Carromboard Puzzle

Yuval Filmus

September 2009

1 Introduction

In this note we consider generalizations of the one-player game analyzed in Dijkstra's note EWD1211a. We quote Dijkstra's description of the game:

> There is a table with four coins in the positions north, east, south and west, and the player's goal is to get them all in the same orientation, i.e. all heads or all tails. The player never sees the coins but will be informed as soon as he has reached his goal. A move consists of the player mentioning one or more positions in which the coins will then be turned over; the complication is that, prior to each move, the table is rotated by a multiple of 90°; the multiple remains unknown to the player and may vary from move to move.

At the outset, it is not at all clear that there is some deterministic algorithm that solves this problem. However, such an algorithm exists, and is in fact very simple. We will need three types of moves:

- C (corner): mention one of the corners.
- AD (adjacent): mention two adjacent corners.
- NA (non-adjacent): mention two non-adjacent corners.

The algorithm is the following:

NA, AD, NA, C, NA, AD, NA

We'll let the reader check the correctness of the algorithm. It is also the only one possible using only seven moves, if we disregard moves mentioning

more than two corners (those are always equivalent to moves mentioning less than two corners).

Dijkstra generalizes the algorithm by considering a table with any given number of edges. We further generalize the game by considering any given Abelian group for the set of orientations. The main result is a description of all minimal solutions for p^n sides and p orientations, for prime p.

In general, everything would be easier to state if the goal would be to reach some fixed set of orientations. In section 6 we show that these two variants are really the same.

2 Definition and basic results

We now formally define the game and its solutions.

Definition 2.1. *Let $n \in \mathbb{N}$ and S be some finite Abelian group. The game $G(n, S)$ is defined implicitly by its solutions as follows.*

A move sequence *for $G(n, S)$ is any finite sequence σ of elements in S^n.*

A realization *of a move sequence σ is another sequence r where each r_i is some rotation of σ_i.*

We denote by $\sum r$ the sequence of partial sums of a realization, including the empty sum.

A move sequence σ is a solution *of $G(n, S)$ if for any rotation r and any $x \in S^n$, there is some index t such that $x + (\sum r)_t$ equals the zero vector. Equivalently, for any $x \in S^n$ there is some index t such that $(\sum r)_t = x$.*

The notation $G(n, m)$ will refer to the game $G(n, \mathbb{Z}_m)$.

There is a simple bound on the length of any solution.

Theorem 2.2. *Any solution of $G(n, S)$ has size at least $S^n - 1$.*

Proof. Take any solution and some realization of it. By definition, the sequence of partial sums must contain any possible vector in S^n. Therefore its length must be at least $S^n - 1$ (recall we allow the empty sum). □

This prompts a definition.

Definition 2.3. *A solution is $G(n, S)$ is* minimal *if its size is exactly $S^n - 1$.*

It turns out that every solvable instance of the game is in fact minimally solvable, as we will see in section 3.

There is a dual property satisfied by minimal solutions.

Lemma 2.4. *A move sequence for $G(n, S)$ of length $|S|^n - 1$ is a minimal solution iff no realization of any non-empty subsequence of it can sum to zero. Put differently, in any realization, no non-empty subsequence sums to zero.*

Proof. By definition, a move sequence is a solution iff the partial sums of any realization cover the set S^n. In fact, since there are $|S|^n$ partial sums, the condition of covering all of $|S|^n$ is equivalent to not covering any element more than once. This is equivalent for having no subsequence summing to zero. □

Some cases are trivially solvable.

Theorem 2.5. *The game $G(n, 1)$ is minimally solved by the empty sequence.*

The game $G(1, S)$ is solvable. The minimal solutions are $\sigma_i = \pi_i - \pi_{i-1}$ for all permutations π of S starting with the zero element.

Proof. The statement about $G(n, 1)$ is trivial.

Next, consider any minimal move sequence for $G(1, S)$. It has only one realization so it forms a solution iff its sequence of partial sums is a permutation of S, which must start with the zero element. □

There is a simple unsolvable case.

Lemma 2.6. *If $p \neq q$ are different primes, then $G(p, q)$ is unsolvable.*

Proof. Consider any solution σ of $G(p, q)$. We can assume that the last move is essential in the sense that if we remove it, we no longer get a solution. Hence there is some realization r in which $x = (\sum r)_i$ does not appear earlier in the sequence of partial sums. This implies that the last move in the sequence must be rotation-invariant, i.e. of the form c^p. Since $p > 1$, not all moves can be rotation-invariant. Choose the last move σ_j which isn't.

Consider next some other realization r' where only r'_j is different. For $k \geq j$ we have $(\sum r')_k = (\sum r)_k + (r'_j - r_j)$. Now x must appear among those $(\sum r')_k$, suppose $x = (\sum r')_l$. Since all further states were rotation-invariant, $x - (\sum r')_j$ is some rotation-invariant vector. The same reasoning works for $\sum r$, and we conclude that $r'_j - r_j$ is rotation-invariant. Thus all rotations of σ_j differ by rotation-invariant vectors.

We can think of moves as elements of $\mathbb{Z}_q[x]/(x^p - 1)$. Rotation is then multiplication by x. Our vector σ_j has the property that $(x - 1)\sigma = c(1 + x + \cdots + x^{p-1})$. Substituting $x = 1$, we find that $c = 0$ and so in fact σ_j must be rotation-invariant, contrary to the way we chose it. □

Most of the games reduce to this unsolvable case, using the next two lemmas.

Lemma 2.7. *Let $f|n$. Then if $G(n, S)$ is solvable then so is $G(f, S)$.*

Proof. Define a mapping from S^n to S^f by taking the coordinates $i(n/f)$. This mapping respects rotation (i.e. a rotation of the input translates to a rotation of the output), and so any solution of $G(n, S)$ also solves $G(f, S)$. □

Lemma 2.8. *Let $H \leq S$. Then if $G(n, S)$ is solvable then so is $G(n, H)$.*

Proof. Since S is Abelian, there is a homomorphism from S to H. Applying this homomorphism translates any solution of $G(n, S)$ into a solution of $G(n, H)$. □

Putting the last few lemmas together, we get the following criterion for solvability.

Theorem 2.9. *If $G(n, S)$ is solvable then either $n = 1$, $S = \mathbb{Z}_1$, or $n = p^N$ for some prime p and S is a p-group.*

Proof. Suppose that $G(n, S)$ is solvable. If p is any prime factor of n and q is any prime order of some element of S, then by lemmas 2.7 and 2.8, $G(p, q)$ is solvable, and so $p = q$ by lemma 2.6.

If we futher assume that $n \neq 1$ and $S \neq \mathbb{Z}_1$, then there must be some prime factor $p|n$ and some element of prime order in S. We easily get that p must be the only prime factor of n and that all elements of prime order in S must be of order p. □

3 Product solutions

Given solutions for two games, we can form a solution for the product game using a very simple construction. In fact, this construction works within an even more general framework than the one given by definition 2.1.

Definition 3.1. *Let R be a finite group acting on a finite Abelian group S. The generalized game $G'(R, S)$ is defined implicitly by its solutions as follows.*

A rotation *of $s \in S$ is the application of any element of R on it.*

A move sequence *for $G'(R, S)$ is any finite sequence σ of elements in S.*

A realization *of a move sequence σ is another sequence r where each r_i is some rotation of σ_i.*

We denote by $\sum r$ the sequence of partial sums of a realization, including the empty sum.

A move sequence σ is a solution *of $G'(R,S)$ if for any rotation r and any $x \in S$, there is some index t such that $x + (\sum r)_t$ equals the zero vector. Equivalently, for any $x \in S$ there is some index t such that $(\sum r)_t = x$.*

Note that $G(n,S)$ is the same as $G'(\mathbb{Z}_n, S^n)$.

In practice the group R used in the definition will always be cyclic.

There are simple analogues of theorem 2.2, definition 2.3 and lemma 2.4, whose proofs directly carry to generalized games.

The product construction is described by the following basic result.

Definition 3.2. *We say the an Abelian group S can be decomposed as the quasi-direct sum $S = T \widetilde{+} U$ if:*

(a) T, U are Abelian groups with embeddings T_S, U_S into S.

(b) Every element $s \in S$ has a unique representation $s = P_T(s) + P_U(s)$, where $P_T \in T_S$ and $P_U \in U_S$.

(c) There's a generalized addition law $(t_1 + u_1) + (t_2 + u_2) = (t_1 + t_2 + f(u_1, u_2)) + (u_1 + u_2)$, where $f \colon U_S \times U_S \to T_S$ is symmetric and satisfies $f(u, 0) = 0$.

If $f(u_1, u_2) = 0$ then the sum is direct and we write simply $S = T + U$.

Definition 3.3. *Let $S = T \widetilde{+} U$. We say that the decomposition* respects *a group R acting on S, T, U if:*

(a) For all $r \in R$ and $s \in S$, $P_U(r(s)) = r(P_U(s))$.

(b) For all $r \in R$ and $t \in T$, $r(T_S(t)) = T_S(r(t))$.

Theorem 3.4. *Let $G'(R,S)$ be a generalized game.*

Suppose that S can be decomposed as a quasi-direct sum $S = T \widetilde{+} U$ which respects R.

Let further τ^i be solutions of $G'(R,T)$, and υ a move sequence for $G'(R,S)$ whose projection into U is a solution of $G'(R,U)$.

Then the following move sequence σ solves $G'(R,S)$:

$$T_S(\tau^0), \upsilon_1, T_S(\tau^1), \ldots, T_S(\tau^{|U|-2}), \upsilon_{|U|-1}, T_S(\tau^{|U|-1}).$$

Moreover, if all τ^i and υ are minimal solutions, so is σ.

Proof. Let $x \in S$. We need to show that x appears in the sequence of partial sums for any realization of σ.

Any realization s of σ corresponds to realizations t^i, u of τ^i, υ. In particular, for some t, $(\sum \upsilon)_t = P_U(x)$. Let the indices of σ start from 1, so that $\sigma_{t|T|} = \upsilon^t$ (unless $t \neq 0$). Thus $P_U\left((\sum s)_{t|T|}\right) = P_U(x)$. Since τ^t is a solution sequence for $G'(R,T)$, there is some $t' < |T|$ such that $P_T\left((\sum s)_{t|T|+t'}\right) = P_T(x)$. Since $P_U(\tau_i^t) = 0$ for all moves in τ^t, we see that $(\sum s)_{t|T|+t'} = x$.

The truth of the *moreover* part follows by calculating the length of the solution. □

In some cases, theorem 3.4 describes the form of *all* minimal solutions.

Definition 3.5. *Let $S = T \widetilde{+} U$, and R be a finite Abelian group. For $s \in S$, let R^s denote the subgroup of T generated by $P_T(r(s) - s)$. We call $s \in S$* admissible *if $s \notin T$ and $P_U(s)$ is R-invariant.*

If for all admissible s, the size of R^s is divisible by some d, we say that R acts on the decomposition d-uniformly*. If $d = |T|$, we say that R* acts on the decomposition uniformly*.*

Theorem 3.6. *Let us be in the setting of theorem 3.4, and suppose the sum is direct.*

If the action of R on the decomposition is d-uniform, then in every minimal solution $(\sigma_i)_{i=1}^{\lceil |S|-1}$ of $G'(R,S)$, if $\sigma_t \notin T$ then t is divisible by d.

If the action of R is uniform, then moreover all minimal solutions of $G'(R,S)$ are of the form described by theorem 3.4.

Proof. Consider some minimal solution σ of $G'(R,S)$. Consider the set

$$N = \{i : \sigma_i \notin T\} \cup \{|S|\}.$$

Suppose not all elements of N are divisible by d. By Lagrange's theorem, d divides $|T|$ and so $|S|$. Thus there are two adjacent elements whose difference is not divisible by d. Consider the last such pair i, j. Note that $i \neq |S|$, and

that $d \nmid i$. Let s be some realization of σ. The equation $P_U(t) = P_U\left((\sum s)_i\right)$ should be true for exactly $|T|$ different times. Suppose that $P_U(s'_i) \neq P_U(s_i)$ for some other rotation s'_i of σ_i. The effect of changing s_i to s'_i on the number of times the aforementioned equation is true would be subtraction of $j - i$, and addition of some multiple of d (since all further differences are multiples of d). The total effect cannot be zero since $d \nmid j - i$, and we conclude that all realizations of σ_i should have the same projection P_U into U. Thus s_i is admissible.

Denote by $H_s(t)$ the number of times $k \geq i$ such that $P_T\left((\sum s)_k\right) = t$. For $r \in R$, denote by s^r the realization differing from s only by applying r to s_i. Notice that $H_s(t) = H_{s^r}(t)$ since the same elements must be covered in both realizations. On the other hand, $H_{s^r}(t) = H_s(t + \Delta^r)$, where $\Delta^r = P_T\left(r(s) - s\right)$; here we use the fact that the sum is direct. Thus, H_s must be constant on each coset of R^s (defined in definition 3.5), whose sizes are a multiple of d. In particular, the number of times $|S| - i$ must be divisible by d, which contradicts our choice of i. We conclude that all times for which $\sigma_i \notin T$ must satisfy $d|i$.

If the action of R is uniform, then we get that σ must be of the form mentioned in 3.4. Since moves in T do not affect P_U, we see that $P_U(\upsilon)$ must be a minimal solution to $G'(R, U)$. It is easy to see that the τ^i must be minimal solutions to $G'(R, T)$. □

Using the product construction, we can form minimal solutions by decomposing S.

Lemma 3.7. *Let S be a group and $S_1 \leq S$ its subgroup. If $G(n, S_1)$ and $G(n, S/S_1)$ are solvable, then so is $G(n, S)$.*

Moreover, if $G(n, S_1)$ and $G(n, S/S_1)$ are minimally solvable, then so is $G(n, S)$.

Proof. Let $S_2 \subset S$ be any set of representatives of the cosets of S_1. It is easy to see that $S = S_1 \widetilde{+} S_2$. This implies that $S^n = S_1^n \widetilde{+} S_2^n$. Trivially the last decomposition respects rotation, and so the lemma follows from theorem 3.4. □

In section 5 we will prove that $G(p^N, p)$ is always minimally solvable (theorem 5.11). This implies the following theorem.

Theorem 3.8. *If the game $G(n, S)$ is solvable then it is minimally solvable.*

Proof. If $n = 1$ or $|S| = 1$ then this is shown in theorem 2.5.

Otherwise, by theorem 2.9 there is some prime p such that $n = p^N$ and S is a p-group. Since S is a p-group, it has some subset H of size p. The quotient group S/H is also a p-group. Thus the theorem follows by induction using lemma 3.7, where the solvability of $G(p^n, H)$ is demonstrated by theorem 5.11. □

4 Solving $G(2^N, 2)$

In this section we will prove that $G(2^N, 2)$ is always solvable, and moreover describe all minimal solutions. The method we use can be generalized to $G(p^N, p)$, however in section 5 we prove this generalization differently.

Lemma 4.1. *For $N \geq 0$, define $S^N = \mathbb{Z}_2^{2^N}$.*

We think of an element in S^{N+1} also as a concatenation of two elements from S^N.

Define the following mappings from S^{N+1} to S^N and vice versa:

$$\begin{aligned} P_T(x, y) &= x, \\ P_U(x, y) &= x + y, \\ T_S(x) &= (x, x), \\ U_S(x) &= (0, x). \end{aligned}$$

Let $T^N = T_S(S^N)$ and $U^N = U_S(S^N)$ be the images of T_S, U_S.

Then $S^{N+1} = T^N + U^N$ in the meaning of definition 3.2, and this sum respects rotation in the meaning of definition 3.3.

Moreover, σ is a solution of $G'(2^N, S^N)$ iff $T_S(\sigma)$ is a solution of $G'(2^{N+1}, T^N)$ iff $U_S(\sigma)$ is a solution of $G'(2^{N+1}, U^N)$.

Proof. Routine verification. □

Lemma 4.2. *The decomposition mentioned in lemma 4.1 is uniform with respect to the group of rotations.*

Proof. Let $s \in S^{N+1}$ be an admissible element. Thus $s \notin T^{N+1}$ and $P_U(s)$ is rotation-invariant. We conclude that $P_U(s) = 1^{2^N}$ and so s is of the form $(x, x) + (0^{2^N}, 1^{2^N})$. Denote r_i rotation i times to the left. Then R^s (defined in definition 3.5) is generated by $P_T\left(r^i(s) - s\right) = 0^{2^N - i}1^i$. It is easy to see that these elements generate all of T^{N+1}. □

These lemmas form the bulk of the structure theorem for all solutions of $G(2^N, 2)$.

Theorem 4.3. *The game $G(2^N, 2)$ is solvable for all $N \geq 0$.*

For $0 \leq x < 2^N$, define the x'th generalized parity p_x of $y \in \mathbb{Z}_2^{2^N}$ to be the parity of the bits y_t for the indices t in which $t_i = 0$ for any zero bit $x_i = 0$ in the function index. If $x = 2^N - 1$, we get the normal parity.

All minimal solutions of $G(2^N, 2)$ are move sequences $(\sigma_i)_1^{2^{2^N}-1}$ such that if $2^d \| i$ then d is the maximum index for which the generalized parity of σ_i is odd.

Proof. The proof is by induction on N.

Clearly, the only minimal solution of $G(2^0, 2)$ is 1, and it is of the mentioned form since 1 is odd.

Lemmas 4.1 and 4.2 imply that all minimal solutions of $G(2^{N+1}, 2)$ can be constructed from minimal solutions of $G(2^N, 2)$ using the construction of theorem 3.4. Now consider some move σ_i in a minimal solution σ. There are two cases: either $2^{2^N} | i$ or not.

If $2^{2^N} | i$ then $\sigma_i = (x, y)$ where $x + y$ corresponds to location $j = i/2^{2^N}$ in a solution of $G(2^N, 2)$. Suppose $2^d \| j$, so that $2^{d+2^N} \| i$. Notice that $p_{2^N+e}(x, y) = p_e(x + y)$, and so the maximum index for which the generalized parity of σ_i is odd is $2^N + d$.

Conversely, if $2^{2^N} \nmid i$ then $\sigma_i = (x, x)$ where x corresponds to location $j = i \mod 2^{2^N}$. Thus if $2^d \| j$ then also $2^d \| i$. For any $e < 2^N$, $p_{2^N+e}(x, x) = p_e(0) = 0$. On the other hand, $p_e(x, x) = p_e(x)$, and so the maximum index for which the generalized parity of σ_i is odd is d. □

5 Solving $G(p^N, p)$

In the previous section 4 we presented a solution of $G(2^N, 2)$. This solution can be adapted to general prime p by generalizing lemma 4.1 to a decomposition with p factors. This approach works by presenting a solution for each length p^N, and thus has N steps. A different approach, which results necessarily in the same minimal solutions, works by taking p^N steps to solve $G(p^N, p)$. The reader may adapt the solution presented here to the method presented in section 4 by considering the case $N = 1$.

For the rest of the section, we assume that p is some prime. All our arithmetic will be done modulo p. The function ρ rotates a vector once to the right.

We begin with a sequence of lemmas about binomial coefficients.

Lemma 5.1. *Let the base p expansion of a be a_d. Then*

$$(-1)^a = (-1)^{\sum a_d}.$$

Proof. If $p = 2$ then this is trivial. Otherwise, it follows from the fact that $(-1)^p = -1$. □

Lemma 5.2. *If $b, d < p$ then*

$$\binom{ap+b}{cp+d} = \binom{a}{c}\binom{b}{d}.$$

Proof. This is a well-known result. One way to prove it is to notice that $\binom{ap+b}{cp+d}$ is the coefficient of x^{cp+d} in the power series $(1+x)^{ap+b}$. By Fermat's theorem,

$$(1+x)^{ap+b} = (1+x)^{ap}(1+x)^b = (1+x^p)^a(1+x)^b.$$

The lemma follows. □

Corollary 5.3. *Let a_d, b_d be the base p expansions of a, b. Then*

$$\binom{a}{b} = \prod_i \binom{a_d}{b_d}.$$

Lemma 5.4. *For $i, j < p$ we have*

$$\binom{i}{j} = (-1)^{i+j}\binom{p-1-j}{p-1-i}.$$

Proof. We can rewrite the equation as follows:

$$\binom{i}{i-j} = (-1)^{i-j}\binom{p-1-j}{i-j}.$$

The factors in the left-hand binomial are $j+1$ up to i, and those in the right-hand binomial are $p-(j+1)$ down to $p-i$. The lemma follows. □

Corollary 5.5. *For $i, j < p^N$ we have*

$$\binom{i}{j} = (-1)^{i+j}\binom{p^N - 1 - j}{p^N - 1 - i}.$$

Proof. This follows directly from corollary 5.3 and lemma 5.1. □

Lemma 5.6. *Let $i + j < p - 1$. Then*

$$\sum_{k=0}^{p-1}\binom{k}{i}\binom{k}{j} = 0.$$

If $i + j = p - 1$, the sum is non-zero and equal to $(-1)^i = (-1)^j$.

Proof. The proof uses lemma 5.4:

$$\sum_{k=0}^{p-1}\binom{k}{i}\binom{k}{j} = \sum_{k=0}^{p-1}\binom{p-1-i}{k}\binom{p-1-j}{k} = \binom{2(p-1)-(i+j)}{p-1-i}.$$

If $i + j < p - 1$, we have $2(p-1) - (i+j) > p - 1$ and so the binomial coefficient $\binom{2(p-1)(i+j)}{p-1-i}$ equals zero. If $i + j = p - 1$, this binomial coefficient is $\binom{p-1}{p-1-i} = (-1)^i\binom{i}{0} = (-1)^i$ by lemma 5.4. □

Corollary 5.7. *Let $i + j < p^N - 1$. Then*

$$\sum_{k=0}^{p^N-1}\binom{k}{i}\binom{k}{j} = 0.$$

If $i + j = p^N - 1$, the sum is non-zero and equal to $(-1)^i = (-1)^j$.

Proof. Let i_d, j_d denote the dth digits of i, j in base p representation. Clearly

$$\sum_{k=0}^{p^N-1}\binom{k}{i}\binom{k}{j} = \prod_{d=0}^{N-1}\sum_{k=0}^{p-1}\binom{k}{i_d}\binom{k}{j_d}.$$

Suppose first that $i + j < p^N - 1$. If always $i_d + j_d \geq p - 1$ then $i + j \geq (p-1)\sum_{d=0}^{N-1} p^d = p^N - 1$, contrary to our assumption. Thus, for some d it must happen that $i_d + j_d < p - 1$, and the corresponding factor zeroes the product.

If $i + j = p^N - 1$ then $i_d + j_d = p - 1$, and so the corollary follows from corollary 5.3 and lemma 5.1. □

Using this sequence of lemmas, we define a decomposition of $\mathbb{Z}_p^{p^N}$ which we call the *rotation basis*. We also define analogues of the generalized parity functions of theorem 4.3 (in reverse order).

Definition 5.8. *The* rotation basis *of* $\mathbb{Z}_p^{p^N}$ *consists of the* p^N *vectors* b^i *for* $0 \le i < p^N$ *defined by* $b^i_j = \binom{j}{i}$ *for* $0 \le j < p^N$.

The subspace spanned by b^i *is* $B^i = \mathrm{span}(b^i)$.

The invariant subspaces *are defined by* $S^i = \mathrm{Span}(b^0, \ldots, b^{i-1})$.

The i*'th* generalized parity function *is defined by* $p_i(x) = (-1)^i \langle x,\, b^{p^N-1-i} \rangle$.

Note that the rotation basis is symmetric in the sense of corollary 5.5 (if we reverse both rows and columns and transpose rows and columns, we reach the same set of vectors).

The rotation basis enjoys the properties summarized in the following lemma.

Lemma 5.9. *The rotation basis satisfies the following properties:*

(a) The dimension of S^i *is* i.

(b) The subspaces S^i *are rotation-invariant.*

(c) The vector b^i *is rotation-invariant modulo* S^i.

(d) The subspace S^{i+1} *consists of all vectors* x *such that* $p_i(x')$ *is constant for all rotations* x' *of* x.

(e) The subspace S^i *consists of all vectors* $x \in S^{i+1}$ *such that* $p_i(x) = 0$.

(f) If $x \in S^{i+1}$ *then* $p_i(x)$ *is the coefficient of* b^i.

Proof. Denote by $\rho(x)$ the rotation of $x \in \mathbb{Z}_p^{p^N}$ once to the right.

Item (a) follows from the easy fact that the vectors b^i are independent as they form a triangular matrix.

We prove items (b) and (c) together by induction on i. Item (b) is trivially true for $i \le 1$ since $b^0_i = \binom{i}{0} = 1$ and so b^0 is a constant vector.

To prove item (c) for i from item (b) for i, note first that the vector $\rho(b^i)$ satisfies $\rho(b^i)_j = \binom{p^N+j-1}{i}$ by an application of corollary 5.3. Pascal's identity $\binom{j}{i} - \binom{j-1}{i} = \binom{j-1}{i-1}$ thus implies $b^i - \rho(b^i) = \rho(b^{i-1}) \in S^i$. Since S^i is rotation-invariant, it follows that $\rho^k(b^i) - \rho^{k+1}(b^i) \in S^i$ and item (c) follows. Item (b) for $i+1$ now trivially follows.

Next, notice that corollary 5.7 implies that $p_j(b^i) = 0$ for $i < j$. Since b^i is rotation-invariant modulo S^i, it follows that any $x \in S^{i+1}$ satisfies $\rho^k(x) - x \in \text{span}(b^0, \ldots, b^{i-1})$ and so $p_i(\rho^k(x)) = p_i(x)$. Thus S^{i+1} contains all vectors x such that $p_i(\rho^k(x)) = p_i(x)$. On the other hand, $p_i(\rho^k(x)) = p_i(x)$ is equivalent to $\langle \rho^k(b^{p^N-1-i}) - b^{p^N-1-i}, x\rangle = 0$. Since $b_j^{p^N-1-i} = 0$ for $j < p^N - 1 - i$, we get that the vectors $\rho^{-k}(b^{p^N-1-i}) - b^{p^N-1-i}$ for $k = 1$ up to $k = p^N - 1 - i$ are all linearly independent. Thus the solution of the set of equations $p_i(\rho^k(x)) = p_i(x)$ has dimension at most $p^N - (p^N - 1 - i) = i + 1$. Item (d) follows.

Again by corollary 5.7 we see that $p_i(b^i) = 1$. Thus the subspace of S^{i+1} consisting of all vectors x such that $p_i(x) = 0$ is strictly smaller than S^{i+1}. On the other hand, again by the corollary, all vectors $x \in S^i$ satisfy $p_i(x) = 0$. Item (e) follows.

Item (f) follows from item (e) since $p_i(b^i) = 1$. □

We can now infer a decomposition of $\mathbb{Z}_p^{p^N}$ along the lines of definitions 3.2, 3.3 and 3.5.

Lemma 5.10. *The decomposition $\mathbb{Z}_p^{p^N}/S_i = B^i + \mathbb{Z}_p^{p^N}/S_{i+1}$ is a direct sum, where rotations act on B^i as the identity.*

Moreover, the decomposition respect rotation, and rotation acts on it uniformly.

Proof. Note that $\mathbb{Z}_p^{p^N}/S_i = \text{span}(b^i, \ldots)$ and $\mathbb{Z}_p^{p^N}/S_{i+1} = \text{span}(b^{i+1}, \ldots)$. Hence lemma 5.9(a) implies that the decomposition is a direct sum.

We can represent any vector in $\mathbb{Z}_p^{p^N}/S_i$ in the form $s = c_i b^i + s'$, where $s' \in \mathbb{Z}_p^{p^N}/S_{i+1}$. By lemma 5.9(c), for b^i as an element of $\mathbb{Z}_p^{p^N}/S_i$, we have $r(b^i) = b^i$ for all rotations r, and $r(s') - s' \in B^i$. Thus $r(s) \in B^i + r(s')$.

In order to show that the decomposition respects rotation, we go over the two condition in definition 3.3. Let r be some rotation. If $s = c_i b^i + c's'$ then the projection of $r(s)$ into $\mathbb{Z}_p^{p^N}/S_{i+1}$ is $r(s')$, confirming the first condition. The second condition follows from the fact $r(b^i) = b^i$ noted above.

In order to show that rotation acts uniformly, consider some admissible element s. Since $s \notin B^i$, it is of the form $s = c_i b^i + s'$ with $s' \neq 0$. Lemma 5.9(e) now implies that for some rotation r, $r(s') - s' \neq 0$ and so $r(s) - s = r(s') - s' = cb^i$ for $c \neq 0$. Since $B^i \approx \mathbb{Z}_p$, the element cb^i generates all of B^i, proving that $|R^s| = |B^i|$. □

We can now prove the structure theorem describing all minimal solutions of $G(p^N, p)$.

Theorem 5.11. *The game $G(p^N, p)$ is solvable for all prime p and $N \geq 0$.*

All minimal solutions of $G(p^N, p)$ are move sequences $(\sigma_i)_1^{p^{p^N}-1}$ such that:

(a) If $p^i \| t$ then $\sigma_t \in S^{i+1} \setminus S^i$.

(b) If $p^i | t$ for $i > 0$ then the subsequence $p_{i-1}(\sigma_{t+p^{i-1}k})_{k=1}^{p-1}$ is a solution of $G(1, p)$.

(c) For each $0 < i \leq p^N$, the subsequence $p_{i-1}(\sigma_{p^{i-1}k})_{k=1}^{p-1}$ is a solution of $G(1, p)$.

Note that condition (c) is a formulation of condition (b) for $t = 0$ and $p^{p^N} \| t$.

Proof. Fix p and N. We know by 3.6 that all minimal solutions are constructed using $p^N - 1$ applications of theorem 3.4 on decompositions produced by lemma 5.10.

For each i, let $\tau_k^i = \sigma_{p^i k}$ be a move sequence of length $p^{p^{N-i}} - 1$. We claim that σ is a minimal solution iff $\tau^i \pmod{S^i}$ is a minimal solution of $G'(p^N, \mathbb{Z}_p^{p^N}/S^i)$ for all $0 \leq i < p^N - 1$. This follows easily from lemma 5.10.

Moreover, looking more carefully at the construction, we see that we can relax this condition to the following one: σ is a minimal solution iff $\tau^i \pmod{S^i}$ satisfies that for all $0 \leq l < p^{p^{N-i-1}} - 1$, the sequence $(\tau_{pl+k}^i)_{k=1}^{p-1}$ is a minimal solution of $B^i \approx G(1, p)$. This is because the the condition on the elements τ_{pl}^i themselves is handled by τ_j for $j > i$, which provide a total description of the sequence τ_{pl}^i.

It is easy to check that this characterization is equivalent to the characterization outlined in the statement of the lemma. □

6 Appendix: the goal of reaching the same orientation

The original problem mentioned in the introduction does not fall into our framework, since we require for all switches to be in the same orientation, rather to be in some fixed orientation. However, it is clearly equivalent to the following generalized game.

Definition 6.1. *For $n \geq 1$ and finite Abelian group S define $C(n,S) \stackrel{def}{=} \{s^n : s \in S\}$ to be the set of constant vectors. Let $S^n/C(n,S)$ be the set of vectors up to addition of a constant vector, with the natural rotation.*

The game up-to-constant is defined by $G_C(n,S) = G'(n, S^n/C(n,S))$.

The following lemma is easy to see.

Lemma 6.2. *For any $n \geq 1$ and finite Abelian group S, we have $S^n = C(n,S)\widetilde{+}S^n/C(n,S)$, where $S^n/C(n,S)$ is embedded in S^n as the set of all vectors starting with 0, the projection $P_{C(n,S)}(s) = s_0$ is the first coordinate, and the other projection is $P_{S^n/C(n,S)}(s) = s - s_0^n$.*

Corollary 6.3. *The up-to-constant game $G_C(n,S)$ is (minimally) solvable iff the game $G(n,S)$.*

Proof. Clearly, any solution of $G(n,S)$, taken modulo $C(n,S)$, also solves $G_C(n,S)$. The converse follows from theorem 3.4 since $G(n, C(n,S))$ is equivalent to $G(1,S)$, which is always minimally solvable by theorem 2.5. □

Moreover, if $|S|$ is prime we can describe all minimal solutions.

Theorem 6.4. *If $G_C(n,S)$ is solvable and $|S| = p$ is prime then all minimal solutions are describe by theorem 3.4 via the decomposition in lemma 6.2.*

Proof. We claim that the decomposition in lemma 6.2 is uniform with respect to rotation. Indeed, for *any* $s \notin C(n,S)$, there is some rotation s' of it such that $s'_0 \neq s_0$ and so for some rotation r, $P_{C(n,S)}(r(s'_0 - s_0))$ generates $C(n,S)$. Thus, the theorem follows from theorem 3.6. □

This theorem is not true in general for $S \neq \mathbb{Z}_p$.