Real Analysis Exchange
Vol. 29(2), 2003/2004, pp. 739–754

Liljana Babinkostova and Marion Scheepers*, Department of Mathematics, Boise State University, Boise, ID 83725.
email:liljanab@math.boisestate.edu, marion@math.boisestate.edu

AN INFINITE GAME ON GROUPS

Abstract

We consider an infinite game on a group G, defined relative to a subset A of G. The game is denoted $\mathsf{G}(G, A)$. The finite version of the game, introduced in [1], was inspired by an attack on the RSA cryptosystem as used in an implementation of SSL.

Besides identifying circumstances under which player TWO does not have a winning strategy, we show for the topological group of real numbers that if C is a set of real numbers having a selection property (*) introduced by Gerlits and Nagy, then for any interval J of positive length, TWO has a winning strategy in the game $\mathsf{G}(\mathbb{R}, J \cup C)$.

1 Introduction

Let $(G, +)$ be a group with identity element $\mathbf{o}$ and let A be a subset of G. We consider the following game, denoted $\mathsf{G}(G, A)$, between players ONE and TWO: In the first inning ONE first chooses a secret element $x \in G$. Then TWO chooses an element a_1 of G, and asks ONE if $x + a_1$ is an element of A. ONE answers truthfully by ϵ_1, where $\epsilon_1 = 1$ indicates "yes", while $\epsilon_1 = 0$ indicates "no". They play an inning per positive integer, thus constructing a sequence

$$x, a_1, \epsilon_1, a_2, \epsilon_2, \ldots, a_n, \epsilon_n, \ldots$$

and after these moves TWO selects an element $y \in G$. TWO wins the play

$$x, a_1, \epsilon_1, a_2, \epsilon_2, \ldots, y$$

if $x = y$. Else, ONE wins.

Key Words: Game, group, winning strategy, selection principle
Mathematical Reviews subject classification: 03E17,20F99,91A05
Received by the editors July 28, 2003
Communicated by: Krzysztof Chris Ciesielski
*Supported by NSF grant DMS 99 - 71282

The finite version of this game was introduced in [1]. The inspiration for this game is a chosen ciphertext attack against certain implementations of cryptographic tools using the RSA crypto-system. Our results show that the infinite version of the game played even on such a standard group as the real line with usual addition, is of independent interest. In particular, our results make use of ideas from the field of selection principles in mathematics, and from the set theory of the real line.

The paper is organized as follows. In Section 2 we study strategies for TWO for general groups. In section 3 we study strategies for TWO specifically on the real line. In the final section we make a few remarks, and pose two problems.

2 Strategies for TWO

A strategy for TWO is a function, ψ, which

1. has as domain the history of moves by ONE and known to TWO, and
2. during the finite innings prescribes TWO's responses to these partial histories, and
3. in the ω–th inning it prescribes TWO's selection y, based on the total history of the finite-numbered innings.

Thus a strategy for TWO is a function

$$\psi : {}^{<\omega}\{0,1\} \cup {}^{\omega}\{0,1\} \to G.$$

For subsets U and V of group G and element a of G we define:

- $a + U = \{a + u : u \in U\}$, $U + a = \{u + a : u \in U\}$,
- $U + V = \{u + v : u \in U \text{ and } v \in V\}$ and
- $-U = \{-u : u \in U\}$.

The set $a + U$ is said to be a *left translate* and $U + a$ is said to be a *right translate* of U in G. For a subgroup H of the group G the set $a + H$, $a \in G$, is said to be a *left coset of H in G*. Moreover, distinct left cosets of H in G are pairwise disjoint, and each left coset of H in G has cardinality $|H|$. Similarly, sets of the form $H + a$ are said to be *right cosets of H in G*, and similar remarks apply. Moreover, for each a in G there is a b in G such that $a + H = H + b$, and vice versa.

The following lemma implies that when we consider strategies for TWO in the game $G(G, A)$, we may assume that $\mathbf{o}$ is an element of A:

Lemma 1. *For a given subset A of the group $(G,+)$, and for any a in G the following are equivalent:*

1. *TWO has a winning strategy in $G(G,A)$.*
2. *TWO has a winning strategy in $G(G,A+a)$.*

PROOF. $\underline{1 \Rightarrow 2:}$ Let ψ be a winning strategy for TWO in the game $G(G,A)$, and define a strategy Γ for TWO in $G(G,A+a)$ so that for each σ in ${}^{<\omega}2$, $\Gamma(\sigma) = \psi(\sigma)+a$, and for each f in ${}^{\omega}2$, $\Gamma(f) = \psi(f)$. Then Γ is a winning strategy for TWO in $G(G,A+a)$.
$\underline{2 \Rightarrow 1:}$ Let Γ be a winning strategy for TWO in $G(G,A+a)$. Define a strategy ψ for TWO in $G(G,A)$ so that for each $\sigma \in {}^{<\omega}2$, $\psi(\sigma) = \Gamma(\sigma)-a$, and for each $f \in {}^{\omega}2$, $\psi(f) = \Gamma(f)$. Then ψ is a winning strategy for TWO in $G(G,A)$. □

We define the *translation number of U over V* as

$$\mathrm{transl}_V(U) = \min\{|X| : X \subset G \text{ and } U + X \supseteq V\}.$$

Thus if H is a subgroup of G, then $\mathrm{transl}_G(H) = |G/H|$ is the number of left cosets of H in G.

Theorem 2. *If A is a subset of G such that $transl_G(A) > \aleph_0$, then TWO does not have a winning strategy in the game $\mathsf{G}(G,A)$.*

PROOF. By Lemma 1 we may assume that $\mathbf{0}$ is in A. Let Ψ be a strategy for TWO. Put $C = \Psi[{}^{<\omega}\{0,1\}] \cup \{-\Psi(\underline{0})\}$ where $\underline{0}$ denotes the infinite constant sequence $(0,0,\dots,0,\dots)$. Since C is countable, the set $G\setminus(A-C)$ is nonempty. Choose $x \in G \setminus (A-C)$. Since $\Psi(\underline{0}) = \mathbf{o} - (-\Psi(\underline{0}))$, $\Psi(\underline{0})$ is an element of $A-C$, and so $x \neq \Psi(\underline{0})$.

Here is how ONE will defeat Ψ: ONE begins the game by choosing x. When TWO computes $\Psi(\emptyset) \in C$, ONE will answer $\epsilon_1 = 0$ because $x + \Psi(\emptyset) \in x + C \subset G \setminus A$. Then TWO will play $\Psi(0) \in C$, and once again $x + \Psi(0) \notin A$, so that once again ONE responds with $\epsilon_2 = 0$. TWO plays $\Psi(0,0) \in C$ and again by choice of x, $x + \Psi(0,0) \notin A$. Continuing in this way we see that the resulting play will be

$$x, \Psi(\emptyset), 0, \Psi(0), 0, \Psi(0,0), 0, \Psi(0,0,0), \dots, \Psi(\underline{0})$$

and since $x \neq \Psi(\underline{0})$, this play is lost by TWO. □

Theorem 3. *Let A be a subgroup of more than one element of the infinite group G. Then TWO has no winning strategy in $\mathsf{G}(G,A)$.*

PROOF. Let σ be a strategy for TWO. Consider any $x \in G$ and construct, using TWO's strategy σ, a σ-play:

$$x, \sigma(\emptyset), \epsilon_1, \sigma(\epsilon_1), \epsilon_2, \sigma(\epsilon_1, \epsilon_2), \epsilon_3, \dots$$

and put $f = (\epsilon_n : n < \infty)$. Consider $y = \sigma(f)$. If $y \neq x$, then TWO has lost this σ-play and we are done. Else, if $x = \sigma(f)$, then choose an $a \in A$ with $a \neq \mathbf{o}$ (A has more than one element). Put $X = a + x$. Then consider the play

$$X, \sigma(\emptyset), \delta_1, \sigma(\delta_1), \delta_2, \sigma(\delta_1, \delta_2), \delta_3, \dots$$

and put $g = (\delta_n : n < \infty)$. We claim that $g = f$.

This is done by induction. First, that $f(1) = g(1)$: Suppose $f(1) = 0$: Thus $x + \sigma(\emptyset) \notin A$, and as A is a subgroup of G also $a + x + \sigma(\emptyset) \notin A$; that is, $X + \sigma(\emptyset) \notin A$. This means also $g(1) = 0$. A similar argument shows that if $f(1) = 1$, then also $g(1) = 1$. Now suppose that $j > 1$ is given and we have verified that $f\lceil_j = g\lceil_j$[1]. For suppose $f(j) = \epsilon_j = 0$. Thus, $x + \sigma(f\lceil_j) \notin A$, and since A is a subgroup of G, also $X + \sigma(g\lceil_j) \notin A$, so that $\delta_j = 0$. Similarly, if $\epsilon_j = 1$, then also $\delta_j = 1$.

But then we find that TWO lost at least one of the σ-plays

$$X, \sigma(\emptyset), \delta_1, \sigma(\delta_1), \delta_2, \sigma(\delta_1, \delta_2), \delta_3, \dots$$

or

$$x, \sigma(\emptyset), \epsilon_1, \sigma(\epsilon_1), \epsilon_2, \sigma(\epsilon_1, \epsilon_2), \epsilon_3, \dots$$

This completes the proof. □

Next we examine some cases where TWO has a winning strategy.

Theorem 4. *If A is a one-element subset of the countable group G, then TWO has a winning strategy in the game $\mathsf{G}(G, A)$.*

PROOF. Write $A = \{a\}$ and let $(g_n : n < \infty)$ be an enumeration of G. TWO's strategy σ calls on TWO to play $\sigma(\emptyset) = g_1$. If ONE's response is "1", then TWO knows that $x + g_1 = a$ and so $x = a - g_1$. Suppose ONE's response is "0". TWO's strategy σ is to play, for any sequence τ of length n, say, of zeroes, the point $\sigma(\tau) = g_{n+1}$. If ONE answers with a "1" in inning $n + 1$, then TWO knows that $x + g_{n+1} = a$; that is,

$$x + \sigma(\overbrace{0, \dots, 0}^{n \text{ zeroes}}) = a$$

[1]For a sequence $(\epsilon_n : n < \infty)$ and $j < \infty$, the notation $(\epsilon_n : n < \infty)\lceil_j$ denotes $(\epsilon_n : n \leq j)$.

and so TWO knows x already in this inning. It is evident that TWO discovers the value of ONE's x in some finite-numbered inning. □

Observe that Theorem 4 shows that it is necessary in the hypotheses of Theorem 3 to assume that the subgroup A has at least two elements. For if A is the subgroup $\{\mathbf{o}\}$, and G is countable, then TWO has a winning strategy in $\mathsf{G}(G, A)$.

Theorem 5. *Let $(G, +, e_G)$ be an infinite group with subsets H and B such that:*

1. *H is a countable subgroup of G;*
2. *TWO has a winning strategy in the game $\mathsf{G}(G, B)$;*
3. *$B \cap H = \emptyset$;*
4. *$(\exists b \in B)((H + b) \cap B = \{b\})$;*
5. *$(\exists h \in H)((h + B) \cap B = \emptyset)$.*

Then TWO has a winning strategy in $\mathsf{G}(G, B \cup H)$.

Proof. Once and for all choose elements $h \in H$ and $b \in B$ as in hypotheses 4 and 5. Also, fix a strategy τ for TWO in the game $\mathsf{G}(G, B)$ as in hypothesis 2, and fix a bijective enumeration $(h_n : n < \infty)$ of H as in hypothesis 1. Define $A := B \cup H$. We will now define a strategy σ for TWO in the game $\mathsf{G}(G, A)$.

To begin, TWO plays $\sigma(\emptyset) = \tau(\emptyset)$, and for every finite sequence $(0, \ldots, 0)$ of zeroes, define $\sigma(0, \ldots, 0) = \tau(0, \ldots, 0)$. Consider a binary sequence which has exactly one "1" in it, of the form $(0, \ldots, 0, 1)$. Intuitively, this sequence occurs when TWO has played $\sigma(0, \ldots, 0)$ and ONE answered with a "1" because $y = x + \sigma(0, \ldots, 0) \in A$, and TWO must now respond to this information. How TWO proceeds from here depends on whether $y \in H$ or $y \in B$. TWO's next move is to first determine which of these two situations is the case. We will call the following analysis the "identification step". Define

$$\sigma(0, \ldots, 0, 1) = \sigma(0, \ldots, 0) + h.$$

Case 1: ONE responds with a "1": Then, as we now have $y+h \in A$ and $y \in A$, we find by the choice of h that indeed $y \in H$.
Now TWO's strategy will be to identify which element of H is y. Define

$$\sigma(0, \ldots, 0, 1, 1) = \sigma(0, \ldots, 0) - h_1 + b.$$

If now ONE responds with a "1", then $x+\sigma(0,\dots,0,1,1) = x+\sigma(0,\dots,0) - h_1 + b$ is in A. By the choice of b this is $\{b\}$, and so TWO discovers that $y = h_1$, and the game is over. Else, ONE responds with a "0", and so TWO responds with

$$\sigma(0,\dots,0,1,1,0) = \sigma(0,\dots,0) - h_2 + b.$$

and the same considerations apply. If ONE replies with a "1", then TWO concludes that $x + \sigma(0,\dots,0) = h_2$. Else, TWO plays

$$\sigma(0,\dots,0,1,1,0,0) = \sigma(0,\dots,0) - h_3 + b.$$

and so on. After a finite number of such innings TWO discovers the value of x.

Case 2: ONE responds with a "0": Then we know that $y \in B$ since $y \in A$ but $y \notin H$, and H is closed under addition.
Now TWO's strategy will be to simulate $\mathsf{G}(G,B)$. In particular, TWO plays

$$\sigma(0,\dots,0,1,0) = \tau(0,\dots,0,1).$$

While ONE responds with "0"'s, TWO continues following the strategy τ - thus, for a finite sequence $(0,0,\dots,0)$ of zeroes, TWO will respond with

$$\sigma(0,\dots,0,1,0,0,\dots,0) = \tau(0,\dots,0,1,0,\dots,0).$$

Should at some point ONE respond again with a "1", then TWO knows that $y = x + \sigma(0,\dots,0,1,0,0,\dots,0) \in A$, and then TWO again follows the plan to identify if $y \in H$ or if $y \in B$. If $y \in H$, then proceed as in Case 1. Else, if $y \in B$, then continue using the strategy of Case 2.

To see that σ is a winning strategy for TWO, consider a σ-play. If ever Case 1 occurred, then within finitely many moves from this occurrence TWO identifies x by identifying the appropriate element of H. If Case 1 never occurred, then σ was, except for the identification steps which might occur, essentially the strategy τ for the game $\mathsf{G}(G,B)$, and the entire play is a legitimate play of this game. Thus, TWO used τ in this case to identify x. □

3 Playing on $\mathbb{R}$

Consider the game on the group of real numbers under addition. In the proof below we will use the following notation: $\mathsf{cov}(\mathcal{M})$ denotes the minimal cardinality of a collection of first category subsets of the real line whose union is equal to $\mathbb{R}$. $\mathsf{cov}(\mathcal{N})$ denotes the minimal cardinality of a family of Lebesgue measure zero subsets of the real line whose union is $\mathbb{R}$. This notation is common in set theory. It is well known that both the cardinals $\mathsf{cov}(\mathcal{M})$ and $\mathsf{cov}(\mathcal{N})$ are uncountable.

Corollary 6. *If A is a first category subset or a Lebesgue measure zero subset of $\mathbb{R}$, then TWO has no winning strategy in the game $\mathsf{G}((\mathbb{R},+,0),A)$.*

Proof. It is evident that if A is a first category set, then $\mathsf{cov}(\mathcal{M}) \leq transl_{\mathbb{R}}(A)$, and if A has Lebesgue measure zero, then $\mathsf{cov}(\mathcal{N}) \leq transl_{\mathbb{R}}(A)$. Thus the set A satisfies the conditions of Theorem 2, so TWO has no winning strategy. □

Thus, if TWO has a winning strategy in $\mathsf{G}(\mathbb{R},A)$, then A is "large". We now identify some examples of such subsets A. First we consider intervals.

Specialized attacks by TWO

Let A be an interval in $\mathbb{R}$ and a proper subset of $\mathbb{R}$. The following two types of attack by TWO, depending on which of two situations exists in the inning of the play of the game in progress, seem to be fundamental in this example. Assume that at some stage TWO has played an a and ONE responded with 1: Thus $x+a$ is in A. TWO chooses a nonzero δ with $|\delta| < \frac{1}{2}$ and proposes $a_1 = a+\delta$:

Entry attacks with δ.

If ONE responds with 0 to a_1: In this case TWO launches an "entry attack with δ": We know that:

1. $x+a_1 \notin A$ since ONE responded with 0;
2. $x+a_1$ is within $|\delta|$ from a known endpoint c of A.

TWO puts $\delta_1 = \frac{1}{2}\cdot\delta$, and proposes $a_2 = a_1 - \delta_1$. If still ONE responds with 0, TWO puts $\delta_2 = \frac{1}{2}\cdot\delta_1$, and proposes $a_3 = a_2 - \delta_2$. This attack from above continues as long as ONE responds with 0: At stage $n+1$, after ONE responded with 0, TWO puts $\delta_n = \frac{1}{2}\cdot\delta_{n-1}$, and proposes $a_{n+1} = a_n - \delta_n$. Observe that $x+a_n$ converges to c.

Exit attacks with δ.

If ONE responds with 1 to a_1: In this case TWO launches an "exit attack with δ": Let c be an endpoint of A. If $x+a_1 < c$, put $\delta_1 = |\delta|$, and else put $\delta_1 = -|\delta|$. Next TWO proposes $a_2 = a_1+\delta_1$. If ONE still responds with 1, TWO proposes $a_3 = a_2+\delta_1$. This exit attack with δ continues as long as ONE responds with 1: At stage $n+1$, after ONE responded with 1, the attacker proposes $a_{n+1} = a_n+\delta_1$. Observe that since the real line has the Archimedean property, after a finite number m of steps in an exit attack, ONE will answer with 0, and then we know that $x+a_m$ is within δ_1 from c.

It is important to keep in mind that in results given below that even if TWO uses only rational numbers δ during entry or exit attacks, TWO still has the corresponding winning strategy. Though using rational values of δ is not required for some of our results, it is actually important to use only rational values in the proof of Theorem 11 below.

Theorem 7. *For $a < b$, if A is any of (a,b), [a,b), (a,b] or [a,b], then TWO has a winning strategy in $\mathsf{G}(\mathbb{R}, A)$.*

PROOF. We describe the strategy for $A = [a, b]$. The same strategy works also for the other cases. Enumerate the set of rational numbers $\mathbb{Q}$ bijectively as $(q_n : n \in \mathbb{N})$. Here is, intuitively, TWO's strategy: After ONE has selected x, TWO successively chooses $a_1 = q_1, \ldots, a_n = q_n$, until an n occurs where $x + q_n \in A$. This happens because A has nonempty interior, and $x + \mathbb{Q}$ is dense in $\mathbb{R}$.

TWO continues as follows: Pick a positive $\delta_1 < \frac{b-a}{2}$ and launch an exit attack with δ_1: That is, play $a_{n+1} = a_n + \delta_1, \ldots, a_m = a_{m-1} + \delta_1$ and so on, until an m is reached in this attack where ONE answers with a 0. Then we know $x + a_m > b$ and $x + a_m$ is within δ_1 from b. Then TWO launches an entry attack with δ_1. There are two possibilities:
Case 1: ONE never answers with 1: Then for all k we have $x + a_{m+k} > b$, and indeed,

$$|b - (x + a_{m+k})| < \delta_1 - (\sum_{j=2}^{k} \delta_j) = \delta_1 \cdot (1 - \sum_{j=2}^{k} (\frac{1}{2})^{(j-1)}).$$

Thus we have $\lim_{k\to\infty}(x + a_k) = b$, and so TWO wins by giving as final move $y = \lim_{k\to\infty}(b - a_k)$.
Case 2: ONE answers with a 1: Then we know that $x + a_m < b$ and also $|b - (x + a_m)| < \delta_m$. Put $\delta_{m+1} = \frac{1}{2} \cdot \delta_m$, and launch an exit attack with δ_{m+1}. At a step p, a finite number of steps later, ONE answers with a 0, and then we know that $|b - (x + a_p)| < \delta_{m+1}$, and also that $b < x + a_p$. Then launch an entry attack with δ_{m+1}.

This strategy is winning for TWO. We only need to discuss the case when TWO follows the strategy and infinitely often launches an entry attack during the course of the game. Let the innings in which entry attacks start be numbered as $k_1 < k_2 < \cdots < k_n < \ldots$. Every time an entry attack starts we have a value of δ with which the attack is launched. Let the δ used during the entry attack starting in inning k_n be denoted δ_n. For each n note that $\delta_{n+1} < \frac{1}{2} \cdot \delta_n$, and $|b - (x + a_{k_n})| < \delta_n$. Thus we have

$$b = \lim_{n\to\infty} (x + a_{k_n})$$

and TWO's last move is $y = \lim_{n\to\infty}(b - a_{k_n})$. □

Next consider the infinite intervals.

Theorem 8. *Suppose A is one of $[a,\infty)$, (a,∞) $(-\infty,a)$ or $(-\infty,a]$. Then TWO has a winning strategy in the game $\mathsf{G}(\mathbb{R},A)$.*

PROOF. We give a description when $A = [a,\infty)$. The other cases are similar. TWO's strategy is in the beginning to play positive integers n (in inning n) until ONE responds with $\epsilon_n = 1$, meaning $a \le x + n$. Then TWO launches an exit attack with $(-\frac{1}{2})$ as follows: For the next innings TWO plays $n-1\cdot\frac{1}{2},\dots,n-j\cdot\frac{1}{2},\dots$ until a j_1 is reached where ONE responds with a "0". Then TWO knows that $a - \frac{1}{2} \le x + n - j_1\cdot\frac{1}{2} < a$. Then TWO launches an entry attack with $\frac{1}{2}$ and plays $n-j_1\cdot\frac{1}{2}+\frac{1}{2^2}, n-j_1\cdot\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3},\dots$ until a j_2 is reached where ONE answers again with a "1" to $x+n-j_1\cdot\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\cdots+\frac{1}{2^{j_2}}$. Then TWO knows that $a \le x+n-j\cdot\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\cdots+\frac{1}{2^{j_2}} < a+\frac{1}{2^{j_2}}$. Then TWO launches an exit attack with $\frac{1}{2^{j_2}}$, and so on. In this way TWO builds a convergent sequence of form $x + a_j$ which converges to a, and so TWO learns that $x = \lim_{j\to\infty}(a - a_j)$. □

And next we consider unions of intervals. For this one considers another game defined as follows for a group G: Finitely many disjoint subsets $I_1,\dots,I_k$ are given. ONE chooses a secret element x in one of these. TWO must discover in a finite number of moves in which set I_j the secret element x is. TWO may propose elements a from G and ONE must answer truthfully whether $x + a$ is in $\cup_{i\le k} I_i$. Let this game be denoted by $\mathsf{G}_2(G,\{I_i : i \le k\})$.

Lemma 9. *Let k be a positive integer and let $I_1,\dots,I_{k+1}$ be disjoint bounded intervals in $\mathbb{R}$. Then TWO has a winning strategy in $\mathsf{G}_2(\mathbb{R},\{I_i : i \le k+1\})$ which wins in $\le k$ innings.*

PROOF. We prove by induction on k.
Case 1: k = 1 Let intervals I_1 and I_2 be given and suppose $I_1 < I_2$. Also suppose $i_1 = length(I_1)$, $i_2 = length(I_2)$ and d is the distance between I_1 and I_2. If $i_1 \le i_2$ TWO asks if $x + i_2 + d \in I_1 \cup I_2$. If ONE answers "yes" then TWO knows that $x \in I_1$, and if ONE answers "no" then TWO knows that $x \in I_2$. If instead $i_2 < i_1$ then ask if $x - i_1 - d \in I_1 \cup I_2$. Again, "yes" means $x \in I_2$ and "no" means $x \in I_1$. Thus TWO wins in the first inning.
Case 2: $k > 1$ and the theorem holds below k: Thus $k = j + 1$ and $j \ge 1$, and we know that for any $j + 1$ disjoint bounded intervals $I_1,\dots,I_{j+1}$ TWO has a winning strategy in this game which wins in $\le j$ innings.

Consider $k + 1 = j + 2$ pairwise disjoint bounded intervals enumerated bijectively as $I_1,\dots,I_{j+2}$ such that $I_m < I_n$ if, and only if, $m < n$. Let i_m be

the length of I_m, and let d_m be the distance between I_m and I_{m+1}, $m < j+2$. If $i_1 < i_{j+2}$ then TWO asks ONE if $x + (d_1 + \cdots + d_{j+1}) + (i_2 + \cdots + i_{j+2}) \in I_1 \cup \cdots \cup I_{j+2}$. If the answer is "yes", then TWO knows $x \in I_1$, and else TWO knows $x \in (I_2 \cup \cdots \cup I_{j+2})$, and we are in the case of $j+1$ intervals. Now TWO applies the strategy for determining in at most j innings in which of $j+1$ intervals x is. Thus, TWO finds the interval containing x in at most $j+1$ innings. □

Theorem 10. *Let k be a positive integer and let $I_1, \ldots, I_k$ be disjoint bounded intervals in $\mathbb{R}$. Then TWO has a winning strategy in $\mathsf{G}(\mathbb{R}, \cup_{i \leq k} I_i)$.*

PROOF. Put $A = \cup_{i \leq k} I_i$, and assume that the I_i's have been enumerated so that $i < j$ implies that $I_i < I_j$. For each i let d_i be the distance between I_i and I_{i+1}.

Let ONE choose a secret $x \in \mathbb{R}$. Now TWO starts as follows: First, choose a rational number a such that $y = x + a \in A$. Such a rational number is found in a finite number of steps, as before. TWO uses a winning strategy for the game $\mathsf{G}_2(\mathbb{R}, \{I_j : j \leq k\})$ to determine in a finite number of steps (indeed, at most $k-1$ steps) to which I_i the point y belongs. Put $\delta_1 = \frac{\min\{d_{i-1}, d_i\}}{2}$. Now TWO launches an exit attack in the game $\mathsf{G}(\mathbb{R}, I_i)$ with δ_1. When ONE responds with a "1", TWO knows a j_1 such that $x + a + j_1 \cdot \delta_1$ is within δ_1 from an endpoint of I_i. Then TWO launches an entry attack with $\delta_2 = \frac{\delta_1}{2}$ and this proceeds until either all innings have elapsed, or else until ONE answers with a "1", and so on. One can show that in this way TWO constructs a sequence $x + a_n, n < \infty$ which converges to an endpoint of I_i, and thus TWO in the end discovers the value of x. □

Combining Theorems 5 and 7 or 10 we find for each finite set $\{I_1, \ldots, I_n\}$ of bounded intervals of positive length and with $0 \notin \cup_{j \leq n} I_j$, there is a large enough positive integer k such that TWO has a winning strategy in the game $\mathsf{G}(\mathbb{R}, (\cup_{j \leq n} I_j) \cup k \cdot \mathbb{Z})$, where $k \cdot \mathbb{Z}$ is the subgroup $\{k \cdot n : n \in \mathbb{Z}\}$ of the additive group of integers.

But we can do a little better than this. Finally, we consider the union of an interval with a small set of real numbers. For a set C of real numbers let $vect_{\mathbb{Q}}(C)$ denote the rational vector space generated by C. It contains the subgroup $\langle C \rangle$ of $\mathbb{R}$ generated by C. For convenience let us say that a subset C of the real line is *algebraically small* if for each interval J of positive length, and for any countable set F of real numbers, $J \setminus vect_{\mathbb{Q}}(C \cup F) \neq \emptyset$. Observe that the property of being algebraically small is hereditary; each subset of an algebraically small set of reals is algebraically small. But a union of two algebraically small sets need not be algebraically small. For let B be a basis

for $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Partition B into two disjoint sets B_1 and B_2 with $|B_1| = |B_2|$. Then B_1 and B_2 are algebraically small, but B is not algebraically small.

Theorem 11. *Let C be an algebraically small set of real numbers. Then for any interval J of positive length, TWO has a winning strategy in the game $\mathsf{G}(\mathbb{R}, J \cup C)$.*

PROOF. Put $A = J \cup C$ where J is an interval of nonzero finite length. Let $(I_n : n < \infty)$ be a bijective enumeration of the open intervals with rational endpoints. Choose real numbers $r_1, \ldots, r_n, \ldots, n < \infty$ so that $r_1 \in I_1 \setminus vect_{\mathbb{Q}}(C \cup \{1\})$ and for each n also $r_{n+1} \in I_{n+1} \setminus (vect_{\mathbb{Q}}(C \cup \{1, r_1, \ldots, r_n\})$. Then the set $\{r_n : n < \infty\}$ is dense in $\mathbb{R}$. Consequently for each $x \in \mathbb{R}$ and for each n the set $\{x + r_j : j > n\}$ is dense in $\mathbb{R}$ and thus has nonempty intersection with J, a subset of A. By the construction we have:

1. For any $x \in \mathbb{R}$ and for any $u \neq v$ in $\{x + r_n : n < \infty\}$, $u - v \notin vect_{\mathbb{Q}}(C \cup \{1\})$: For suppose that $(x + r_i) - (x + r_j) = r_i - r_j$ is a member of $vect_{\mathbb{Q}}(C \cup \{1\})$. Without loss of generality $i < j$. Then it is a member of $vect_{\mathbb{Q}}(C \cup \{1, r_1, \ldots, r_i\})$, and so $r_j = r_i - (r_i - r_j)$ is a member of $vect_{\mathbb{Q}}(C \cup \{1, r_1, \ldots, r_i\})$, contradicting the choice of r_j.
2. Thus, for each $x \in \mathbb{R}$, $|\{x + r_n : n < \infty\} \cap vect_{\mathbb{Q}}(C \cup \{1\})| \leq 1$.

TWO's strategy has two stages, as follows:
Stage 1: Select $r_1, \ldots, r_k$ until $n_0 < n_1 < n_2 < n_3 < n_4 < n_5$ have been found such that ONE answered "1" to each of the moves $r_{n_0}, r_{n_1}, r_{n_2}, r_{n_3}, r_{n_4}$ and r_{n_5} by TWO. This happens because for each n the set $\{x + r_j : j > n\}$ is dense in $\mathbb{R}$. So, each of $x + r_{n_0}$, $x + r_{n_1}$, $x + r_{n_2}$, $x + r_{n_3}$, $x + r_{n_4}$ and $x + r_{n_5}$ is in A. We may assume without loss of generality that $r_{n_0} < r_{n_1} < r_{n_2} < r_{n_3} < r_{n_4} < r_{n_5}$. Observe that among these $x + r_{n_0}$ might be in $C \setminus J$, and $x + r_{n_1}$ and $x + r_{n_5}$ might be endpoints of J. Thus by 2 above each of $x + r_{n_2}$, $x + r_{n_3}$ and $x + r_{n_4}$ is in the interior of the interval J. One, but not two, of these points might be in C. Indeed, by item 2 above again, all rational translates of at least two of them are not in $vect_{\mathbb{Q}}(C \cup \{1\})$.

Thus, by the end of Stage 1 TWO is in possession of three points, $u < v < w$, such that

- Each of $x + u$, $x + v$ and $x + w$ is in the interior of J;
- At most one of these points is in C;
- For at least two of these points, all rational translates of these points are outside $vect_{\mathbb{Q}}(C \cup \{1\})$, and thus outside C.

Note that TWO does not know which two points have the property in the third remark.

Stage 2: For the two points whose rational translates are all outside C, TWO's entry and exit attacks in the game $G(\mathbb{R}, A)$ using only rational values of δ are exactly entry and exit attacks in the game $G(\mathbb{R}, J)$. Note that an exit attack in $G(\mathbb{R}, J)$ using some $\delta < length(J)$ will result answering with a "0" within at most $m_\delta = \frac{length(J)}{\delta} + 1$ innings.

TWO now plays as follows: TWO pretends to be playing $G(\mathbb{R}, J)$ instead of $G(\mathbb{R}, A)$ on three different "boards" against three different player ONE's. The boards are the "u"-board, the "v"-board and the "w"-board. We are assuming that the three player ONE's have started the game by choosing the same secret x in each of the games, and that the player ONE of each of the three boards answers correctly for the game $G(\mathbb{R}, A)$ on that board. Moreover, in all entry- and exit- attacks player TWO uses only rational values of the number δ used during the attack. On two of the boards, even though ONE thinks he is answering for $G(\mathbb{R}, A)$, he is really answering for moves of $G(\mathbb{R}, J)$, since the rational translates of the points from $\{u, v, w\}$ for these two boards are disjoint from C.

If on some board, say board u, an exit attack lasts longer than $m_\delta = \frac{length(J)}{\delta} + 1$ steps before ONE answers with a "0", then TWO knows that u is in C, and abandons the game on that board and continues on only one of the remaining boards. The game on the continuation board is $G(\mathbb{R}, J)$, and TWO follows a winning strategy on it as in Theorem 7, and so discovers x.

Thus we may assume that on all three boards exit attacks are shorter than m_δ, and thus that TWO continues play on all three boards. Since on two of the boards the game $G(\mathbb{R}, A)$ has been reduced to $G(\mathbb{R}, J)$, and since TWO is following a winning strategy for $G(\mathbb{R}, J)$ on all three boards, TWO will win on two of the three boards by discovering the correct value of x on these two boards. Thus, TWO will win the original game $G(\mathbb{R}, A)$ by simply announcing the majority value (namely x) revealed by the strategies for these three games. □

There are several ways of implementing these ideas as a single strategy for TWO in $G(\mathbb{R}, A)$: TWO could for example pace moves so that when the inning number is n and $j = n \mod 3$, and $k = \frac{n-j}{3}$, then TWO makes the k-th move of the game on the u-board if $j = 0$, the v-board if $j = 1$ and the w-board if $j = 2$.

Corollary 12. *Let C be a set of real numbers of cardinality less than $2^{\aleph_0}$. Then for any interval J of positive length TWO has a winning strategy in the game $\mathsf{G}(\mathbb{R}, J \cup C)$.*

PROOF. A set of real numbers of cardinality less than $2^{\aleph_0}$ is algebraically small. □

Algebraically small sets of real numbers may be of large cardinality. For example a Hamel basis B for the set of real numbers considered as a vector space over the field $\mathbb{Q}$ has cardinality $2^{\aleph_0}$, and if we consider any subset C of B such that $B \setminus C$ is uncountable, then C is algebraically small. But such such C's can have cardinality $2^{\aleph_0}$.

As another example, recall that a cover $\mathcal{U}$ for a topological space X is said to be

1. an ω-cover if it is an open cover such that $X \notin \mathcal{U}$, and for each finite subset $F \subset X$ there is a $U \in \mathcal{U}$ with $F \subseteq U$;
2. a γ-cover if it is an open cover, is infinite, and each element of X is in all but finitely many elements of $\mathcal{U}$;
3. a γ-groupable cover if there is a partition $\mathcal{U} = \cup_{n<\infty}\mathcal{F}_n$ where for each n $\mathcal{F}_n$ is finite, and for each $x \in X$, for all but finitely many n we have $x \in \cup\mathcal{F}_n$.

The symbol Ω denotes the collection of ω-covers of a space, and Γ denotes the collection of γ-covers of the space. The symbol $\mathcal{O}$ denotes the collection of open covers, and $\mathcal{O}^{\gamma-gp}$ denotes the collection of γ-groupable open covers of the space.

For families $\mathcal{A}$ and $\mathcal{B}$ of sets of subsets of the set S the symbol $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ denotes the statement that there is for each sequence $(A_n : n < \infty)$ of elements of $\mathcal{A}$ a sequence $(B_n : n < \infty)$ such that for each n we have $B_n \in A_n$ and $\{B_n : n < \infty\} \in \mathcal{B}$. $\mathsf{S}_1(\mathcal{A},\mathcal{B})$ is an example of a selection principle.

The selection principle $\mathsf{S}_1(\mathcal{O},\mathcal{O})$ was introduced by Rothberger in [7], and is sometimes called Rothberger's property. The selection principle $\mathsf{S}_1(\Omega,\Gamma)$ was introduced in [4]; according to Gerlits and Nagy a set C of real numbers with the property $\mathsf{S}_1(\Omega,\Gamma)$ is said to be a γ-set.

Corollary 13. *If C is a set of real numbers with property $\mathsf{S}_1(\Omega,\mathcal{O}^{\gamma-gp})$, then for each interval J of positive length TWO has a winning strategy in $\mathsf{G}(\mathbb{R}, J \cup C)$.*

PROOF. Suppose that G has properties $\mathsf{S}_1(\Omega,\mathcal{O}^{\gamma-gp})$. Then $\mathbb{Q}\cdot G$, a countable union of sets with this property, also has this property. But then by [9] all finite products of such sets have Rothberger's property $\mathsf{S}_1(\mathcal{O},\mathcal{O})$. Since addition is a uniformly continuous function it follows that the rational vector space generated by a set of reals with property $\mathsf{S}_1(\mathcal{O},\mathcal{O})$ is algebraically small. □

4 Remarks

In [3] Galvin and Miller showed that Martin's Axiom (indeed, $\mathfrak{p} = \mathfrak{c}$) implies that there is a γ-set C of real numbers such that $|C| = |\mathbb{R}| = 2^{\aleph_0}$. The selection principle $\mathsf{S}_1(\Gamma, \Gamma)$ was introduced in [8], and $\mathsf{S}_1(\Omega, \Gamma)$ implies both $\mathsf{S}_1(\Gamma, \Gamma)$ and $\mathsf{S}_1(\mathcal{O}, \mathcal{O})$.

In [6] it was shown that a property denoted (*) in [4] is equivalent to the property $\mathsf{S}_1(\Omega, \mathcal{O}^{\gamma-gp})$. Results of [6] imply that if a space is member of both $\mathsf{S}_1(\Gamma, \Gamma)$ and of $\mathsf{S}_1(\mathcal{O}, \mathcal{O})$, then it has property $\mathsf{S}_1(\Omega, \mathcal{O}^{\gamma-gp})$.

If we let C be a γ-set of cardinality $2^{\aleph_0}$, then for each interval J of positive length TWO has a winning strategy in $\mathsf{G}(\mathbb{R}, J \cup C)$, and yet TWO has no winning strategy in the game $\mathsf{G}(\mathbb{R}, C)$ since C has Lebesgue measure zero. Thus even if TWO has a winning strategy in $\mathsf{G}(G, A)$, there may yet be a subset B of A such that TWO has no winning strategy in $\mathsf{G}(G, B)$. Let A be the union of an interval of positive length and the group $\mathbb{Z}$, and let B be the group of the integers, and apply Theorem 3 or Theorem 2. It also illustrates that a set on which TWO does not have a winning strategy may be extendible to one on which TWO does have a winning strategy.

By generalizing some of the arguments one can generalize Theorem 7 to: If A is comeager in an interval [a,b] and if there is a countable dense set C such that $\mathbb{R} = A + C$, then TWO has a winning strategy in $\mathsf{G}(\mathbb{R}, A)$.

Also Theorem 11 can be generalized to the statement that if $I_1, \ldots, I_n$ are intervals of real numbers, each of positive length, and if C is algebraically small, then TWO has a winning strategy in the game $\mathsf{G}(\mathbb{R}, (\cup_{j \leq n} I_j) \cup C)$.

Theorem 7 can also be generalized in a different direction. For an $n > 1$ consider this game on $\mathbb{R}^n$, with $A = \Pi_{j=1}^n I_j$ where for each j we have a bounded interval I_j of positive length. Then TWO has a winning strategy in $\mathsf{G}(\mathbb{R}^n, A)$.

The most general open problem for the additive group of reals seems to be:

Problem 1. *Characterize the members of the set*

$$\{A \subset \mathbb{R} : \text{ TWO has a winning strategy in } \mathsf{G}(\mathbb{R}, A)\}.$$

A more specific problem that we have not solved is:

Problem 2. *Characterize the members of the set of $A \subset \mathbb{R}$ such that: For each proper interval J of positive length TWO has a winning strategy in $\mathsf{G}(\mathbb{R}, J \cup A)$.*

This set includes all sets having property $(*)$, and no intervals of infinite length (since the real line is a union of two such intervals).

References

[1] L. Babinkostova and M. Scheepers, *A game on groups and information security*, Proceedings of the Third International Conference for Informatics and Information Technologies - 2002, to appear.

[2] J. A. Gallian, *Contemporary Abstract Algebra* 4th edition, Houghton Mifflin Company, 1998.

[3] F. Galvin and A. W. Miller, *On γ-sets and other singular sets of real numbers*, Topology and its Applications, **17** (1984), 145–155.

[4] Gerlits and Nagy, *Some properties of C(X), I*, Topology and its Applications, **14** (1982), 151–161.

[5] W. Just, A. W. Miller, M. Scheepers and P. J. Szeptycki, *The Combinatorics of open covers (II)*, Topology and its Applications, **73** (1996), 241–266.

[6] A. Nowik, M. Scheepers and T. Weiss, *The algebraic sum of sets of real numbers with strong measure zero sets*, The Journal of Symbolic Logic, **63** (1998), 301–324.

[7] F. Rothberger, *Eine Verschärfung der Eigenschaft* C, Fundamenta Mathematicae, **30** (1938), 50–55.

[8] M. Scheepers, *Combinatorics of open covers (I): Ramsey Theory*, Topology and its Applications, **69** (1996), 31–62.

[9] T. Weiss, *On finite products of special sets of real numbers*, preprint.