$2u_i - v_i = c_i,$$

where

$$u_i = \pi(\alpha_i), \quad v_i = \pi(\beta_i), \quad i = 1, ..., s.$$

The important point is that : firstly, each v_i has the same parity as the corresponding c_i, and hence the opposite parity to n, that is,

$$\{v_1, ..., v_s\} \subseteq B, \tag{9}$$

and secondly, that each β_i has the same parity as b_j, i.e.:

$$\beta_i \equiv b_j \pmod 2, \quad i = 1, ..., s. \tag{10}$$

By (8) and (9) there are strictly less than $n/6$ elements in B other than the v_i. By an argument similar to the one just presented (note (10)), this implies that, for any position ϵ such that $\pi(\epsilon) > 7n/3$, we have

$$\epsilon \equiv b_j \pmod 2. \tag{11}$$

But how many such positions are there? Let's look at the set Z again. We have $|Z| > 5n/3$. But each member of Z has the same parity as n. Hence there are strictly more than $n/2$ elements in Z which are greater than $7n/3$.

Let's summarise our findings! Put

$$\Phi := \{\pi^{-1}(z_j) : z_j \in Z \text{ and } z_j > 7n/3\},$$
$$\Psi := \{\beta_1, ..., \beta_s\}.$$

The sets Φ and Ψ are disjoint subsets of $\{1, ..., \lfloor 8n/3 \rfloor\}$ such that

$$|\Phi| > n/2, \qquad |\Psi| > 5n/6. \tag{12}$$

But, by (10) and (11), all the elements of $\Phi \cup \Psi$ have the same parity, which forces

$$|\Phi \cup \Psi| \leq \frac{1}{2}\left\lfloor \frac{8n}{3} \right\rfloor + \frac{1}{2}. \tag{13}$$

Relations (12) and (13) contradict one another, which completes the proof of Theorem 3.3.

We turn next to the proof of Theorem A(i). We adopt the following terminology : if (a, b, c, d) is an ordered quadruple of elements of the abelian group G such that $a+b = c+d$ but neither $a = c$, $b = d$ nor $a = d$, $b = c$ holds, we refer to it as a *Sidon quadruple*.

First note that the condition that $G/\Omega_2(G)$ be infinite is obviously necessary. Since if a, b are any two distinct elements of order 2 in G then the quadruple (a, a, b, b) is Sidon, so if the permutation π is Sidon then $\pi(a)$, $\pi(b)$ have to lie in different cosets of $\Omega_2(G)$.

So let G be an infinite abelian group with $G/\Omega_2(G)$ infinite. The idea for constructing a Sidon permutation of G is to apply a greedy algorithm to a suitable well-ordering of the elements of G. More precsiely, let $(x_n)_{n=1}^{\infty}$ be a well-ordering of the elements of G. Then an injective mapping $\pi_g : G \rightarrow G$ can be described inductively as follows :

(i) $\pi_g(x_1) := x_1$,
(ii) suppose $\pi_g(x_1), ..., \pi_g(x_{n-1})$ have been chosen. Then choose $\pi_g(x_n)$ to be x_t where t is the least positive integer such that x_t has not already been chosen and such that, whenever (a, b, c, d) is a quadruple of positive integers such that

- not all of a, b, c, d are equal,
- all of a, b, c, d are less than or equal to n, and at least one of them equals n,
- the quadruple (x_a, x_b, x_c, x_d) is Sidon in G,

then the quadruple (y_a, y_b, y_c, y_d) is not Sidon in G, where $y_a = \pi_g(x_a)$ if $a < n$ and $y_n = x_t$.

The trick is to choose the well-ordering so that the map π_g is surjective. We need a lemma

Lemma 3.4 *Let S be any countably infinite semigroup. Let $(s_n)_{n=1}^{\infty}$ be a well-ordering of the elements of S. For each $N > 0$, let A_N denote the number of Sidon quadruples among $s_1, ..., s_N$ and suppose that there exists $\epsilon > 0$ such that*

$$A_N < (1-\epsilon)N, \quad \textit{for all } N >> 0. \tag{14}$$

Then the mapping $\pi_g : S \rightarrow S$ described by the greedy algorithm is surjective..

Remark : Note that (14) is not satisfied by the usual well-ordering of $\mathbf{N}$. See Remark 3.7 below.

Proof of Lemma : Fix $n > 0$. We'll show that s_n is in the image of π_g. Let N_0

be an integer sufficiently large so that $N_0 - n > (1-\epsilon)N_0$ and (14) holds for $N = N_0$. If s_n does not appear among $\{\pi_g(i)\}_{i=1}^{N_0}$ then there are more than $N_0 - n$ indices $i \leq N_0$ such that s_n was tested for $\pi(s_i)$ but rejected each time. Each rejection implies the existence of a Sidon quadruple among $s_1, ..., s_{N_0}$ (it implies more of course, but we don't need that). But by the choice of N_0, this contradicts (14) and the lemma is proven.

So given the group G, we need to well-order its elements so that (14) holds. In fact, we can always find a well-ordering such that $A_N = o(N)$. Henceforth, we shall assume the reader is familiar with the theory of infinite abelian groups as presented in [**K**], for example.

Proof of Theorem A(i) : Let G be a countably infinite abelian group such that $G/\Omega_2(G)$ is infinite. By Kulikov's Theorem, at least one of the following three things must hold :

(i) G contains an element of infinite order,
(ii) G has a direct summand isomorphic to C_{p^∞} for some prime p,
(iii) G contains an infinite sequence $a_1, a_2, ...$ of elements, each of order 4 or an odd prime, such that for any n, the subgroup of G generated by $a_1, ..., a_n$ is the direct sum of the cyclic groups $< a_i >$, $i = 1, ..., n$.

Depending on which property holds, we define a subsequence $(z_n)_1^\infty$ of elements of G as follows : If (i) holds, let g be any element of infinite order and set $z_n = 2^n g$. If (ii) holds, choose any quasicyclic p-subgroup A of G and let z_n be any element of order p^n in A. If (iii) holds, put $z_n = a_n$.

Let $(y_n)_1^\infty$ be any well-ordering of the elements of $G \backslash \{z_n\}$ and now let $(x_n)_1^\infty$ be the well-ordering of all elements of G given by the following :

If n is a 2-power, say $n = 2^t$, set $x_n := y_t$. Otherwise, if $2^{t-1} < n < 2^t$, set $x_n := z_{n-t}$.

It is easy to check that, in the notation of (14), $A_N = o(N)$. Hence, by Lemma 3.4, the proof of Theorem A(i) is complete.

We now turn to part (ii) of the theorem. We shall use the result of part (i), together with the following lemma -

Lemma 3.5 *Let G be an abelian group and H a subgroup. Suppose there exist k-term AP-avoiding permutations π_1, π_2 of H and G/H respectively. Then there also exists a k-term AP-avoiding permutation π of G. Moreover, π can be chosen so that $\pi(H) = H$ and $\pi|_H = \pi_1$.*

Proof : Choose a set of representatives $\{g_\lambda\}_{\lambda \in \Lambda}$ for the cosets of G/H with $g_0 = 0$

representing the identity coset H. Then π_2 can be identified with a permutation $\tilde{\pi_2}$ of the set $\{g_\lambda\}$. The map $\pi : G \to G$ given by

$$\pi(h + g_\lambda) := \pi_1(h) + \tilde{\pi_2}(g_\lambda), \qquad \forall\, h \in H,\ \forall\, \lambda \in \Lambda,$$

is easily checked to be a k-term AP-avoiding permutation of G. Since any translation of a k-term AP-avoiding permutation is also such, we may choose π_2 so that $\tilde{\pi_2}(g_0) = g_0 = 0$. And then the permutation π has the property that $\pi(H) = H$ and $\pi|_H = \pi_1$.

Proof of Theorem A(ii) : By the same argument as in the proof of part (i), the condition that $G/\Omega_2(G)$ have the same cardinality as G is obviously necessary. So let G be a group satisfying this condition, which we henceforth denote by (*). Informally, the idea of the proof is to show that G can be built up in countable pieces, each satisfying (*), so that we may exploit Theorem A(i) and Lemma 3.5.

Case 1 : G is torsion-free.

Let $\leq$ be any well-ordering of the elements of G. Let Φ be the ordinal of this well-ordering (so the elements of G are listed as x_α for every ordinal $\alpha < \Phi$). For each $\alpha < \Phi$ let S_α be the pure subgroup of G generated by the elements $x_\beta : \beta \leq \alpha$. We shall prove, using transfinite induction, that there exists, for each ordinal $\alpha < \Phi$, an AP-avoiding permutation π_α of S_α such that, for all $\beta < \alpha$, π_α extends π_β. Denote this property of the ordinal α by $P(\alpha)$.

If α is a successor ordinal, then either $S_\alpha = S_{\alpha-1}$, in which case we put $\pi_\alpha := \pi_{\alpha-1}$ or $S_\alpha/S_{\alpha-1}$ is a torsion-free group of rank 1. In particular, such a group is countable, hence has an AP-avoiding permutation by Theorem A(i). Hence, by Lemma 3.5, there exists an AP-avoiding permutation π_α of S_α extending $\pi_{\alpha-1}$.

If α is a limit ordinal, then π_α is well-defined by setting

$$\pi_\alpha|_{S_\beta} := \pi_\beta, \quad \text{for all } \beta < \alpha.$$

By transfinite induction, this completes the proof in Case 1.

Case 2 : G is a torsion group.

Then G is the direct sum of its p-primary components, for different primes p. Using Theorem A(i) and Lemma 3.5, it is easily seen that we can reduce the proof to one of the following two subcases :

(a) G is an uncountable 2-group,

(b) $G = P \oplus Q \oplus X$, where X is a finite group, P and Q are uncountable of the same cardinality, Q is a 2-group such that $Q/\Omega_2(Q)$ has smaller cardinality than Q, and P is a p-group for some odd prime p.

Suppose (a) holds. For each $n \geq 0$ let $G_n := \Omega_{2^n}(G)$. Since G is uncountable, that

G/G_1 has the same cardinality as G is equivalent to G_1 and G_2/G_1 having the same cardinality. Hence

$$G_2 = (\oplus_{\lambda \in \Lambda} A_\lambda) \bigoplus (\oplus_{\phi \in \Phi} B_\phi),$$

where each $A_\lambda \cong \mathbf{Z}_4$, each $B_\phi \cong \mathbf{Z}_2$, and $\mathrm{card}(\Lambda) \geq \mathrm{card}(\Phi)$. But this means that G_2 can be written as as a direct sum $\oplus C_\mu$ where each C_μ is a countably infinite group of exponent 4 satisfying (*). By Theorem A(i) and Lemma 3.5, we conclude that there exists an AP-avoiding permutation of G_2. By extending this argument, one sees that if G has finite exponent, then there exists an AP-avoiding permutation of G.

So we may assume that G has infinite exponent. We have a direct decomposition

$$G_4 = A \oplus B,$$

where A is homocyclic of exponent 16 and B has exponent 8. Let

$$H = \Omega_4(A) \oplus B.$$

Then H satisfies (*) and H has finite exponent, so there exists an AP-avoiding permutation of H. Let $K := G/H$. By construction, K satisfies (*). If K is countable, we're done. Otherwise, we start all over again with K. If we iterate this procedure then the worst that can happen is that we produce an infinite sequence of subgroups of G,

$$0 = H_0 \subset H_1 \subset H_2 \subset \cdots$$

such that $G = \cup H_n$ and each quotient H_n/H_{n-1} possesses an AP-avoiding permutation. By Lemma 3.5, we can still conclude that G possesses such a permutation also, and this completes Case 2(a).

Now suppose (b) holds. Let

$$H := \Omega_p(P) \oplus Q \oplus X.$$

There is no loss of generality in assuming that $G/H := K$ is an infinite group. By Lemma 3.5, it suffices to construct AP-avoiding permutations of H and K.

First we consider H. Since P is uncountable, so also is $\Omega_p(P)$, and we can write a direct decomposition,

$$\Omega_p(P) = \oplus_{n=1}^\infty P_n,$$

where each P_n has the same cardinality as P. We define an increasing chain of subgroups $(H_n)_0^\infty$ of H as follows :

$$\begin{aligned} H_0 &:= \{0\}, \\ H_1 &:= \Omega_2(Q) \oplus P_1 \oplus X, \\ \forall\, n \geq 2, \quad H_n &:= \Omega_{2^n}(Q) \bigoplus (\oplus_{i=1}^n P_i) \oplus X. \end{aligned}$$

Since G is the union of the H_n, it suffices by Lemma 3.5 to find an AP-avoiding permutation of each quotient H_n/H_{n-1}. But it is clear that, since G satisfies (*), each such quotient can be decomposed as a direct sum of countable groups satisfying (*). Hence a further application of Lemma 3.5 and Theorem A(i) gives us what we need.

Similarly, consider K. If it is countable, we're done. Otherwise, we can at least decompose $K_1 := \Omega_p(K)$ as a direct sum of countably infinite groups and construct an AP-avoiding permutation of this subgroup in the usual way. We then consider K/K_1 and, by iterating this procedure, prove the existence of an AP-avoiding permutation of K.

This completes the proof in Case 2.

Case 3 : G is a mixed group.

Let T be the torsion subgroup of G and let $F = G/T$. By Lemma 3.5, it suffices for both T and F to possess AP-avoiding permutations. By Cases 1 and 2, we'd be done if T satisfied (*). Hence, we may assume it does not. But since G does so, this implies at the very least that $\text{card}(T) \leq \text{card}(F)$. The argument now is only a slight modification of the one used in Case 1, so we only outline it. Let $(S_\alpha)_{\alpha \in \Phi}$ be a (transfinite) chain of pure subgroups of F, as described in Case 1, whose union is F. By Zorn's Lemma, we can pick a maximal subchain consisting of pairwise disjoint groups, which we can also denote by $(S_\alpha)_{\alpha \in \Phi}$. Let $(t_\lambda)_{\lambda \in \Lambda}$ be any well-ordering of the elements of T, where $\Lambda \leq \Phi$, since $\text{card}(T) \leq \text{card}\ (F)$. We then consider the chain $(H_\alpha)_{\alpha \in \Phi}$ of subgroups of G, where H_α is the subgroup generated by $\{t_\lambda : \lambda < \alpha\}$ and any chosen set of representatives for the cosets of T in S_α. For every successor ordinal α, the quotient $H_\alpha/H_{\alpha-1}$ will be a countable non-torsion group, hence possess an AP-avoiding permutation, by Theorem A(i). The proof of Theorem A(ii) is then completed by transfinite induction.

Remark 3.6 The proof of Lemma 3.5 will not work if we instead consider Sidon permutations. Hence the question remains whether the condition (*) is sufficient for an uncountable abelian group to possess a Sidon permutation.

Remark 3.7 Though $\mathbf{N}$ is not a group and hence not covered by Theorem A(i), it should be clear from its' proof how one can find a well-ordering of $\mathbf{N}$ such that (14) is satisfied. Hence, there exists a Sidon permutation of $\mathbf{N}$. However, If we adopt the usual well-ordering of $\mathbf{N}$ and apply the greedy algorithm as on p.9, we don't know whether it is the resulting 'Sidon mapping' π_g is surjective. Compare this with Theorem 3.1.

4 Permutations of finite abelian groups

The first purpose of this section is to prove Theorem B.

Proof of Theorem B : One readily checks that there is no permutation of either $\mathbf{Z}_2$ or $\mathbf{Z}_3$ avoiding 4-term APs. Lemma 3.5 thus reduces the proof of Theorem B to finding 4-term AP-avoiding prmutations of $\mathbf{Z}_n$, where n is of the from $p, 2p$ or $3p$, for some odd prime $p > 3$, or one of the numbers $2^2 = 4$, $2 \cdot 3 = 6$, $3^2 = 9$, $2^2 \cdot 3 = 12$ and $2 \cdot 3^2 = 18$.

For each of these last five values of n, there in fact exists a 3-term AP-avoiding permutation of $\mathbf{Z}_n$, as is seen from the table on p.19. For $n = p > 3$, we identify $\mathbf{Z}_p$ with the set $[p]$, addition being modulo p. Then one readily checks that the map π_p given by

$$\begin{aligned} \pi_p(x) \cdot x \equiv 1 \pmod{p}, \quad \text{if } x \neq p, \\ \pi_p(p) := p, \end{aligned} \tag{15}$$

is a permutation of $\mathbf{Z}_p$ avoiding 4-term APs.

For $n = 2p$ or $3p$ one uses a similar construction, but the verification that 4-term APs are avoided requires more care. We now present the construction in detail for the case $n = 2p$, and then briefly indicate what one does for $n = 3p$, leaving it to the reader to fill in the blanks.

Let $p > 3$ be a prime. Let π_p denote the permutation of $[p]$ given by (15).

First suppose $p \equiv 2 \pmod{3}$. The map π defined by

$$\begin{aligned} \pi(2t-1) = \pi_p(t), \quad 1 \leq t \leq p, \\ \pi(2t) = \pi_p(t) + p, \quad 1 \leq t \leq p, \end{aligned}$$

will be shown to avoid APs of length 4. Denote

$$\begin{aligned} L := \{1, ..., p\}, \\ H := \{p+1, ..., 2p\}. \end{aligned}$$

Suppose (a, b, c, d) is an AP of length 4 for π - we shall obtain a contradiction. If each of $\pi(a), \pi(b), \pi(c), \pi(d) \in L$, then $(\frac{a+1}{2}, \frac{b+1}{2}, \frac{c+1}{2}, \frac{d+1}{2})$ would be an AP of length 4 for π_p, a contradiction. Similarly, we can't have $\pi(a), \pi(b), \pi(c), \pi(d) \in H$.

Hence, there is no loss of generality in assuming that $\pi(a), \pi(c) \in L$ and $\pi(b), \pi(d) \in H$. Henceforth in this proof, unless otherwise stated, all congruences are modulo p. Let $x, s \in [p]$ be such that $\frac{a+1}{2} \equiv x$ and $\frac{b}{2} \equiv x + s$. Then $\frac{c+1}{2} \equiv x + 2s + 1$ and $\frac{d}{2} \equiv x + 3s + 1$, so that

$$\begin{aligned} \pi(a) \equiv \pi_p(x), \quad \pi(b) \equiv \pi_p(x+s), \\ \pi(c) \equiv \pi_p(x+2s+1), \quad \pi(d) \equiv \pi_p(x+3s+1). \end{aligned} \tag{16}$$

We now divide the analysis into two cases.

Case I : None of $\pi(a), \pi(b), \pi(c), \pi(d)$ is congruent to zero modulo p. Then

$$\pi(a) \equiv \frac{1}{x}, \quad \pi(b) \equiv \frac{1}{x+s}, \quad \pi(c) \equiv \frac{1}{x+2s+1}, \quad \pi(d) \equiv \frac{1}{x+3s+1}. \tag{17}$$

The condition of being an AP of length 4 for π implies, in particular, that

$$\begin{aligned} \frac{2}{x+s} &\equiv \frac{1}{x} + \frac{1}{x+2s+1} \\ \Rightarrow 2x(x+2s+1) &\equiv (x+s)(2x+2s+1) \qquad (18) \\ \text{and} \qquad \frac{2}{x+2s+1} &\equiv \frac{1}{x+s} + \frac{1}{x+3s+1} \\ \Rightarrow 2(x+s)(x+3s+1) &\equiv (x+2s+1)(2x+4s+1). \qquad (19) \end{aligned}$$

The hypothesis of CASE I implies that neither side of (18) is congruent to zero modulo p. Hence, we may divide (19) by (18) to get

$$\frac{2(x+3s+1)}{2x+2s+1} \equiv \frac{2x+4s+1}{2x}.$$

Cross-multiplying and expanding then leads to the one-variable congruence

$$8s^2 + 6s + 1 \equiv 0,$$

which has the two solutions $s \equiv -\frac{1}{4}$ and $s \equiv -\frac{1}{2}$.

Say $s \equiv -\frac{1}{2}$. Substituting into (18) leads to

$$2x^2 \equiv 2x\left(x - \frac{1}{2}\right),$$

and hence either $x \equiv 0$, contradicting the hypotheses of CASE I, or $x \equiv x - \frac{1}{2}$, which is ridiculous.

So $s \equiv -\frac{1}{4}$. Substituting into (18) and solving for x yields $x \equiv -\frac{1}{8}$. Substituting back into (17) we get

$$\pi(a) \equiv -8, \quad \pi(b) \equiv -\frac{8}{3}, \quad \pi(c) \equiv \frac{8}{3}, \quad \pi(d) \equiv 8. \qquad (20)$$

Note that these four numbers do indeed form an AP in $\mathbf{F}_p$. For an element g of the finite field $\mathbf{F}_p$, we now denote by $r(g)$ the unique integer in $[p]$ which represents g under the natural identification of $\mathbf{F}_p$ with $[p]$.

Now, since $\pi(a), \pi(c) \in L$ and $\pi(b), \pi(d) \in H$, we deduce from (20) that, as ordinary integers,

$$\begin{aligned} \pi(a) = p - r(8), \quad \pi(b) = 2p - r\left(\frac{8}{3}\right), \\ \pi(c) = r\left(\frac{8}{3}\right), \quad \pi(d) = p + r(8). \qquad (21) \end{aligned}$$

We have still to show that these four numbers do not form an AP modulo $2p$. It's now that we finally make use of the assumption that $p \equiv 2 \pmod 3$. If $p = 5$, then we can read off from the table on p.19 a permutation of $[10]$ avoiding APs. So we may assume $p > 5$, in which case $r(8) = 8$. Let $p = 3t+2$. Then $r(\frac{1}{3}) = t+1$, from which one calculates that $r(\frac{8}{3}) = 2t+4$. Substituing into (21) we have

$$\pi(a) = 3t - 6, \quad \pi(b) = 4t, \quad \pi(c) = 2t + 4, \quad \pi(d) = 3t + 10. \tag{22}$$

But then, modulo $2p$ at last,

$$\pi(b) - \pi(a) = t + 6 \not\equiv 4 - 2t = \pi(c) - \pi(b),$$

so we don't after all have an AP of length 4 modulo $2p$. This deals with Case I.

Case II : At least one of $x, x+s, x+2s+1, x+3s+1$ is congruent to zero modulo p.

If at least two of them were $\equiv 0$ then, since $3 \not\equiv 0$, all four would have to be so for $(\pi(a), \pi(b), \pi(c), \pi(d))$ to form an AP (modulo p). But this is plainly ridiculous. Hence exactly one of the four is $\equiv 0$.

Say $x \equiv 0$. Then

$$\pi(a) \equiv 0, \quad \pi(b) \equiv \frac{1}{s}, \quad \pi(c) \equiv \frac{1}{2s+1}, \quad \pi(d) \equiv \frac{1}{3s+1}.$$

The analogues of (18) and (19) are, respectively,

$$\frac{1}{2s+1} \equiv \frac{2}{s}, \tag{23}$$

$$\frac{1}{3s+1} + \frac{1}{s} \equiv \frac{2}{2s+1}. \tag{24}$$

Solving (23) gives $s \equiv -\frac{2}{3}$ which, substituted into (24) yields $7 \equiv 0$; that is, $p = 7$, which contradicts the assumption that $p \equiv 2 \pmod 3$.

Next, say $x + s \equiv 0$. Then

$$\pi(a) \equiv -\frac{1}{s}, \quad \pi(b) \equiv 0, \quad \pi(c) \equiv \frac{1}{s+1}, \quad \pi(d) \equiv \frac{1}{2s+1}.$$

The analogues of (18) and (19) are now, respectively,

$$\frac{1}{s+1} \equiv \frac{1}{s}, \tag{25}$$

$$\frac{1}{2s+1} \equiv \frac{2}{s+1}. \tag{26}$$

We simply need to note that (25) is unsatisfiable.

Finally, assuming $x + 2s + 1 \equiv 0$ leads to the same two equations as (25) and (26), whereas assuming $x+3s+1 \equiv 0$ leads to the same two equations as (23) and (24). Hence, Case II is fully dealt with, and with it the case $p \equiv 2 \pmod 3$.

To deal with the case when $p \equiv 1 \pmod 3$, we just have to adjust the permutation π slightly. In this case we take

$$\begin{aligned}\pi(2t-1) &= r\left(\frac{1}{2}\pi_p(t)\right), \quad 1 \le t \le p, \\ \pi(2t) &= r\left(\frac{1}{2}\pi_p(t)\right) + p, \quad 1 \le t \le p.\end{aligned} \tag{27}$$

The analysis is similar to before so we omit most of the details. In Case II, the prime $p = 7$ arises as an exception in the same way as before, and we refer to p.19 for an explicit AP-avoiding permutation of [14]. In Case I, the analogue of (21) is

$$\begin{aligned}\pi(a) = p - r(4), \quad \pi(b) = 2p - r\left(\frac{4}{3}\right), \\ \pi(c) = r\left(\frac{4}{3}\right), \quad \pi(d) = p + r(4).\end{aligned} \tag{28}$$

We then use the fact that $p \equiv 1 \pmod 3$. Putting $p = 3t+1$, we have $r(\frac{1}{3}) = 2t+1 \Rightarrow r(\frac{4}{3}) = 2t+2$ and hence

$$\pi(a) = 3t-3, \quad \pi(b) = 4t, \quad \pi(c) = 2t+2, \quad \pi(d) = 3t+5.$$

Finally, working modulo $2p$,

$$\pi(b) - \pi(a) = t + 3 \not\equiv 2 - 2t = \pi(c) - \pi(b).$$

This contradiction completes the analysis of the case $n = 2p$.

When $n = 3p$, the map $\pi : [3p] \to [3p]$ given by

$$\begin{aligned}\pi(3t-2) &= \pi_p(t), \quad 1 \le t \le p, \\ \pi(3t-1) &= \pi_p(t) + p, \quad 1 \le t \le p, \\ \pi(3t) &= \pi_p(t) + 2p, \quad 1 \le t \le p.\end{aligned}$$

can be checked to avoid APs of length 4, when $p \equiv 2 \pmod 3$. The prime $p = 5$ arises as a special case, and then an AP-avoiding permutation of [15] can be read off from the table on p.19. When $p \equiv 1 \pmod 3$, we adjust π as in (27). For the special case $p = 7$, we may again refer to p.19 for an explicit AP-avoiding permutation of [21].

This completes the proof of Theorem B.

We now turn to Conjecture C. One may verify by hand that there is no AP-avoiding permutation of $\mathbf{Z}_n$ for $n = 2, 3, 5, 7$. On the other hand, Lemma 3.5 reduces the proof of the conjecture to the construction of AP-avoiding permutations of $\mathbf{Z}_n$, for $n = p, 2p, 3p, 5p$

or $7p$, where $p > 7$ is a prime, together with a finite number of integers involving only the primes $2, 3, 5, 7$, namely :

4,6,8,9,10,12,14,15,18,20,21,25,27,28,30,35,42,45,49,50,63,70,75,98,125,147, 175,245.

Beyond this however, we know nothing. Our evidence for the conjecture is purely numerical. The table on p.19-20 summarises our computations for all $n \leq 32$. The table is divided into three parts :

The first part applies to $n < 14$. For each $n \neq 2, 3, 5, 7$, the example given is the minimal AP-avoiding permutation with respect to the lexicographic ordering of S_n inherited from the usual ordering of the positive integers. For this range of n, we have found all AP-avoiding permutations of $\mathbf{Z}_n$, and their number is denoted by C_n. Notice that these numbers are 'large'. Otherwise, except for Remark 4.1 below, they are quite mysterious to us.

The second part applies to the range $14 \leq n \leq 22$. The examples are still the lexicographically minimal AP-avoiding permutations.

The third part applies to $n > 22$. To reduce computing times, we searched at this point randomly for AP-avoiding permutations, except for $n = 24, 32$ where we used Lemma 3.5.

n	C_n	$\frac{C_n}{n!}$	Example
1	1	1	(1)
2	0	0	
3	0	0	
4	$16 = 2^4$	$\frac{2}{3} \approx 0.667$	$(1, 3, 2, 4)$
5	0	0	
6	$72 = 2^3 \cdot 3^2$	$\frac{1}{2\cdot 5} = 0.1$	$(1, 2, 4, 3, 6, 5)$
7	0	0	
8	$768 = 2^8 \cdot 3$	$\frac{2}{3\cdot 5\cdot 7} \approx 0.0190$	$(1, 2, 4, 8, 6, 5, 3, 7)$
9	$11664 = 2^4 \cdot 3^6$	$\frac{3^2}{2^3\cdot 5\cdot 7} \approx 0.0321$	$(1, 2, 4, 3, 5, 8, 9, 6, 7)$
10	$15200 = 2^5 \cdot 5^2 \cdot 19$	$\frac{19}{2^3\cdot 3^4\cdot 7} \approx 0.0042$	$(1, 2, 4, 3, 5, 9, 8, 10, 6, 7)$
11	$258940 = 2^2 \cdot 5 \cdot 11^2 \cdot 107$	$\frac{11\cdot 107}{2^6\cdot 3^4\cdot 5\cdot 7} \approx 0.0065$	$(1, 2, 4, 3, 5, 8, 9, 11, 6, 7, 10)$
12	$1,217,664$ $= 2^7 \cdot 3^2 \cdot 7 \cdot 151$	$\frac{151}{2^3\cdot 3^3\cdot 5^2\cdot 11}$ ≈ 0.0025	$(1, 2, 4, 3, 5, 6, 8, 11, 12, 7, 9, 10)$
13	$8,927,412$ $= 2^2 \cdot 3 \cdot 13 \cdot 89 \cdot 643$	$\frac{89\cdot 643}{2^8\cdot 3^4\cdot 5^2\cdot 7\cdot 11}$ ≈ 0.0014	$(1, 2, 4, 3, 5, 6, 8, 11, 7, 12, 13, 9, 10)$

n	Example
14	$(1, 2, 4, 3, 5, 6, 8, 7, 12, 14, 13, 10, 9, 11)$
15	$(1, 2, 4, 3, 5, 6, 8, 7, 12, 14, 13, 15, 9, 11, 10)$
16	$(1, 2, 4, 3, 5, 6, 8, 7, 12, 14, 13, 15, 16, 10, 9, 11)$
17	$(1, 2, 4, 3, 5, 6, 8, 7, 10, 12, 15, 13, 17, 16, 9, 14, 11)$
18	$(1, 2, 4, 3, 5, 6, 8, 7, 10, 9, 13, 16, 14, 18, 17, 11, 12, 15)$
19	$(1, 2, 4, 3, 5, 6, 8, 7, 10, 9, 13, 12, 18, 11, 17, 19, 15, 14, 16)$
20	$(1, 2, 4, 3, 5, 6, 8, 7, 10, 9, 13, 16, 17, 20, 19, 14, 11, 15, 12, 18)$
21	$(1, 2, 4, 3, 5, 6, 8, 7, 10, 9, 13, 15, 20, 18, 19, 14, 11, 21, 12, 16, 17)$
22	$(1, 2, 4, 3, 5, 6, 8, 7, 10, 9, 13, 15, 12, 16, 19, 21, 20, 22, 14, 11, 17, 18)$

n	Example
23	$(14, 10, 16, 12, 4, 3, 9, 13, 19, 20, 8, 23, 7, 2, 17, 18, 11, 22, 15, 5, 21, 6, 1)$
24	$(1, 2, 4, 3, 6, 5, 13, 14, 16, 15, 18, 17, 7, 8, 10, 9, 12, 11, 19, 20, 22, 21, 24, 23)$
25	$(4, 24, 8, 2, 10, 23, 7, 13, 12, 18, 15, 6, 16, 5, 11, 22, 14, 9, 21, 25, 17, 3, 20, 1, 19)$
26	$(23, 9, 24, 19, 17, 13, 18, 5, 26, 11, 10, 25, 7, 20, 1, 2, 16, 12, 6, 8, 14, 22, 21, 4, 3, 15)$
27	$(25, 16, 19, 12, 11, 18, 7, 9, 8, 5, 23, 4, 1, 24, 21, 10, 3, 15, 20, 27,$ $6, 14, 13, 22, 26, 17, 2)$
28	$(8, 1, 13, 14, 5, 28, 4, 19, 20, 12, 10, 9, 6, 16, 18, 24, 23, 3, 22, 26, 25,$ $15, 17, 7, 2, 11, 21, 27)$
29	$(5, 21, 12, 28, 16, 1, 26, 2, 23, 7, 18, 17, 6, 4, 20, 11, 13, 14, 3, 19,$ $15, 22, 10, 29, 8, 27, 25, 24, 9)$
30	$(29, 8, 20, 21, 3, 11, 10, 7, 26, 1, 13, 18, 16, 2, 30, 19, 17, 9, 27, 24,$ $5, 4, 14, 6, 25, 12, 23, 15, 22, 28)$
31	$(4, 6, 29, 20, 8, 28, 24, 1, 7, 12, 22, 5, 25, 30, 26, 13, 11, 31, 23, 19,$ $16, 21, 15, 27, 17, 3, 2, 14, 10, 18, 9)$
32	$(1, 2, 4, 8, 6, 5, 3, 7, 17, 18, 20, 24, 22, 21, 19, 23, 9, 10, 12, 16,$ $14, 13, 11, 15, 25, 26, 28, 32, 30, 29, 27, 31)$

Remark 4.1 C_n is always a multiple of $n\phi(n)$. One sees this as follows : For each pair of integers $a, b \in [n]$ such that $\gcd(a, n) = 1$, the map $\tau_{a,b} : [n] \to [n]$ defined by

$$\tau_{a,b}(i) \equiv ai + b \pmod{n},$$

is a permutation of $[n]$. The set L_n of such 'linear' permutations of $[n]$ is a non-normal subgroup of S_n of order $n\phi(n)$. Then it is easily verified that, if X_n denotes the set of AP-avoiding permutations of $\mathbf{Z}_n$, then $X_n = X_n^{-1} = L_n X_n L_n$.

Remark 4.2 Theorem B and Conjecture C consider which finite cyclic groups possess k-term AP-avoiding permutations. Despite Lemma 3.5, it is not clear to us what happens for non-cyclic groups. By the same argument used to prove necessity of the condition of Theorem A, a necessary requirement for the finite group G to possess a k-term AP-avoiding permutation is that

$$|\Omega_2(G)| \leq \sqrt{|G|}.$$

The full classification of those finite groups which admit such permutations is an important open question for us.

5 Concluding remarks

In addition to answering the questions posed in our earlier remarks and conjectures, there are many directions in which one might pursue our ideas. Here are just two suggestions :

1. We have mainly studied permutations avoiding the arithmetic patterns 'AP' and 'Sidon'. But, as outlined in the introduction, there are many other patterns one might profitably study.

2. Instead of just studying pattern-avoiding permutations on a (subset of a) semigroup S, one might study arbitrary (not necessarily injective or surjective) pattern-avoiding functions $\pi : S_1 \rightarrow S_2$ between two semigroups S_1, S_2.

Acknowledgement. I wish to thank Urban Larsson and Jonas Knape for help with producing numerical data. I also thank them and Johanna Pejlare for useful discussions.

References

[**CD**] C.J. Colbourn and J.H. Dinitz eds., The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton, 1996.

[**G1**] W.T. Gowers, A new proof of Szemerédi's theorem. *Geom. Funct. Anal.* **11** (2001), no. 3, 465-588.

[**G2**] W.T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four. *Geom. Funct. Anal.* **8** (1998), no. 3, 529-551.

[**GGL**] R.L. Graham, M. Grötschel and L. Lovász eds., The Handbook of Combinatorics, Vol. I. North Holland, 1995.

[**K**] A.G. Kurosh, The Theory of Groups, Vol. I. Chelsea Publishing Company, New York, 1960.

[**S**] A.F. Sidorenko, An infinite permutation without arithmetic progressions. *Discrete Math* **69** (1988), 211.

[**SS**] R. Simion and F. Schmidt, Restricted permutations. *European J. Combin.* **6** (1985), no. 4, 383-406.