INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 8 (2008), #A45

UNIVERSAL SETS AND THE VECTOR GAME

Zhivko Nedev[1]
Department of Mathematics and Statistics, University of Victoria, Victoria, British Columbia, Canada V8W 3R4
znedev@gmail.com

Received: 3/19/08, Accepted: 10/8/08, Published: 10/27/08

Abstract

We consider two complementary classes of subsets in $\mathbb{Z}_n$. A non-empty subset U of $\mathbb{Z}_n$ is *universal* if, for all $x \in U$ and all $0 < \ell \leq \frac{n}{2}$, at least one of $x \pm \ell \pmod{n}$ is in U. A proper subset M of $\mathbb{Z}_n$ is *middle-inclusive* if, for all $a, b \in M$, all solutions x of $2x \equiv a + b \pmod{n}$ are in M. We derive a formula for $\beta(n)$, the minimum cardinality of a universal set modulo n, and examine how universal sets arise in the context of the *Vector Game*, studied in an earlier paper by Nedev and Muthukrishnan.

1. Introduction

In this paper we introduce the concept of a *universal* subset of $\mathbb{Z}_n$, and derive a formula for $\beta(n)$, the minimal cardinality of a universal set modulo n, in terms of the factorization of n.

We also study the connection between universal sets and the *Vector Game*, a two-player game in which one player attempts to minimize, and the other to maximize the cardinality of the set of positions visited during the course of the game. This game was studied for the first time in [2, 3]. We prove that the set of positions visited is $\beta(n)$ when both players play optimally.

2. Universal and Middle-inclusive Sets

Definition. A nonempty subset S of $\mathbb{Z}_n$ is called *universal modulo n* if, for each $x \in S$ and for each magnitude $\ell \in \mathbb{N}, 1 \leq \ell \leq \left\lfloor \frac{n}{2} \right\rfloor$, at least one of $\{x + \ell \pmod{n}, x - \ell \pmod{n}\}$ is in S. Let $\beta(n)$ denote the minimum cardinality of a universal set modulo n.

Note that $\mathbb{Z}_n$ is trivially universal. Furthermore, when n is odd, $\mathbb{Z}_n \setminus \{y\}$ is universal for

[1] This paper was partially written at DIMACS/Rutgers University.

any $y \in \mathbb{Z}_n$.

Definition. A proper subset S of $\mathbb{Z}_n$ is called *middle-inclusive modulo n* if, for all $a, b \in S$, when $x \in \mathbb{Z}_n$ is a solution of $2x \equiv a + b \pmod{n}$, $x \in S$. In other words, if $a, b \in S$, then so is their midpoint x.

Notice that for $a = b$, the congruence $2x \equiv a + b \pmod{n}$ has only the trivial solution a when n is odd, and has exactly one non-trivial solution, $a + \frac{n}{2}$, when n is even. For distinct a and b, there is exactly one solution when n is odd, and either zero or two solutions when n is even.

Note that $\emptyset$ is trivially middle-inclusive. Furthermore, when n is odd, $\{y\}$ is middle-inclusive for any $y \in \mathbb{Z}_n$.

Lemma 1. *S is universal modulo n if and only if $\mathbb{Z}_n \setminus S$ is middle-inclusive modulo n.*

Proof. ($\Rightarrow$) Let $S \subseteq \mathbb{Z}_n$ be universal modulo n. Now $S \neq \emptyset$, so $\mathbb{Z}_n \setminus S \subsetneq \mathbb{Z}_n$. Let $a, b \in \mathbb{Z}_n \setminus S$. Let $x \in \mathbb{Z}_n$ be a solution to $2x \equiv a + b \pmod{n}$, and assume by way of contradiction that $x \notin \mathbb{Z}_n \setminus S$. Then $x \in S$. Now one of $x - a \pmod{n}, -x + a \pmod{n}$ will be $\leq \lfloor \frac{n}{2} \rfloor$; we assume, without loss of generality, that $x - a \pmod{n} \leq \lfloor \frac{n}{2} \rfloor$. Then since S is universal, $x + (x - a) \equiv 2x - a \equiv b \pmod{n}$ or $x - (x - a) \equiv a \pmod{n}$ is in S, contradicting our choice of a and b. Therefore $\mathbb{Z}_n \setminus S$ is middle-inclusive modulo n.

($\Leftarrow$) Let $S \subseteq \mathbb{Z}_n$ be such that $\mathbb{Z}_n \setminus S$ is middle-inclusive modulo n. Now $\mathbb{Z}_n \setminus S \subsetneq \mathbb{Z}_n$, so $S \neq \emptyset$. Let $x \in S, \ell \in \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$. Assume by way of contradiction that $x + \ell \pmod{n}$, $x - \ell \pmod{n}$ are in $\mathbb{Z}_n \setminus S$. Since $\mathbb{Z}_n \setminus S$ is middle-inclusive, and since x is a solution to $2x \equiv (x + \ell) + (x - \ell) \pmod{n}$, it follows that $x \in \mathbb{Z}_n \setminus S$, contradicting our choice of x. Therefore S is universal modulo n. □

Corollary 2. *$\beta(n) = n - \max|S|$, where S ranges over all middle-inclusive sets modulo n.*

3. Minimum Size Universal Sets

Theorem 3. *For any positive integer n,*

$$\beta(n) = \begin{cases} n & \text{if } n = 2^k \text{ for some } k > 0, \\ \frac{p-1}{p} \cdot n & \text{otherwise, where } p \text{ is the smallest odd prime factor of } n. \end{cases}$$

Note that $\beta(n)$ is non-monotonic; for example, for $n = 1 \ldots 16$, $\beta(n)$ is $1, 2, 2, 4, 4, 4, 6, 8, 6, 8, 10, 8, 12, 12, 10, 16$. This is a new sequence in the Encyclopedia of Integer Sequences [1] with reference to [2].

We will prove Theorem 3 by characterizing all non-empty middle-inclusive sets modulo n.

Definition. Let d be a positive integer such that $d \mid n$. Let $0 \le r < d$ be an integer. We let $C_n(r,d) = \{r + id \mid 0 \le i < \frac{n}{d}\} \subseteq \mathbb{Z}_n$ be the arithmetic progression beginning at r with common difference d.

Lemma 4. *Let n be a positive integer, and $d > 2$ an odd divisor of n. Then for all integers r, with $0 \le r < d$, $C_n(r,d)$ is a middle-inclusive subset of $\mathbb{Z}_n$. Conversely, if M is a non-empty middle-inclusive subset of $\mathbb{Z}_n$, then there exists an odd positive integer d with $d \mid n$, and an integer $0 \le r < d$, such that $M = C_n(r,d)$.*

Proof. ($\Rightarrow$) Let $S = C_n(r,d)$. Since $d > 2$, $S \subsetneq \mathbb{Z}_n$. Let $a, b \in S$. Then $a = r + id, b = r + jd, 0 \le i, j < \frac{n}{d}$. If $x \in \mathbb{Z}_n$ is a solution to $2x \equiv a + b \pmod{n}$, then $2x \equiv 2r + (i+j)d \pmod{n}$. It follows that $x \equiv r + \frac{i+j}{2}d \pmod{n}$ or $x \equiv r + \frac{i+j}{2}d + \frac{n}{2} \equiv r + \frac{i+j+\frac{n}{d}}{2}d \pmod{n}$, and so $x \in S$. Therefore S is middle-inclusive.

($\Leftarrow$) Let M be a non-empty middle-inclusive subset of $\mathbb{Z}_n$.

Case 1) $|M| = 1$. Denote $M = \{r\}$. Note that n is odd; otherwise, r and $r + \frac{n}{2} \pmod{n}$ would both be in M. Thus $M = C_n(r,n)$.

Case 2) $|M| > 1$. Denote $M = \{i_0, i_1, \ldots, i_{\ell-1}\}$, where $0 \le i_0 < i_1 < \ldots < i_{\ell-1} \le n-1$. Since M is middle-inclusive, $\ell = |M| < n$. We will adopt the convention for the rest of this proof that all index arithmetic is performed modulo ℓ; that is, $i_\ell = i_0$.

(For the intuition: let a round table have n symmetric positions labeled as $0, 1, \ldots, n-1$ in clockwise direction.) For $i, j \in \{0, 1, \ldots, n-1\}$, let $d_+(i,j)$ denote the distance from i to j traveling in the clockwise direction. Thus,

$$d_+(i,j) = \begin{cases} j - i & \text{if } i \le j, \\ n - (i-j) & \text{otherwise.} \end{cases}$$

Suppose there exists an index $j \in \{0, 1, \ldots, \ell-1\}$ such that $d_+(i_j, i_{j+1})$ is even. Since M is middle-inclusive, the midpoint between i_j and i_{j+1} is in M, contradicting i_j and i_{j+1} being consecutive elements of M. Thus $d_+(i_j, i_{j+1})$ is odd for all j. Now, consider three consecutive elements of M, $i_{j-1}, i_j, i_{j+1}, j \in \{0, 1, \ldots, \ell-1\}$. Since $d_+(i_{j-1}, i_j)$ and $d_+(i_j, i_{j+1})$ are odd, their sum $d_+(i_{j-1}, i_{j+1})$ is even. Suppose $d_+(i_{j-1}, i_j) \ne d_+(i_j, i_{j+1})$. Then the midpoint between i_{j-1} and i_{j+1} is not i_j. However, since M is middle-inclusive, this midpoint is in M, contradicting the three elements being consecutive. Thus $d_+(i_{j-1}, i_j) = d_+(i_j, i_{j+1})$. Since this is true for all j, it follows that $d = d_+(i_0, i_1) \mid n$.

Let $r = i_0$. Then $M = \{r, r+d, r+2d, \ldots, r + (\frac{n}{d} - 1)d\} = C_n(r,d)$. □

Proof of Theorem 3. We have two cases to consider.

Case 1) $n = 2^k$ for some $k > 0$. Suppose there exists a non-empty middle-inclusive subset of $\mathbb{Z}_n$. Then by Lemma 4, there must exist an odd divisor $d > 2$ of n, contradicting $n = 2^k$. Therefore, the only middle-inclusive subset of $\mathbb{Z}_n$ is $M = \emptyset$. It follows that $S = \mathbb{Z}_n \setminus M = \mathbb{Z}_n$ is the only universal subset of $\mathbb{Z}_n$. Thus $\beta(n) = n$.

Case 2) $n \neq 2^k$. By Lemma 4, all non-empty middle-inclusive subsets of $\mathbb{Z}_n$ are of the form $C_n(r,d)$, where $d > 2$ is odd and $d \mid n$. The largest of these subsets is $C_n(r,p)$, where $0 \leq r < d$ and p is the smallest odd prime factor of n. Then $\mathbb{Z}_n \setminus C_n(r,p)$ is the smallest universal subset, and thus $\beta(n) = n - |C_n(r,p)| = n - \frac{n}{p} = \frac{p-1}{p} \cdot n$.

□

4. An Application for Small Universal Sets: The Vector Game

In [2], the following two-player game was introduced, which we will here call the *maximal variant* of the *Vector Game*. The game is played on a circular board with n positions around its circumference labelled from 0 to $n-1$. A token is initially placed at position 0; as the game proceeds, the token will mark the current position, denoted i. A round consists of the first player, Magnus (from *magnitude*), choosing an integer magnitude $0 < \ell \leq \frac{n}{2}$, followed by the second player, Derek (from *direction*), choosing a direction $+$ or $-$. The token is then moved to $i + \ell \pmod{n}$ or $i - \ell \pmod{n}$ according to Derek's choice. Magnus aims to maximize the cardinality of the set of positions visited over the course of the game; Derek aims to minimize this same quantity.

In the *minimal variant* of the game which has been introduced in [3], instead of maximizing the eventual set of occupied positions, Magnus's goal was to minimize the set of occupied positions. From the results in [3], we only know approximately the size of the set of occupied positions if both players play optimally.

Returning to the maximal variant, in [2] the game was studied with an emphasis on finding algorithmic strategies for the players to achieve their goals in a minimal number of rounds. A simple formula in terms of the prime factorization of n was given in [2] for the size of the set of visited positions when both players play optimally. In this paper we give a simpler proof of the result.

Proposition 5. *The set of visited positions has size $\beta(n)$ when both players play optimally.*

Proof. Suppose U is a universal set containing the current position. Consider the following strategy for Derek. Given the current position i and a magnitude ℓ chosen by Magnus, Derek chooses a direction such that that the next position is also in U; this is possible as one of $x \pm \ell \pmod{n} \in U$ by the definition of a universal set. As any universal set may be translated to include the initial position 0, Derek can follow this strategy from the beginning of the game. Since the token never visits a position outside of U, at most $\beta(n)$ positions are visited irrespective of Magnus's strategy.

Conversely, consider the following strategy for Magnus. For each position j, Magnus maintains a counter k_j, initially set to 1. Given the current position i, Magnus chooses the value of k_j for the magnitude, and then updates $k_i \leftarrow k_i + 1 \pmod{\lfloor \frac{n}{2} \rfloor}$. In this manner, Magnus chooses a different magnitude (modulo $\lfloor \frac{n}{2} \rfloor$) each time the same position is visited.

Let S be the set of positions that are visited infinitely often in a continuous game. Since there are finitely many positions, the set S is non-empty. We claim that S is universal. Let $j \in S$. Since the token visits position j infinitely many times, Magnus chooses each magnitude $0 < \ell \leq \frac{n}{2}$ for position j infinitely many times. Consequently, one of $j \pm \ell \pmod{n}$ is visited infinitely many times, and so belongs to S. It follows that S is universal.

Therefore, $|S| \geq \beta(n)$, and since S is a subset of the set of visited positions, at least $\beta(n)$ positions are visited. □

Note that to achieve $\beta(n)$ both players need to know the smallest prime factor of n. When n has no small factors, this becomes equivalent to factoring n. A player that can factor n has a definite advantage over a player that cannot factor n. To our knowledge, this game is the first game in which playing well requires the ability to factor.

Acknowledgments

We are grateful to the following people and institutions for their advice, discussions and support: Valerie King, Nikola S. Nikolov, Uriel Feige, S. Muthu Muthukrishnan, Mario Szegedy and the DIMACS Center, Jeffrey O. Shallit and the School of Computer Science at the University of Waterloo, and Noam Sturmwind for editing assistance.

References

[1] N. Sloane. On line Encyclopedia of Sequences. http://www.research.att.com/ njas/sequences/

[2] Nedev, Zhivko and Muthukrishnan, S., *The Magnus-Derek Game*, Theoretical Computer Science, Volume 393, Issues 1-3, 20 March 2008, Pages 124-132.

[3] Nedev, Zhivko and Quas, Anthony, *Balanced sets and the vector game*, International Journal of Number Theory, 4 (2008), Pages 339-347.