On the Independence Number of Some Hypergraph

by

Zechun Yang

A thesis submitted to the Graduate Faculty of
Auburn University
in partial fulfillment of the
requirements for the Degree of
Master of Science

Auburn, Alabama
August 4, 2018

Keywords: Hypergraphs, Arithmetic Progressions, Van der Waerden Hypergraphs,
Independent Sets, Abelian Groups

Approved by

Peter D. Johnson, Chair, Professor of Department of Mathematics and Statistics
Dean G. Hoffman, Professor of Mathematics and Statistics
Jessica M. McDonald, Assistant Professor of Mathematics and Statistics

Abstract

For integers $1 \leq m < n$ and a prime p (we require $2 \leq m$ when $p = 2$), a subset $I(p^n, p^m) \subseteq \{0, \ldots, p^n - 1\}$ is described which contains no p^m-term cyclic arithmetic progression modulo p^n, and which is maximal among subsets of $\{0, \ldots, p^n - 1\}$ with that property. Furthermore, we investigate the same setting, but for any such group.

Acknowledgments

There are many people I would like to thank. First, I would like to thank my advisor Dr. Peter Johnson for all his guidance and encouragement through out this work. Second, I would like thank my parents, Yu Yu and Larry Wilkinson, for their endless support and love. Lastly, I would like to thank to all of my friends.

Table of Contents

The contents of this thesis has also resulted a publication which is currently submitted to the journal *Geombinatorics*, under the title *On the Independence Numbers of the Van der Waerden and cyclic Van der Waerden Hypergraphs* $W(k,t)$ *and* $W_c(k,t)$ *When* t *and* k *Are Powers of the Same Prime*.

Chapter 1

Introduction

1.1 Hypergraphs

A (simple) *hypergraph* is a pair $(V, E) = \mathcal{H}$ in which $V = V(\mathcal{H})$ is a non-empty set, the set of *vertices* of the hypergraph, and $E = E(\mathcal{H})$ is a set of subsets of V, called *hyperedges*, or just *edges*. Sometimes the elements of E are *multisubsets* of V – i.e. vertices can be repeated on edges. Sometimes E is a multiset; i.e. repeated edges are allowed. When neither of these are allowed, the hypergraph is *simple*. All of our hypergraphs will be simple, and we require $|e| \geq 2$ for all $e \in E$.

A set $S \subseteq V$ is *independent* in $\mathcal{H} = (V, E)$ if and only if S contains no edge $e \in E$. The (vertex) *independence number* of H is $\alpha(\mathcal{H}) = \max\{|S| : S \subseteq V \text{ and } S \text{ is independent in } \mathcal{H}\}$. An independent set $S \subseteq V$ such that $|S| = \alpha(\mathcal{H})$ is a *maximum independent set* in $\mathcal{H}$. An independent set $S \subseteq V$ is *maximal* in H if and only if it is not properly contained in any other independent set in $\mathcal{H}$. The *independent domination number* of $\mathcal{H}$ is $i(\mathcal{H}) = \min\{|S| : S \subseteq V \text{ and } S \text{ is a maximal independent set in } \mathcal{H}\}$.

The *chromatic number* of a hypergraph $H = (V, E)$, denoted $\chi(\mathcal{H})$, is the smallest number of colors with which V can be colored so that no $e \in E$ is monochromatic. Coloring V is the same as partitioning V into independent sets, from which we infer the well know inequality

$$|V| \leq \alpha(\mathcal{H})\chi(\mathcal{H}).$$

The independence number is also related to another chromatic hypergraph parameter: the *anti-rainbow number* of $\mathcal{H}$, denoted $\mathrm{AR}(\mathcal{H})$, is the maximum number of colors appearing in

a coloring of V such that no $e \in E$ is rainbow; e is rainbow (with reference to the coloring) if no color appears on two different vertices of e. Given an anti-rainbow coloring of $\mathcal{H}$ with $\mathrm{AR}(\mathcal{H})$ colors, form a set of vertices by choosing one representative from each color class. Since the set obtained is rainbow, it can contain no edges; that is, the set is independent. Thus, $\mathrm{AR}(\mathcal{H}) \leq \alpha(\mathcal{H})$.

1.2 The Van der Waerden hypergraphs

The set of non-negative integers will be denoted $\mathbb{N}$, and the set of integers will be denoted $\mathbb{Z}$. We will use the following notational distinction: if $a, b \in \mathbb{Z}$ and $t \in \mathbb{N} \setminus \{0\}$, $a \equiv b \pmod{t}$ means (as usual) that $t|b-a$ (t divides $b-a$), but $a = b \pmod{t}$ means that a is the smallest non-negative integer satisfying $a \equiv b \pmod{t}$. In other words, $b \pmod{t}$ stands for the non-negative remainder obtained by dividing b by t. If $X \subseteq \mathbb{Z}$, $X \pmod{t} = \{x \pmod{t} : x \in X\}$. If $t \in \mathbb{N} \setminus \{0\}$, $[t] = \{0, \ldots, t-1\}$. Note that $x \pmod{t} \in [t]$ for all $x \in \mathbb{Z}$.

Let $t, k \in \mathbb{N}$ and suppose that $t \geq k \geq 3$. A *k-term arithmetic progression* in $[t]$ is a subset $A = \{a + sd : 0 \leq s \leq k-1\} \subseteq [t]$, for some integers $a \geq 0$ and $d > 0$. The integer d is the *difference* of the arithmetic progression A. Note that for A to be a subset of $[t]$, it is necessary and sufficient that $0 \leq a$ and $a + (k-1)d \leq t-1$, given that $d > 0$.

A *k-term cyclic arithmetic progression mod t* is a set $A \pmod{t} = \{(a + sd) \pmod{t} : 0 \leq s \leq k-1\}$, for some integers $a, d \in [t]$, $d > 0$, satisfying $|A \pmod{t}| = k$. Note that every such set is automatically a subset of $[t]$. Unlike the situation with ordinary k-term arithmetic progressions, the pair (a, d) with reference to which a cyclic arithmetic progression is defined is not unique (you can always replace a by $a' = (a + (k-1)d) \pmod{t}$ and d by $d' = t - d$), and it is not automatic that the set defined with respect to a and d will have k distinct elements. Thus, because $k \geq 3$, there are no k-term cyclic arithmetic progressions mod t with $d = t/2$, when t is even. If need be we will refer to the smallest d appearing in a presentation of a k-term cyclic arithmetic progression mod t as *the* difference of the cyclic arithmetic progression mod t. We can always arrange for $d < t/2$.

The Van der Waerden hypergraph $W(k, t)$, for $t \geq k \geq 3$, has vertex set $[t]$ and edge set $E(k, t) = \{k\text{-term arithmetic progressions in } [t]\}$. The cyclic Van der Waerden hypergraph

$W_c(k,t)$ has vertex set $[t]$ and edge set $E(k,t) = \{k\text{-term cyclic arithmetic progressions mod } t\}$.

Since every ordinary k-term arithmetic progression in $[t]$ is also a k-term cyclic arithmetic progression mod t, $W(k,t)$ is a spanning (same vertex set) subhypergraph of $W_c(k,t)$. Therefore, $\chi(W(k,t)) \leq \chi(W_c(k,t))$, $\mathrm{AR}(W_c(k,t)) \leq \mathrm{AR}(W(k,t))$, and $\alpha(W_c(k,t)) \leq \alpha(W(k,t))$.

These hypergraphs are named after Bartel van der Waerden, who in 1927 proved a famous theorem [8] to the effect that for each fixed $k \geq 3$, $\chi(W(k,t)) \to \infty$ as $t \to \infty$. By remarks above, this implies that $\chi(W_c(k,t)) \to \infty$ as $t \to \infty$. However, while $\chi(W(k,t))$ is clearly monotonically non-decreasing as t increases, this is not true of $\chi(W_c(k,t)$, at least for k=3 [3].

Our aim here is to exhibit a maximal independent set $I(p^m, p^n)$ in $W_c(p^m, p^n)$, when p is a prime and $1 \leq m \leq n$, thus providing a lower bound on $\alpha(W_c(p^m, p^n))$ and an upper bound on $i(W_c(p^m, p^n))$. We do not have a nice formula for $|I(p^m, p^n)|$ except when $m = 1$ and p is an odd prime, in which case $|I(p, p^n)| = (p-1)^n$; we shall deal with this special case in the next chapter and then with the general case in the third chapter. The reason for the separation is that we think that the description of $I(p^m, p^n)$ and the proof that it is a maximal independent set of vertices in $W_c(p^m, p^n)$ will be much easier to understand after the case $m = 1$ is understood.

The case $m = 1, n = 2$, and p is an odd prime was dealt with by Berglund [1], and we must acknowledge that there was something in his proof that opened the way to our generalization.

Possibly the first attention to the independence number $\alpha(W(k,t))$ was paid by Erdős and Turán [2], who did not use hypergraph terminology. Their notation for $\alpha(W(k,t))$ was $r_k(t)$. As reported in [5], there was a great deal of work done on estimating the numbers $r_k(t)$ between 1936 and 1974. The best known of the results on this topic is a consequence of Szemerédi's Lemma [6], to which [5] is an introduction. It is a corollary of the lemma that for each $k \geq 3$, $r_k(t)/t \to 0$ as $t \to \infty$.

Our contribution here was inspired by Berglund [1]. Frankly, we were unaware of all this earlier work until very recently. We think that our main result is of a different nature from what went before, and look forward to seeing if light is thrown by it onto the older discoveries, or on it by those discoveries.

Chapter 2

The $I(p, p^n)$ case, where p is an odd prime

Lemma 2.1. *Suppose $m, p, b \in \mathbb{N}$, p is a prime and $m > 0$. Suppose that $d \in \mathbb{N}$ satisfies $d \equiv 0 \mod p^{b-1}$ and $d \not\equiv 0 \mod p^b$. Then*

$$\{id \,(\mathrm{mod}\ p^{b+m-1}) : i \in [p^m]\} = \{ip^{b-1} : i \in [p^m]\}.$$

Proof. From the hypothesis, it must be that $d = kp^{b-1}$ for some $k \not\equiv 0 \mod p$. Since p is a prime, $\gcd(k, p^m) = 1$, so that $\{ik \,(\mathrm{mod}\ p^m) : i \in [p^m]\} = [p^m]$. For $i \in [p^m]$, let $r_i = ik \,(\mathrm{mod}\ p^m) \in [p^m]$.

For $i \in [p^m]$, for some $q_i \in \mathbb{N}$, $ik = r_i + q_i p^m$. Therefore, for $i \in [p^m]$, $id = ikp^{b-1} = (r_i + q_i p^m)p^{b-1} = r_i p^{b-1} + q_i p^{m+b-1} \equiv r_i p^{b-1} \mod p^{b+m-1}$. Since $r_i \in [p^m]$, $r_i p^{b-1} < p^{b+m-1}$. Therefore $id \,(\mathrm{mod}\ p^{b+m-1}) = r_i p^{b-1} = (ik \,(\mathrm{mod}\ p^m))p^{b-1}$. Since $ik \,(\mathrm{mod}\ p^m)$ roams all over $[p^m]$ as i roams over $[p^m]$, the lemma claim is proved. □

Lemma 2.2. *If $a, b, c \in \mathbb{N}$, $b, c > 0$, and $b|c$, then $a \,(\mathrm{mod}\ b) = (a \,(\mathrm{mod}\ c)) \,(\mathrm{mod}\ b)$.*

Proof. Suppose $a, b, c \in \mathbb{N}$, $b, c > 0$, and $b|c$. Let $r = a \,(\mathrm{mod}\ c)$. Then r is the remainder of c divided into a. Then $0 \leq r < c$ and for some $q \in \mathbb{Z}$, $a = qc + r$. Since $b|c$, $c = bt$ for some $t \in \mathbb{Z}$. Dividing $r = a \,(\mathrm{mod}\ c)$ by b, we have $r = bx + z$ for $x, z \in \mathbb{N}$ with $0 \leq z < b$; $z = r \,(\mathrm{mod}\ b)$. We have $a = qc + r = qbt + bx + z = (q + x)b + z$. So, by the uniqueness of the remainder, $a \,(\mathrm{mod}\ b) = z = r \,(\mathrm{mod}\ b) = (a \,(\mathrm{mod}\ c)) \,(\mathrm{mod}\ b)$. □

For each integer $b > 1$, it is fundamental that every positive integer a has a unique b-ary (or, base b) representation,

$$a = \sum_{j=0}^{n} c_j b^j,$$

for some $n \in \mathbb{N}$, $c_n > 0$, and $c_j \in [b]$, for $j = 0, \ldots, n$. Whether or not $c_n > 0$, if $c_0, \ldots c_n \in [b]$, then $0 \leq \sum_{i=0}^{n} c_j b^j \leq b^{n+1} - 1$.

Now, for $n \in N$ and for a prime $p \in \mathbb{N}$, let

$$I(p, p^n) = \{\sum_{i=0}^{n-1} p^i a_i : a_i \in [p-1]\}.$$

For each positive integer prime p, the set $I(p, p^n)$ is the subset of $[p^n]$ consisting of those integers a such that $p - 1$ does not appear among the coefficients $c_0, \ldots, c_{n-1}$ in a's unique p-ary representation, $a = \sum_{i=0}^{n-1} p^i c_i$. Therefore $I(p, p^n)$ has a one-to-one correspondence with the set of sequences $(c_0, \ldots, c_{n-1}) \in [p-1]^n$. Thus, the conclusions of the following lemma are straightforward to see.

Lemma 2.3. *Suppose p is a positive prime, n is a positive integer. Then $|I(p, p^n)| = (p-1)^n$ and $\max(I(p, p^n)) = (p-2)\frac{p^n - 1}{p-1}$.*

Lemma 2.4. *Suppose that p is a positive prime, $m, n \in \mathbb{N}$ and $0 < m \leq n$. Then*

i. $I(p, p^m) \subseteq I(p, p^n)$*;*

ii. $I(p, p^m) = I(p, p^n) \pmod{p^m}$*;*

iii. if $y \in \mathbb{N}$ and $y \pmod{p^m} \notin I(p, p^m)$, then $y \pmod{p^n} \notin I(p, p^n)$

Proof. i. If $x \in \sum_{j=0}^{m-1} c_j p^j \in I(p, p^m)$, $c_j \in [p-1]$, $j = 0, \ldots, m-1$, then $x = \sum_{j=0}^{n-1} c_j p^j \in I(p, p^n)$ if $c_j = 0$, $m \leq j \leq n-1$.

ii. ($\subseteq$) Since $I(p, p^m) \subseteq I(p, p^n)$ and $x \in I(p, p^m)$ implies that $x \leq p^m - 1$, it follows that if $x \in I(p, p^m)$, then $x = x \pmod{p^m} \in I(p, p^n) \pmod{p^m}$. Thus, $I(p, p^m) \subseteq I(p, p^n) \pmod{p^m}$.

($\supseteq$) If $x = \sum_{j=0}^{n-1} c_j p^j \in I(p, p^n)$, $c_j \in [p-1]$, $j = 0, \ldots, n-1$, then $x \equiv \sum_{j=0}^{m-1} c_j p^j \pmod{p^m}$ and $\sum_{j=1}^{m-1} c_j p^j < p^m - 1$, so $\sum_{j=0}^{m-1} c_j p^j \in I(p, p^m)$. Thus, $I(p, p^m) \supseteq I(p, p^n) \pmod{p^m}$.

Hence, $I(p, p^m) = I(p, p^n) \pmod{p^m}$.

iii. Suppose that $y \in \mathbb{N}$ and $y \pmod{p^n} \in I(p, p^n)$. Then $y \pmod{p^m} = (y \pmod{p^n}) \pmod{p^m} \in I(p, p^m)$, by ii and Lemma 2.2. The desired conclusion follows by contraposition.

□

Theorem 2.5. *Let $p \in \mathbb{N}$ be an odd prime and let $n \in \mathbb{N}$. $I(p, p^n)$ does not contain any p-term cyclic arithmetic progression modulo p^n.*

Proof. Let $e \subseteq I(p, p^n)$ be a p-term cyclic arithmetic progression modulo p^n. Let $d < \frac{p^n}{2}$ be the common difference of e. Then $e = \{a + id \pmod{p^n} : i \in [p]\}$, for some $a \in [p^n]$. Let $c_0, \ldots, c_{n-1} \in [p]$ such that $a = \sum_{j=0}^{n-1} c_j p^j$.

Since $0 < d < p^n$, $p^n \nmid d$. Let m be the positive integer such that $d \equiv 0 \mod p^{m-1}$ and $d \not\equiv 0 \mod p^m$; then $m \leq n$.

By Lemma 2.1, with the role of b there played by m here, there exists $i \in [p]$ such that

$$id \pmod{p^m} = (p - 1 - c_{m-1})p^{m-1}.$$

Then

$$\begin{aligned} a + id &\equiv \sum_{j=0}^{m-1} c_j p^j + (p - 1 - c_{m-1})p^{m-1} \\ &= \sum_{j<m-1} c_j p^j + (p-1)p^{m-1} \mod p^m, \end{aligned}$$

which implies that

$$(a + id) \pmod{p^m} = \sum_{j<m-1} c_j p^j + (p-1)p^{m-1} \notin I(p, p^n),$$

which implies that $(a + id) \pmod{p^n} \notin I(p, p^n)$, by Lemma 2.4 (iii). Thus, e is not contained in $I(p, p^n)$. □

Corollary 2.6. *Let p be an odd prime and $n \in \mathbb{N}$ with $n \geq 1$. Then $\alpha(W_c(p, p^n)) \geq (p-1)^n$.*

Proof. By Theorem 2.5, $I(p, p^n)$ is an independent set of $W_c(p, p^n)$. The conclusion follows. □

In the next chapter, we will show that the set $I(p, p^n)$ is a maximal independent set in $W_c(p, p^n)$, and in $W(p, p^n)$.

Chapter 3

The General Case, $I(p^m, p^n)$, where p is a prime and $m, n \in \mathbb{N}$ with $0 < m \leq n$

Let $m, n \in \mathbb{N}$ with $0 < m \leq n$. Let p be a prime. Let $g : \mathbb{N} \to [p]^\infty$ be the function that maps n to its p-ary representation. For $i \in \mathbb{N}$, we denote by $g_i(x)$ the i-th digit of the p-ary representation of $x \in \mathbb{N}$. Note that if $g_i(x) = a$, then $g_{i+q}(p^q x) = a$, for all $i, a, q, x \in \mathbb{N}$.

Theorem 3.1. *Suppose that p is a prime, $1 \leq m \leq n$, ($2 \leq m$ if $p = 2$), and $e \subseteq [p^n]$ is a p^m-term cyclic arithmetic progression mod p^n. Then e contains a term $y \in [p^n]$ such that for some $t \in \{0, \ldots, n-m\}$, $g_{t+j}(y) = p-1$, $j = 0, \ldots, m-1$.*

Proof. Let $e = \{(a+id) \pmod{p^n} : i \in [p^m]\}$ be a p^m-term cyclic arithmetic progression mod p^n, where $a, d \in [p^n]$. Then $d = kp^{b-1}$ for some integers $1 \leq k, b$ such that $b \leq n$ and $p \nmid k$. By Lemma 2.1,

$$\{id \pmod{p^{m+b-1}} : i \in [p^m]\} = \{jp^{b-1} : j \in [p^m]\} \qquad (*)$$

Claim: $m + b - 1 \leq n$.

Proof: Suppose $m + b - 1 > n$. Then, because $b - 1 < n$, $b - 1 + t = n$ for some $t \in \{1, \ldots, m-1\}$. Then $p^t \in [p^m]$, so $(a+p^t d) \pmod{p^n})) \in E$. But $a+p^t d = a+kp^{b-1+t} = a + kp^n \equiv a \mod p^n$, so $a = a \pmod{p^n} = (a + p^t d) \pmod{p^n}$, yet $0 < p^t \in [p^m]$. This contradicts the supposition that $e = \{(a+id) \pmod{p^n} | i \in [p^m]\}$ is a p^m-term cyclic arithmetic progression mod p^n. Therefore $m + b - 1 \leq n$. □

Let $a = qp^{b-1} + r$, $0 \leq q$, $0 \leq r < p^{b-1}$, and let $q = sp^m + q'$, $0 \leq s$, $0 \leq q' < p^m$. Then $p^m - 1 - q' \in [p^m]$. Therefore, by $(*)$, for some $z \in [p^m]$, $zd \pmod{p^{m+b-1}} = (p^m - 1 - q')p^{b-1}$.

For short, let $x = zd \pmod{p^{m+b-1}}$. We see that

$$\begin{aligned} a + x &= (sp^m + q')p^{b-1} + r + (p^m - 1 - q')b^{b-1} \\ &= sp^{m+b-1} + (p^m - 1)p^{b-1} + r \\ &\equiv (p^m - 1)p^{b-1} + r \mod p^{m+b-1}. \end{aligned}$$

Since $x = zd \pmod{p^{m+b-1}}$, we have that

$$a + zd \equiv a + x \equiv (p^m - 1)p^{b-1} + r \mod p^{m+b-1}.$$

Then, since $(p^m - 1)p^{b-1} + r = p^{m+b-1} - p^{b-1} + r < p^{m+b-1}$,

$$\begin{aligned} (a + zd) \pmod{p^{m+b-1}} &= (p^m - 1)p^{b-1} + r \\ &= r + (p-1)(1 + \cdots + p^{m-1})p^{b-1}. \end{aligned}$$

Since $r < p^{b-1}$ and $m + b - 1 \leq n$, the p-ary representation of

$$y = (a + zd) \pmod{p^n} \in e$$

will be

$$y = \sum_{0 \leq j < b-1} g_j(r)p^j + \sum_{j=b-1}^{b-1+m-1} (p-1)p^j + \sum_{m+b-1 \leq j \leq n-1} g_j(y)p^j.$$

□

Corollary 3.2. *With $m, n,$ and p as in Theorem 3.1, the set $I(p^m, p^n)$ of integers $w \in [p^n]$, such that the sequence $(g_0(w), g_1(w), \ldots, g_{n-1}(w))$ of p-ary coefficients contains no constant block of m consecutive entries all equal to $p-1$, contains no $p^m - term$ cyclic arithmetic progression mod p^n; thus $I(p^m, p^n)$ is an independent set of vertices in the hypergraph $W_c(p^m, p^n)$.*

Note, the set $I(p^m, p^n)$ we defined in Corollary 3.2 is the same as the one we defined in chapter 2, when $m = 1$.

Theorem 3.3. *Let m, n, p, and $I(p^m, p^n)$ be as in Corollary 3.2. $I(p^m, p^n)$ is a maximal independent set in $W_c(p^m, p^n)$ and $W(p^m, p^n)$.*

Proof. Suppose that $u \in [p^n] \setminus I(p^m, p^n)$. Then the sequence $(g_0(u), g_1(u), \ldots, g_{n-1}(u)) \in [p]^n$ contains a block of m consecutive $p-1$'s. We aim to show that $I(p^m, p^n) \cup \{u\}$ contains some p^m-term cyclic arithmetic progression mod p^n. (In fact, the arithmetic progression that we will find will be an ordinary p^m-term arithmetic progression in $[p^n]$.)

Consider all the blocks of at least m consecutive entries in $(g_i(u))_{i=0}^{n-1}$ with constant entry $p-1$. Partition each maximal such block into subblocks of length exactly m, with, possibly, a remainder, or "runt" block of length less than m left over. Let the blocks of m consecutive indices for the blocks $(p-1, \ldots, p-1) = \{p-1\}^m$ thus obtained in the sequence $(g_i(u))_{i=0}^{n-1}$ be $Z_1, \ldots, Z_q$. That is, for some indices $j_1, \ldots, j_q$, satisfying $0 \le j_1 < j_1 + m \le j_2 < \cdots \le j_q < j_q + m \le n$, $Z_i = \{j_i, \ldots, j_i + m - 1\}$, $i = 1, \ldots, q$, and $g_{j_i+s}(u) = p-1, i = 1, \ldots, q$, $0 \le s \le m-1$.

Note that, if $Z = \bigcup_{i=1}^{q} Z_i$, then $[n] \setminus Z$ contains no block $\{t, \ldots, t+m-1\}$ such that $g_{t+j}(u) = p-1$ for all $j = 0, \ldots, m-1$. Therefore, if $a = \sum_{j \in [n] \setminus Z} g_j(u) p^j$ and $d = \sum_{i=1}^{q} p^{j_i}$ (recall that j_i is the smallest index in Z_i), then $a + sd \in I(p^m, p^n)$, $s = 0, \ldots, p^m - 2$, while $a + (p^m - 1)d = u$. Thus, $I(p^m, p^n) \cup \{u\}$ contains a p^m-term arithmetic progression. Therefore, $I(p^m, p^n)$ is a maximal independent set in both $W(p^m, p^n)$ and in $W_c(p^m, p^n)$. □

It is easily verified that $I(3, 9) = \{0, 1, 3, 4\}$ is a maximum independent set in $W_c(3, 9)$, but $\{0, 1, 5, 7, 8\}$ is an independent set in $W(3, 9)$, so $I(3, 9)$ is not maximum in $W(3, 9)$. Obviously $\{0, 1, 5, 7, 8\}$ is not independent in $W_c(3, 9)$, as it contains the 3-term cyclic arithmetic progression $\{5, 7, 0\}$.

Corollary 3.4. *With m, n, and p as in Theorem 3.1,*

$$\begin{aligned} \max(i(W(p^m, p^n)), i(W_c(p^m, p^n))) &\le |I(p^m, p^n)| \\ &\le \alpha(W_c(p^m, p^n)) \le \alpha(W(p^m, p^n)). \end{aligned}$$

Determining $|I(p^m, p^n)|$ is an enumeration problem about words of length n over the alphabet $[p] = \{0, \ldots, p-1\}$. It appears that this problem can be "solved" by giving a generating function [7]. We leave the investigation of this enumeration problem for the future; but here are three remarks bearing on the matter.

1. For fixed n, $|I(p^m, p^n)|$ non-decreases as m increases. Therefore, for $1 \leq m \leq n$,

$$(p-1)^n = |I(p, p^n)| \leq |I(p^m, p^n)| \leq |I(p^n, p^n)| = p^n - 1 = \alpha(W(p^n, p^n)).$$

2. For fixed $m \geq 1$, $|I(p^m, p^n)|$ is non-decreasing as n increases. (This is an easy corollary of Corollary 3.2.) Therefore, for $1 \leq m \leq n$,

$$|I(p^m, p^n)| \geq |I(p^m, p^m)| = p^m - 1.$$

3. By a corollary of Szemerédi's Lemma, previously mentioned, for each $m \geq 1$, $|I(p^m, p^n)|/p^n \leq \alpha(W(p^m, p^n))/p^n \to 0$ as $n \to \infty$.

Chapter 4

Van der Waerden hypergraphs for finite abelian groups of order p^n, where $n \in \mathbb{N}$ and p is a prime

4.1 Definitions

Let $k \in \mathbb{N}$ and suppose that $k \geq 3$. let A be an abelian group. A *k-term arithmetic progression over A* is a subset $e = \{a + sd : 0 \leq s \leq k-1\} \subseteq A$, for some $a, d \in A$ and $|e| = k$, and same as before, we say d is the *difference* of the arithmetic progression. Note A has a k-term arithmetic progression if and only if A has a element with order at least k. The *Van der Waerden hypergraph over A*, $W(k, A)$, has vertex set A and edge set $E(k, A) = \{k$-term arithmetic progression over $A\}$.

Let $\mathcal{H}_1 = (V_1, E_1)$, $\mathcal{H}_2 = (V_2, E_2)$ be two hypergraphs. A *hypergraph isomorphism* from $\mathcal{H}_1$ to $\mathcal{H}_2$ is a bijection $f : V_1 \to V_2$ such that for every $e \subseteq V$, $e \in E_1$ if and only if $f(e) \in E_2$. If such f exists, we say $\mathcal{H}_1$ and $\mathcal{H}_2$ are *isomorphic*. Note for p prime, $m, n \in \mathbb{N}$ with $n \geq m \geq 1$, $\pi : W_c(p^m, p^n) \to W(p^m, Z_{p^n})$ by $\pi(x) = x$ is a hypergraph isomorphism, hence $W_c(p^m, p^n)$ and $W(p^m, Z_{p^n})$ are isomorphic. In fact, $W_c(k, t)$ and $W(k, \mathbb{Z}_t)$ are isomorphic for all $3 \leq k \leq t$, $k, t \in \mathbb{N}$.

4.2 Abelian group of order p^n where $n \in \mathbb{N}$ and p is a prime

Theorem 4.1. *Fundamental theorem of finite abelian groups Let A be a non trivial finite abelian group. There exists unique integers $m_1|m_2|\ldots|m_t$ such that*

$$A \cong \bigoplus_{i=1}^{t} \mathbb{Z}_{m_i}$$

.

This theorem is a classic result and its proof can be found in [4]. Also, by the fundamental theorem of finite abelian groups, to study finite abelian groups of order p^n, p prime, all we have to do is to study the direct sums of the cyclic groups of order p^r, $\mathbb{Z}_{p^r}$, for some $r \in \mathbb{N}$.

For an abelian group A and $d \in A$, we use $o(d)$ denote the order of d in A. Let $m_1, m_2, \ldots, m_n$ be positive integers. Let $A = \bigoplus_{i=1}^{n} \mathbb{Z}_{m_i}$. Let $\pi_i : A \to Z_{m_i}$ be the canonical projection, for $1 \leq i \leq n$. Let $d \in A$. Let $o_i(d) = o(\pi_i(d))$ in $\mathbb{Z}_{m_i}$.

Lemma 4.2. *Let l the least common multiple of $o_1(d), o_2(d), \ldots, o_n(d)$. Then $o(d) = l$.*

Proof. On one hand, $l\pi_i(d) = 0$ for every $1 \leq i \leq n$, so $ld = 0$, hence $o(d)|l$. On the other hand, $o_i(d)|o(d)$ for every $1 \leq i \leq n$, since $o(d)\pi_i(d) = 0$ for every $1 \leq i \leq n$, so $l|d$. Hence, $l = o(d)$. □

Theorem 4.3. *Let p be a prime. Let $r_1 \leq r_2 \cdots \leq r_n$ be positive integers. Let $A = \bigoplus_{i=1}^{n} \mathbb{Z}_{p^{r_i}}$. For $k \in \mathbb{N}$ with $k \geq 3$, if e is a k-term arithmetic progression over A, then $\pi_i(e)$ is a k-term arithmetic progression over $\mathbb{Z}_{p^{r_i}}$ for some $1 \leq i \leq n$.*

Proof. Let $k \in \mathbb{N}$ such that $k \geq 3$ and suppose e is a k-term arithmetic progression over A. Let d be a common difference of e. Then $o(d) \geq k$. Now, by lemma 4.2, $l = o(d) \geq k$, where l is the least common multiple of $o_1(d), o_2(d), \ldots, o_n(d)$. Since $o_i(d)|p^{r_i}$, for every $1 \leq i \leq n$, $o_i(d) = p^{q_i}$ for some $q_i \leq r_i$ for every $1 \leq i \leq n$. Let $1 \leq i \leq n$ such that $q_i = \max_{1 \leq j \leq n} q_j$. Then the least common multiple of $o_1(d), o_2(d), \ldots, o_n(d)$ is p^{q_i}, which means, $o_i(d) = p^{q_i} = l = o(d) \geq k$. Now we claim that $\pi_i(e)$ is a k-term arithmetic progression over A. Indeed, since order of $o_i(d) \geq k$ and $e = \{a + jd : 0 \leq j \leq k-1\}$ for some $a \in A$, so

$$\begin{aligned}
\pi_i(e) &= \pi_i(\{a + jd : 0 \leq j \leq k-1\}) \\
&= \{\pi_i(a + jd) : 0 \leq j \leq k-1\} \\
&= \{\pi_i(a) + \pi_i(jd) : 0 \leq j \leq k-1\} \\
&= \{\pi_i(a) + j\pi_i(d) : 0 \leq j \leq k-1\},
\end{aligned}$$

which is a k-term arithmetic progression in $\mathbb{Z}^{p^{r_i}}$. □

Note the converse of Theorem 4.3 is false. Indeed, let $A = \mathbb{Z}_3 \oplus \mathbb{Z}_9$. Then $e = \{(0,1),(0,2),(1,3)\}$ is not a 3-term arithmetic progression over A; however, $\pi_2(e) = \{1,2,3\}$ is a 3-term arithmetic progression over $\mathbb{Z}_9$. However, by Theorem 4.3, we do have some corollaries on the independent sets of the hypergraph $W(k,A)$.

Corollary 4.4. *Let p be a prime. Let $r_1 \leq r_2 \cdots \leq r_n$ be positive integers. Let $A = \bigoplus_{i=1}^{n} \mathbb{Z}_{p^{r_i}}$. Let $I \subseteq A$. If $\pi_i(I)$ is independent in $W(k, Z_{p^i})$ for every $1 \leq i \leq n$. Then I is independent in $W(k,A)$.*

Corollary 4.5. *Let p be a prime. Let $r_1 \leq r_2 \cdots \leq r_n$ be positive integers. Let $A = \bigoplus_{i=1}^{n} \mathbb{Z}_{p^{r_i}}$. Let $\pi : \mathbb{Z} \to \mathbb{Z}_{p_i}$ be the canonical epimorphism, that is $\pi(x) = x$. Let*

$$I(p^m, \mathbb{Z}_{p^q}) = \begin{cases} \mathbb{Z}_{p^q} & \text{if } m > q \\ \pi(I(p^m, p^q)) & \text{if } m \leq q. \end{cases}$$

Let $m \in \mathbb{N}$. Then $I = \bigoplus_{i=1}^{n} I(p^m, \mathbb{Z}_{p^q})$ is an independent set in the hypergraph $I(p^m, A)$ and $\alpha(W(p^m, A) \geq |I|$.

References

[1] Kenneth Berglund, *The maximum size of subset forbidding cyclic arithmetic progressions*, Geombinatorics **27** (January, 2018), 103–108.

[2] P Erdős and P. Turàn, *On some sequences of integers*, J. London Math. Suc **11** (1936), 261–264.

[3] Daniel Grier, *On the cyclic van der Waerden number*, Geombinatorics **21** (April, 2012), 129–131.

[4] Thomas W. Hungerford, *Algebra*, Springer, 1974.

[5] Endre Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Proceedings of the International Congress of Mathematicians, Vancouver, 1974, pp. 503–505.

[6] ———, *On sets of integers containing no k elements in arithmetic progression*, Acta Arithmetica **27** (1975), 199–254.

[7] Jair Taylor, *Counting words with Laguerre series*, The Electronic Journal of Combinatorics **21** (2014), no. 2, #P2.1.

[8] B. L. van der Waerden, *Beweis einer baudetschen vermutung*, Nieuw. Arch. Wisk. **15** (1927), 212–216.