Colorings and Nowhere-Zero Flows of Graphs in Terms of Berlekamp's Switching Game

Uwe Schauz

Department of Mathematics and Statistics
King Fahd University of Petroleum and Minerals
Dhahran 31261, Saudi Arabia
schauz@kfupm.edu.sa

Submitted: Jul 22, 2010; Accepted: Mar 14, 2011; Published: Mar 24, 2011
Mathematics Subject Classifications: 91A43, 05C15, 05C50, 05C20, 94B05

Abstract

We work with a unifying linear algebra formulation for nowhere-zero flows and colorings of graphs and matrices. Given a subspace (code) $U \leq \mathbb{Z}_k^n$ – e.g. the bond or the cycle space over $\mathbb{Z}_k$ of an oriented graph – we call a nowhere-zero tuple $f \in \mathbb{Z}_k^n$ a *flow* of U if f is orthogonal to U. In order to detect flows, we view the subspace U as a light pattern on the n-dimensional *Berlekamp Board* $\mathbb{Z}_k^n$ with k^n light bulbs. The lights corresponding to elements of U are *ON*, the others are *OFF*. Then we allow axis-parallel switches of complete rows, columns, etc. The core result of this paper is that the subspace U has a flow if and only if the light pattern U cannot be switched off. In particular, a graph G has a nowhere-zero k-flow if and only if the $\mathbb{Z}_k$-bond space of G cannot be switched off. It has a vertex coloring with k colors if and only if a certain corresponding code over $\mathbb{Z}_k$ cannot be switched off. Similar statements hold for Tait colorings, and for nowhere-zero points of matrices. Studying different normal forms to equivalence classes of light patterns, we find various new equivalents, e.g., for the Four Color Problem, Tutte's Flow Conjectures and Jaeger's Conjecture. Two of our equivalents for colorability and existence of nowhere zero flows of graphs include as special cases results by Matiyasevich, by Balázs Szegedy, and by Onn. Alon and Tarsi's sufficient condition for k-colorability also arrives, remarkably, as a generalized full equivalent.

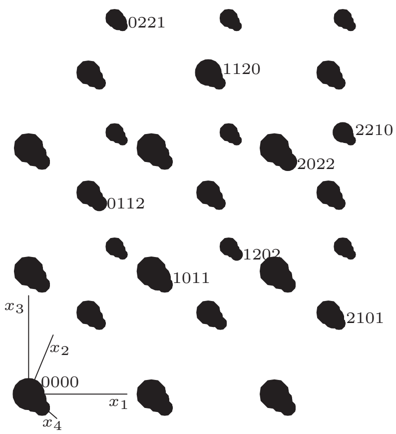
Introduction

While working at Bell Labs in the 1960s, Elwyn Berlekamp built a 10×10 grid of light bulbs. The grid had an array of 100 switches in the back to control each light bulb individually. It also had 20 switches in the front, one for every row and column. Flipping a row or column switch would invert the state of each bulb in the row or column.

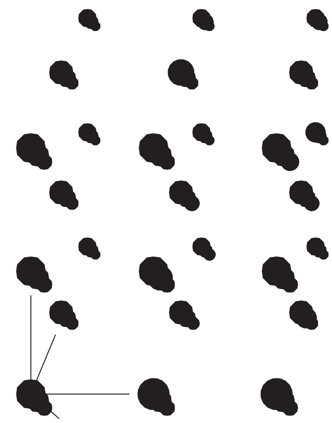
A simplistic game that can be played with such a grid is to arrange some initial pattern of lighted bulbs using the rear switches, and then try to turn off as many bulbs as possible using the row and column switches, as, e.g., described in [FiSl, CaSt, RoVi]. The problem of finding a configuration with most light bulbs switched on, and with the property that no combination of row and column switches can reduce this number, is equivalent to the problem of finding the covering radius of the binary code generated by row and column switches. One can also ask how few lights we may turn on if we start with a dark board. This corresponds to finding the minimal weight of the binary code. Such kinds of examinations have been the primary focuses in the literature. Aside from the binary code generated by row and column switches, we are not aware of any previously known useful application of the game.

In this paper, we consider an n-dimensional version of Berlekamp's game with $k_1 \times k_2 \times \cdots \times k_n$ many light bulbs, where mostly $k_1 = k_2 = \cdots = k_n =: k$, so that we can identify the light bulbs with the points in the group $\mathbb{Z}_k^n$. An elementary move in the game inverts all lights $v \in \mathbb{Z}_k^n$ that lie on an axis-parallel affine line of the free $\mathbb{Z}_k$-module $\mathbb{Z}_k^n$. We call this game *Berlekamp* or *Affine Berlekamp modulo* 2 of *order* k and *dimension* n, k, n
for short $\mathrm{AB}_2^n(k)$. Actually, it is more general to examine a nonmodular version $\mathrm{AB}^n(k)$, $\mathrm{AB}_2^n(k)$
with the integers $\mathbb{Z}$ as the set of possible states of a light bulb. In this version, an $\mathrm{AB}^n(k)$
elementary move increases or decreases the state of the bulbs along an axis-parallel affine line. $\mathrm{AB}_r^n(k)$ is the modulo r version of this game. Figure 1 shows the 4-dimensional $\mathrm{AB}_r^n(k)$
$3 \times 3 \times 3 \times 3$ cube $\mathrm{AB}_2^4(3)$ with the characteristic function of a certain 2-dimensional subspace as initial *light pattern*. This pattern can be *switch off*. Figure 1 illustrates this fact using a special 4-step procedure. The strategy is to switch off all lights on 4 fixed pairwise orthogonal "side faces" of the cube (here $e_1^\perp$, $e_3^\perp$, $2e_4 + e_2^\perp$ and $2e_4 + e_4^\perp$), and then to hope for the best for the remaining light bulbs. In each step of the procedure, we shuts off all 3^3 lights in one side face, only using *moves* in the direction orthogonal to the side face (3^3 possible moves, one through each point of the side face). We will see that this procedure is best possible. A pattern can be switched off by a combination of elementary moves if and only if it can be switched off in this way (Theorem 3.1). Actually, we are only interested in the question if a given light pattern can be switched off or not, since this *switchability* will turn out to be important in applications. Therefore, we provide several normal forms and invariants to investigate this property. Different *switchability equivalents* follow from this first approach to the problem. They are employed in different fields of application.

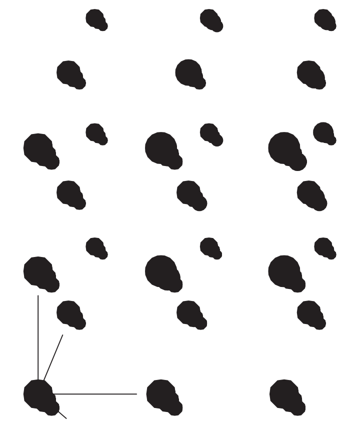
As we will see, in many applications we have to deal with characteristic functions of subspaces $U \leq \mathbb{Z}_k^n$ as initial patterns. Our core result is the surprising discovery that $U \leq \mathbb{Z}_k^n$
such 0-1 patterns $U \in \mathbb{Z}^{\mathbb{Z}_k^n}$ can be switched off if and only if there does not exist a $U \in \mathbb{Z}^{\mathbb{Z}_k^n}$
nowhere-zero vector $f \in \mathbb{Z}_k^n$ orthogonal to U, $f \perp U$. More precisely, it will turn $f \perp U$
out that U can be switched off over $\mathbb{Z}$, in $\mathrm{AB}^n(k)$, if and only if it can be switched off modulo r, in $\mathrm{AB}_r^n(k)$, with any given r not dividing $|U|$. We just speak about switchability when we refer to any of these equivalent cases. So, if U is not switchable in this sense, then there is a nowhere-zero $f \perp U$. The existence of such a *flow* f is a very important property with respect to many combinatorial problems. We will study various



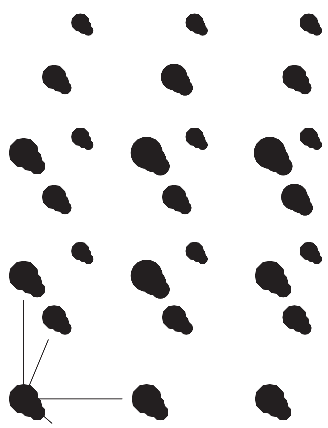
The initial characteristic function of $\langle(1,0,1,1),(0,1,1,2)\rangle \leq \mathbb{Z}_3^{\,4}$ *(yellow)*



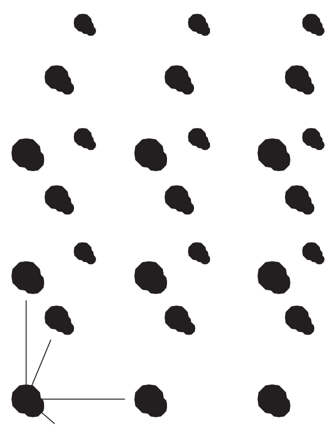
After switching off $e_1^{\perp}$ *(blue) through 3 moves parallel to* $e_1 = $ —



After switching off $e_3^{\perp}$ *(blue) through 4 moves parallel to* $e_3 = |$



After switching off $2e_2 + e_2^{\perp}$ *(blue) through 5 moves parallel to* $e_2 = /$



Success after switching off $2e_4 + e_4^{\perp}$ *(blue) through 5 moves parallel to* $e_4 = \diagdown$

In $\mathrm{AB}_2^4(3)$ *each of the* 3^4 *bulbs has* 2 *possible states:*

0 = grey
1 = yellow

Actually, $\langle(1,0,1,1),(0,1,1,2)\rangle$ *even can be switched in* $\mathrm{AB}^4(3)$, *in contrast to* $\langle(1,1)\rangle \leq \mathbb{Z}_2^{\,2}$, *which only can be switched modulo* 2 , *in* $\mathrm{AB}_2^2(2)$.

Figure 1: *The pattern* $\langle(1,0,1,1),(0,1,1,2)\rangle \leq \mathbb{Z}_3^{\,4}$ *can be switched off in* $\mathrm{AB}_2^4(3)$

subspaces U related to graphs and matrices. The flow f of U will then be a nowhere-zero flow or coloring of a graph, or a nowhere-zero point of a matrix. If, e.g., we take the $\mathbb{Z}_k$-bond space $\mathcal{B}_k(\vec{G})$ of a directed graph $\vec{G}$, then a flow f of $\mathcal{B}_k(\vec{G})$ is just a nowhere-zero flow of $\vec{G}$. Therefore, $\vec{G}$ has a nowhere-zero k-flow if and only if $\mathcal{B}_k(\vec{G})$ is not switchable. Based on this fact, we can translate our switchability equivalents into new equivalents for the existence of nowhere-zero flows of graphs. This is our general strategy, and the resulting new equivalents will usually have the flavor of Alon and Tarsi's sufficient condition for the existence of feasible graph colorings. Typically, one has to count certain combinatorial substructures, usually with weights of ± 1 , in order to detect the existence of nowhere-zero flows, colorings, etc.

The polynomial method is the main tool behind our core results. Experts with this method certainly will see in each light pattern a polynomial, and behind each move, a way to modify it. Such readers may even see the introduction of the whole Berlekamp language as unnecessary. However, we wanted to distinguish between tools and structural insights. The surprising connection between switchability and nonexistence of flows (Theorem 7.3) is a structural insight, and we tried to formulate it without mentioning polynomials. In our formulation, one does not even have to know polynomials in order to be able to apply the theorem. If somebody has new insights in Berlekamp's Switching Game, he can apply Theorem 7.3, and may end up with a proof of the Five Flow Conjecture or a short verification of the Four Color Theorem.

In order to clarify the different methods used we divided this article into two parts. Part I, Section 1 – Section 8, deals with the light switching game. Part II, Section 9 – Section 11, deals with flows of subspaces and their specializations to colorings and nowhere-zero flows of graphs and matrices. The actual interface between these two parts is Theorem 7.3, but we combined in Theorem 7.4 this interface with all results from the first part, so that only Theorem 7.4 is used in Part II. Readers interested in the new graph-theoretic results can read this part without reading the first part. The first part, however, contains the main ideas of this paper. This part is organized from general to special, so that each section introduces new assumptions, and the reader always will know which properties have to be used in each section. The sometimes very high degree of generality is required to obtain the "modulo r statements" in the graph-theoretic results of the second part, and to provide a solid base for further research.

Section 1 introduces the Berlekamp Game, together with some useful notations. Section 2 provides two bases of the free module of light patterns. These bases go well together with the Berlekamp Moves. In particular, we will see that the submodule of switchable patterns is saturated. In Sections 3 and 4, we study the equivalence classes of light patterns and introduce two types of normal forms for them. Formulas are given to calculate these normal forms and switchability criteria are deduced. Section 5 describes light patterns as polynomials and studies the corresponding polynomial maps on certain grids $\mathfrak{X} := \mathfrak{X}_1 \times \mathfrak{X}_2 \times \cdots \times \mathfrak{X}_n$. As a result, we obtain a complete invariant for the equivalence classes of the game. In particular, we see that the existence of a nonzero of such a polynomial map is equivalent to the nonswitchability of the polynomial as a light pattern. In order to incorporate the linear structure of the board $\mathbb{Z}_k^n$ as a $\mathbb{Z}_k$-module, in Section 6, we modify the underlying concept of polynomial rings to certain group rings. Section 7 uses this modified framework to study switchability of subspaces $U \leq \mathbb{Z}_k^n$ as 0-1 light patterns given by their characteristic function $U\colon \mathbb{Z}_k^n \longrightarrow \{0,1\}$, $x \longmapsto U(x)$. It turns U
out that U can be switched off if and only if U possesses a *flow*, i.e., a full weight vector orthogonal to U . This surprising insight is the mentioned interface to the second part. Combined with the switchability criteria from Sections 3 and 4, this interface yields Theorem 7.4, a collection of equivalents to the existence of flows of subspaces. Finally, Section 8 briefly discusses the Wedderburn Decomposition of the set of all light patterns as a group algebra. This decomposition is not required in the second part of the paper.

In Part II, starting with Section 9, we translate and specialize the results captured in Theorem 7.4 about subspace flows into graph-theoretic insights about nowhere-zero flows. To do this, we specialize our definitions for flows of subspaces to matrices and graphs. Actually, such linear algebra generalizations of graph-theoretic notions go back at least as far as Veblen's paper [Ve] from 1912. In our terminology, it is easy to see that a flow of the bond space $\mathcal{B}_R(\vec{G})$ over a commutative ring R is a nowhere-zero R-flow of $\vec{G}$. This fact leads us to new equivalents for the existence of nowhere-zero graph flows, and new equivalents to the Four Color Problem. Section 10 examines nowhere-zero points of matrices in connection with Jaeger's Conjecture. The matrix transformation in Lemma 10.2 provides the connection between flows and nowhere-zero points needed here. Finally, Section 11 applies the results of the two previous sections to derive a bunch of new equivalents for k-colorability of graphs. These equivalents are contained in the two similar-looking but different Theorems 11.2 and 11.4. The first one is based on the duality between proper colorings and nowhere-zero flows, the second one uses an interpretation of a nowhere-zero point of a certain incidence matrix as a "nowhere-zero coloring" of the underlying graph.

Part I

Berlekamp's Switching Game

1 Tensor Products of Berlekamps

We start here with a more general situation than described in the introduction. We take any finite set I (of *light bulbs*) as *board*, and any system $\mathcal{M} \subseteq \mathbb{Z}^I$ of *(light) patterns* (i.e. maps $M: I \longrightarrow \mathbb{Z}$) as our collection of elementary *moves*:

Definition 1.1 (General Berlekamp)**.** A pair $(I, \mathcal{M})$ of a finite set I and a system $\mathcal{M} \subseteq \mathbb{Z}^I$ of *patterns* is a *(General) Berlekamp* on the *board* I. The elements of $\mathcal{M}$ are its *(elementary) moves*. The elements of its $\mathbb{Z}$-linear span $\langle \mathcal{M} \rangle$ are its *switchable patterns* or *composed moves*, they can be *switched off* by a sequence of moves. By replacing $\mathbb{Z}$ with $\mathbb{Z}_r := \mathbb{Z}/r\mathbb{Z}$, we obtain $(I, \mathcal{M})_r$, *(General) Berlekamp modulo* r. $(I, \mathcal{M})$ $\langle \mathcal{M} \rangle$, $\mathbb{Z}_r$ $(I, \mathcal{M})_r$

We identify subsets $U \subseteq I$ with their characteristic functions $I \longrightarrow \{0, 1\} \subseteq \mathbb{Z}$ as light patterns, i.e., $U(v)$

$$U(v) \ := \begin{cases} 1 & \text{if } v \in U, \\ 0 & \text{if } v \notin U. \end{cases} \tag{1}$$

This is used extensively. It simplifies notation, but can lead to unusual expressions. For example, the one-point sets $\{v\}$ ($v \in I$) are also viewed as 0-1 patterns $\{v\}$

$$\{v\}: \ I \longrightarrow \{0, 1\}, \ \ u \longmapsto \{v\}(u). \tag{2}$$

They form the standard basis of $\mathbb{Z}^I$. We also need:

Definition 1.2 (Tensor Product)**.** The *tensor product* $\otimes$

$$(I, \mathcal{M}) \;:=\; (I_1, \mathcal{M}_1) \otimes (I_2, \mathcal{M}_2)$$

of two Berlekamps $(I_1, \mathcal{M}_1)$ and $(I_2, \mathcal{M}_2)$ is the Berlekamp played on

$$I \;:=\; I_1 \times I_2$$

with elementary moves given by

$$\mathcal{M} \;:=\; \big\{ M \otimes \{v\} \;\big|\; M \in \mathcal{M}_1, v \in I_2 \big\} \;\cup\; \big\{ \{v\} \otimes M \;\big|\; v \in I_1, M \in \mathcal{M}_2 \big\},$$

where

$$(U_1 \otimes U_2)((v_1, v_2)) \;:=\; U_1(v_1)\, U_2(v_2) \quad \text{for } U_j \in \mathbb{Z}^{I_j} \text{ and } v_j \in I_j \quad (\, j = 1, 2\,).$$

The set of all possible light patterns over the board $I = I_1 \times I_2$, actually, is the analytic tensor product

$$\mathbb{Z}^{I_1} \otimes \mathbb{Z}^{I_2} \;=\; \mathbb{Z}^{I_1 \times I_2}. \tag{3}$$

For two subsets $U_1 \subseteq I_1$ and $U_2 \subseteq I_2$, their direct product (viewed as a 0-1 pattern on $I = I_1 \times I_2$) and tensor product (with U_1, U_2 as 0-1 patterns in $\mathbb{Z}^{I_1}$ respectively $\mathbb{Z}^{I_2}$) coincide,

$$U_1 \times U_2 \;=\; U_1 \otimes U_2. \tag{4}$$

In particular, the standard basis of $\mathbb{Z}^I$ is just the tensor product basis of the standard bases of $\mathbb{Z}^{I_1}$ and $\mathbb{Z}^{I_2}$,

$$\{(v_1, v_2)\} \;=\; \{v_1\} \otimes \{v_2\} \quad \text{for } v_1 \in I_1 \text{ and } v_2 \in I_2\,. \tag{5}$$

Equipped with the tensor product, we now can give the following definition (see Figure 2):

Definition 1.3 (Affine Berlekamp)**.** *Affine Berlekamp* on a $k_1 \times k_2 \times \cdots \times k_n$ board $I := I_1 \times I_2 \times \cdots \times I_n$ is the game $\mathrm{AB}[I]$

$$\mathrm{AB}[I] \;=\; \mathrm{AB}(I_1, I_2, \ldots, I_n) \;:=\; (I_1, \{I_1\}) \otimes (I_2, \{I_2\}) \otimes \cdots \otimes (I_n, \{I_n\}). \tag{6}$$

If $|I_j| = k_j$ for $j = 1, \ldots, n$, we also write $\mathrm{AB}(k_1, k_2, \ldots, k_n)$ for this type of game. If all n entries are the same, we abbreviate AB^n

$$\mathrm{AB}^n(I_1) \;:=\; \mathrm{AB}(I_1, I_1, \ldots, I_1) \quad \text{and} \quad \mathrm{AB}^n(k_1) \;:=\; \mathrm{AB}(k_1, k_1, \ldots, k_1).$$

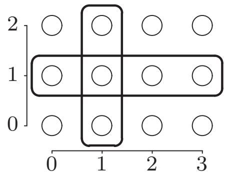
In the modulo r case, with $\mathbb{Z}_r$ in the place of $\mathbb{Z}$, we write AB_r respectively AB^n_r with r as index. AB^n_r

The elementary moves of $\mathrm{AB}[I]$ are of the form $v{\restriction}j$

$$v{\restriction}j \;=\; (v_1, \ldots, v_{j-1}, *, v_{j+1}, \ldots, v_n) \;:=\; \{v_1\} \times \cdots \times \{v_{j-1}\} \times I_j \times \{v_{j+1}\} \times \cdots \times \{v_n\}, \tag{7}$$

where $v = (v_1, v_2, \ldots, v_n) \in I$ (see Figure 2). Obviously, the patterns $v{\restriction}J$ with $\emptyset \neq J \subseteq$ $v{\restriction}J$
$\{1, 2, \ldots, n\}$ are switchable as well, where, e.g. if $n = 6$ and $J = \{2, 4, 5\}$, $(v_1, *, v_3)$

$$v{\restriction}J \;=\; (v_1, *, v_3, *, *, v_6) \;:=\; \{v_1\} \times I_2 \times \{v_3\} \times I_4 \times I_5 \times \{v_6\}. \tag{8}$$



Two moves are highlighted:
$(*,1) = (0,1)\restriction 1 = (1,1)\restriction 1 = I_1 \times \{1\}$ *identified with* $I_1 \otimes \{1\}$ *as a 0-1 pattern,*
$(1,*) = (1,0)\restriction 2 = (1,1)\restriction 2 = \{1\} \times I_2$ *identified with* $\{1\} \otimes I_2$ *as a 0-1 pattern.*

Figure 2: $\mathrm{AB}(I_1, I_2)$ *with* $I_1 = \{0,1,2,3\}$ *(horizontal) and* $I_2 = \{0,1,2\}$ *(vertical)*

2 Two Convenient Bases

In Affine Berlekamp, we have a convenient basis for the module of all light patterns. In the one-dimensional case $\mathrm{AB}(I_1) = (I_1, \{I_1\})$, we may select one element $\{a_1\}$ of the standard basis $\{\{v_1\} \mid v_1 \in I_1\}$, and replace it with I_1 as all-1 pattern. The new basis B_{a_1} consists of the vectors B_{a_1}

B_{a_1,v_1}

$$B_{a_1,v_1} \;:=\; \begin{cases} \{v_1\} & \text{if } v_1 \neq a_1, \\ I_1 & \text{if } v_1 = a_1, \end{cases} \tag{9}$$

where v_1 runs through I_1. In the n-dimensional case, if $a = (a_1, a_2, \ldots, a_n)$ is a fixed given point of our board I

$$I \;:=\; I_1 \times I_2 \times \cdots \times I_n, \tag{10}$$

the patterns (see Figure 3) $B_{a,v}$

$$B_{a,v} \;:=\; B_{a_1}(v_1) \otimes \cdots \otimes B_{a_n}(v_n) \;=\; B_{a_1}(v_1) \times \cdots \times B_{a_n}(v_n) \;=\; v\restriction\{j \mid v_j = a_j\}, \tag{11}$$

where $v = (v_1, v_2, \ldots, v_n)$ runs through I, form the corresponding tensor product basis B_a of B_a

$$\mathbb{Z}^{I_1 \times \cdots \times I_n} \;=\; \mathbb{Z}^{I_1} \otimes \cdots \otimes \mathbb{Z}^{I_n}. \tag{12}$$

This basis has the advantage that it contains a basis of the subspace of all switchable light patterns. Indeed, for any fixed j, the $B_{a,v}$ with $v_j = a_j$ can be composed from elementary moves $u\restriction j$, but there are not enough such $u\restriction j$ to generate more elements than those in the span of these $B_{a,v}$. Both sets span the same subspace. Summarizing, we have (where $\langle\!\langle \ldots \rangle\!\rangle$ stands for the linear independent span over $\mathbb{Z}$): $\langle\!\langle \ldots \rangle\!\rangle$

Theorem 2.1 (First Basis)**.** *Let* $a \in I := I_1 \times I_2 \times \cdots \times I_n$ *be given. The* $B_{a,v}$ *with* $v \in I$ *form a basis* B_a *of the module of all light patterns over* I,

$$\mathbb{Z}^I \;=\; \langle\!\langle\, B_{a,v} \mid v \in I \,\rangle\!\rangle.$$

Those with $v_j = a_j$ *for at least one* $j \in \{1, 2, \ldots, n\}$ *form a basis of the* $\mathbb{Z}$*-submodule of all switchable light patterns in* $\mathrm{AB}(I_1, I_2, \ldots, I_n) =: (I, \mathcal{M})$,

$$\langle \mathcal{M} \rangle \;=\; \langle\!\langle\, B_{a,v} \mid v \in I \;\text{ with }\; v_j = a_j \;\text{ for at least one }\; j \,\rangle\!\rangle.$$

If a pattern U cannot be switched, then one basis vector $B_{a,v}$ with $v \equiv\!\!\!\!\!\not\;\; a$ (“v *nowhere equal* a ”) must occur in its linear combination of basis vectors; where the “$\equiv$” in “$\equiv\!\!\!\!\!\not\;\;$” stands for “*everywhere*” or “*always*”, i.e., $v \equiv\!\!\!\!\!\not\;\; a$

$$v \equiv\!\!\!\!\!\not\;\; a \quad :\Longleftrightarrow \quad v_j \neq a_j \text{ for } j = 1, \ldots, n\,. \tag{13}$$

Such a $B_{a,v}$ will also occur in a decomposition of a z-times multiple of U. Hence, if U is not switchable then the multiple zU is not switchable either. More precisely, we have:

Corollary 2.2. *The $\mathbb{Z}$-submodule of all switchable light patterns in* $\mathrm{AB}(I_1, I_2, \ldots, I_n)$ *is saturated, i.e., its elementary divisors are units. In particular, if the z-times multiple $zU\colon v \mapsto zU(v)$ ($0 \neq z \in \mathbb{Z}$) of a pattern U can be switched off, then U can be switched off as well.* zU

Based on these results we can introduce another even more convenient basis b_a. Again, $a \in I := I_1 \times I_2 \times \cdots \times I_n$ is a fixed point, and b_a $I \mathbin{\backslash\!\!\backslash} a$

$$I \mathbin{\backslash\!\!\backslash} a \;:=\; \{\, v \in I \mid v \equiv\!\!\!\!\!\not\;\; a \,\} \;=\; \prod_{j=1}^{n} I_j \backslash a_j \;=\; \bigotimes_{j=1}^{n} I_j \backslash a_j. \tag{14}$$

For each $v \in I$, we introduce a new basis vector $b_{a,v}$ as follows: $b_{a,v}$

$$b_{a,v} \;:=\; \begin{cases} \{v\} & \text{if } v \in I \mathbin{\backslash\!\!\backslash} a, \\ \{v\} - (-1)^{|\{j \mid v_j = a_j\}|}\,(B_{a,v} \cap I \mathbin{\backslash\!\!\backslash} a) & \text{else,} \end{cases} \tag{15}$$

where, once again, we identified sets with their characteristic functions, and “$-$” is the minus in $\mathbb{Z}^I$ (“$\backslash$” is the set-theoretic minus). If $v \in I \setminus (I \mathbin{\backslash\!\!\backslash} a)$ then $b_{a,v}$ is one point at v together with a d-dimensional axis-parallel “layer” of the n-dimensional $(k_1 - 1) \times (k_2 - 1) \times \cdots \times (k_n - 1)$ cuboid $I \mathbin{\backslash\!\!\backslash} a$, where $d := |\{j \mid v_j = a_j\}|$. Actually, $b_{a,v}$ takes the value -1 on this layer if d is even (see Figure 3). $-$ $\backslash$

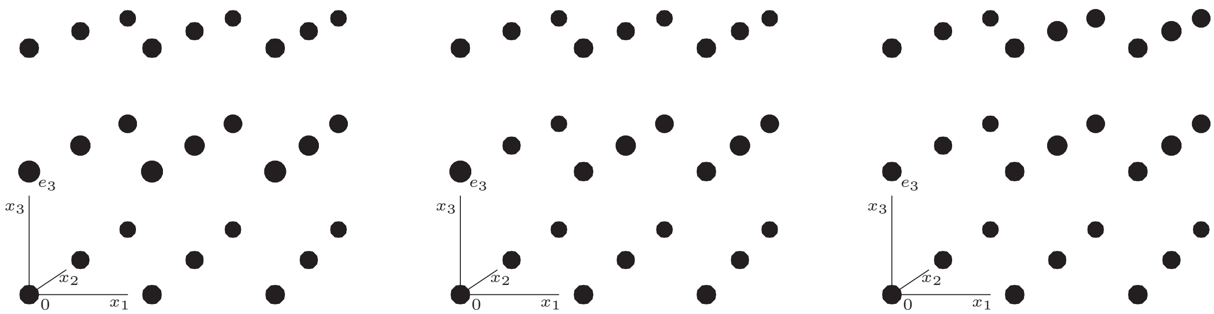
If we want to switch a given pattern U by using the $b_{a,v}$ as moves, then for each $v \in I \setminus (I \mathbin{\backslash\!\!\backslash} a)$, only the basis vector $b_{a,v}$ can switch the point v (as outside $I \mathbin{\backslash\!\!\backslash} a$ the $b_{a,v}$ coincide with the patterns $\{v\}$). After switching off all lights in $I \setminus (I \mathbin{\backslash\!\!\backslash} a)$, for each of the remaining points $v \in I \mathbin{\backslash\!\!\backslash} a$, exactly one among the so far unused basis vectors can switch it, namely $b_{a,v} = \{v\}$. Hence, each pattern can uniquely be written as a linear combination of the $b_{a,v}$, i.e., the $b_{a,v}$ form a basis:

Theorem 2.3 (Second Basis)**.** *Let $a \in I := I_1 \times I_2 \times \cdots \times I_n$ be given. The $b_{a,v}$ with $v \in I$ form a basis b_a of the module of all light patterns over I,*

$$\mathbb{Z}^I \;=\; \langle\!\langle\, b_{a,v} \mid v \in I \,\rangle\!\rangle.$$

Those with $v_j = a_j$ for at least one $j \in \{1, 2, \ldots, n\}$ form a basis of the subspace of all switchable light patterns in $\mathrm{AB}(I_1, I_2, \ldots, I_n) =: (I, \mathcal{M})$,

$$\langle \mathcal{M} \rangle \;=\; \langle\!\langle\, b_{a,v} \mid v \in I \text{ with } v_j = a_j \text{ for at least one } j \,\rangle\!\rangle.$$



The basis vector $B_{0,e_3} =$ $(0,0,1)\restriction 1 + (0,1,1)\restriction 1 + (0,2,1)\restriction 1$

The basis vector $b_{0,e_3} =$ $(0,0,1)\restriction 1 - (1,0,1)\restriction 2 - (2,0,1)\restriction 2$

$J_{(1,1,1),(2,2,2)}$ *from page* 10. *Here* $\operatorname{supp}(J_{(1,1,1),(2,2,2)}) = I \mathbin{\setminus\!\!\setminus} 0$

Figure 3: *Important patterns in* $\mathrm{AB}^3(3)$ (yellow, gray, blue *stand for values of* $+1,\ 0, -1$)

Proof. Only the second part is left to prove. We show, by induction on the number of indices j with $v_j = a_j$, that any $b_{a,v}$ with at least one such j can be switched off:

If there is exactly one such j, then $b_{a,v} = B_{a,v} = v\restriction j$ is just an elementary axis-parallel move. If j is not the only such index, we decrease the state of the bulbs in $v\restriction j$, and obtain

$$\begin{aligned} b_{a,v} - v\restriction j \;&=\; \pm\left[B_{a,v} \cap I \mathbin{\setminus\!\!\setminus} a\right] + \{v\} - v\restriction j \;=\; \pm\Big[\big(\bigcup_{u\in(v\restriction j)\setminus v} B_{a,u}\big) \cap I \mathbin{\setminus\!\!\setminus} a\Big] - \sum_{u\in(v\restriction j)\setminus v} \{u\} \\ &=\; -\sum_{u\in(v\restriction j)\setminus v} \big[\mp(B_{a,u} \cap I \mathbin{\setminus\!\!\setminus} a) + \{u\}\big] \;=\; -\sum_{u\in(v\restriction j)\setminus v} b_{a,u}. \end{aligned} \tag{16}$$

However, each of the patterns $b_{a,u}$ in the last expression can be switched off by the induction assumption. Hence, all $b_{a,v}$ with $v_j = a_j$ for at least one j are switchable, and span a submodule of $\langle\mathcal{M}\rangle$. As this submodule is spanned by basis vectors it is saturated. It also has the same rank as $\langle\mathcal{M}\rangle$, by Theorem 2.1, so that the $b_{a,v}$ with $v_j = a_j$ for at least one j span the whole of $\langle\mathcal{M}\rangle$. □

3 First Normal Form

In this section, we use the basis b_a of the $\mathbb{Z}$-module $\mathbb{Z}^I$ of all light patterns to derive a normal form for the equivalence classes of $\mathrm{AB}[I]$, where we call two classes *equivalent* if they can be transformed into each other by Berlekamp Moves. If we look at a pattern

$$U \;=\; \sum_{v\in I} \lambda_v b_{a,v}, \tag{17}$$

then

$$\lambda_v \;=\; U(v) \quad \text{for all } v \in I \setminus (I \mathbin{\setminus\!\!\setminus} a), \tag{18}$$

since, for $v \in I \setminus (I \mathbin{\setminus\!\!\setminus} a)$, only the basis vector $b_{a,v}$ switches the point v. From this we see that we have to add the basis move $b_{a,v}$ exactly $-U(v)$ many times in order to switch off the light at $v \in I \setminus (I \setminus\!\!\setminus a)$. We have enough basis moves to switch off all v in $I \setminus (I \setminus\!\!\setminus a)$, but afterwards there are no moves in $\langle \mathcal{M} \rangle$ left to modify the pattern. If the board is dark afterwards then the initial pattern was switchable, otherwise not. We call the remaining pattern of burning lights the *normal form* $N_a(U)$ of U with respect to a, $N_a(U)$

$$N_a(U) \;:=\; U - \sum_{v \in I \setminus (I \setminus\!\!\setminus a)} U(v) b_{a,v} \;=\; \sum_{v \in I \setminus\!\!\setminus a} \lambda_v b_{a,v}. \tag{19}$$

If U_1 and U_2 are two patterns, then they can be transformed into each other using regular moves if and only if the difference $U_1 - U_2$ can be switched off, i.e., if and only if $N_a(U_1) - N_a(U_2) \equiv\!\!= 0$ (*"everywhere-zero"*). In other words two patterns are equivalent in this sense if and only if they have the same normal form. The normal forms are unique representatives of the equivalence classes. We have: $\equiv\!\!=$

Theorem 3.1 (First Normal Form)**.** *Let $a \in I := I_1 \times I_2 \times \cdots \times I_n$ be given. Each light pattern $U \in \mathbb{Z}^I$ can be transformed, using regular moves, into a pattern $N_a(U) \in \mathbb{Z}^I$ with*

$$\operatorname{supp}(N_a(U)) \;\subseteq\; I \setminus\!\!\setminus a.$$

This normal form *is uniquely determined, and the map $U \longmapsto N_a(U)$ is linear, i.e.,*

$$N_a(U_1 + U_2) \;=\; N_a(U_1) + N_a(U_2) \qquad \textit{for all} \quad U_1, U_2 \subseteq \mathbb{Z}^I .$$

A pattern U can be switched off if and only if $N_a(U) \equiv\!\!= 0$.

In order to say more about the normal form N_a, we need the patterns $J_{a,v} \in \mathbb{Z}^I$, $v \in I$, given by (see Figure 3) $J_{a,v}$

$$J_{a,v}(u) \;:=\; \begin{cases} 0 & \text{if } u \notin \lfloor a, v \rceil , \\ 1 & \text{if } u \in \lfloor a, v \rceil \text{ and } u_j = a_j \text{ for evenly many } j, \\ -1 & \text{if } u \in \lfloor a, v \rceil \text{ and } u_j = a_j \text{ for oddly many } j, \end{cases} \tag{20}$$

where $\lfloor a, v \rceil$

$$\lfloor a, v \rceil \;:=\; \{a_1, v_1\} \times \{a_2, v_2\} \times \ldots \times \{a_n, v_n\}. \tag{21}$$

With this we have the following explicit formula for the normal form of a pattern:

Theorem 3.2 (Normal Form Formula)**.** *Let $a \in I := I_1 \times I_2 \times \cdots \times I_n$. The normal form $N_a(U)$ of a pattern $U \colon I \longrightarrow \mathbb{Z}$ is determined, on its actual domain $I \setminus\!\!\setminus a$, by the formula*

$$N_a(U)(v) \;=\; \sum_{x \in I} J_{a,v}(x)\, U(x) \qquad \textit{for all} \quad v \in I \setminus\!\!\setminus a .$$

Proof. We transform U into $N_a(U)$ with its characterizing property $\operatorname{supp}(N_a(U)) \subseteq I \setminus\!\!\setminus a$. For each fixed given $x \in I \setminus (I \setminus\!\!\setminus a)$, we have to switch off the corresponding bulb by switching $b_{a,x}$. Since the original state of x is $U(x)$, we have to add $-U(x)\, b_{a,x}$. A bulb at v in $I \setminus\!\!\setminus a$ is switched by such a move if and only if $x \in \lfloor a, v \rceil$. Therefore, its original state

$$U(v) \;=\; \big((-1)^0\, U(x)\big)|_{x=v} \;=\; \Big((-1)^{|\{j \,\mid\, x_j = a_j\}|}\, U(x)\Big)|_{x=v} \tag{22}$$

will increase by

$$(-1)^{|\{j \,\mid\, x_j = a_j\}|}\, U(x) \tag{23}$$

for each

$$x \;\in\; \big(I \setminus (I \setminus\!\!\setminus a)\big) \cap \lfloor a, v \rceil \;=\; \lfloor a, v \rceil \setminus v, \tag{24}$$

i.e.,

$$N_a(U)(v) \;=\; \sum_{x \in \lfloor a, v \rceil} (-1)^{|\{j \,\mid\, x_j = a_j\}|}\, U(x) \;=\; \sum_{x \in I} J_{a,v}(x)\, U(x). \tag{25}$$

□

From the two last theorems we derive:

Theorem 3.3 (Switchability Criterion)**.** *Assume* $a \in I := I_1 \times I_2 \times \cdots \times I_n$ *, and let, for* $j = 1, 2, \ldots, n$ *, the map* $\varphi_j \colon I_j \longrightarrow I_j$ *be such that for any* $x_j \in I_j$ *there exists* $t_j \in \mathbb{N}$ *with* $\varphi_j^{t_j}(x_j) = a_j$ *. Define the map* $\varphi \colon I \longrightarrow I$ *by* $\varphi(x) := (\varphi_1(x_1), \varphi_2(x_2), \ldots, \varphi_n(x_n))$ *. Then for patterns* $U \colon I \longrightarrow \mathbb{Z}$ *, the following statements are equivalent:*

(i) U *can be switched off.*

(ii) $\sum_{x \in I} J_{a,v}(x)\, U(x) \;=\; 0$ *for all* $v \in I \setminus\!\!\setminus a$ *.*

(iii) $\sum_{x \in I} J_{v,\varphi(v)}(x)\, U(x) \;=\; 0$ *for all* $v \in I \setminus\!\!\setminus a$ *.*

This equivalence holds also modulo $r \geq 2$ *, i.e. over* $\mathbb{Z}_r$ *, in* $\mathrm{AB}_r[I]$ *.*

Proof. By Theorems 3.2 and 3.1 $(ii) \Rightarrow (i) \Rightarrow (iii)$, so that we only have to prove the implication $(iii) \Rightarrow (ii)$. Let $v \in I \setminus\!\!\setminus a$ be given, and select $t = (t_1, t_2, \ldots, t_n) \in \mathbb{N}^n$ by choosing

$$t_j > 0 \;\text{ minimal with }\; \varphi^{t_j}(v_j) \;=\; a_j\;, \quad j = 1, 2, \ldots, n. \tag{26}$$

For $s \in \mathbb{N}^n$, define $\varphi^s \colon I \longrightarrow I$ by

$$\varphi^s(x) \;:=\; (\varphi_1^{s_1}(x_1),\, \varphi_2^{s_2}(x_2), \ldots,\, \varphi_n^{s_n}(x_n)), \;\text{ i.e., }\; \varphi^t(v) \;=\; a. \tag{27}$$

Then, with $\mathbf{1} = (1, 1, \ldots, 1)$, 1

$$\sum_{x \in I} J_{a,v}(x)\, U(x) \;=\; \sum_{x \in I} J_{v,\varphi^t(v)}(x)\, U(x) \;=\; \sum_{0 \leq t' \leq t-1} \sum_{x \in I} J_{\varphi^{t'}(v), \varphi^{t'+1}(v)}(x)\, U(x) \overset{(iii)}{=} 0, \tag{28}$$

as

$$\sum_{0 \leq t' \leq t-1} J_{\varphi^{t'}(v), \varphi^{t'+1}(v)} \;=\; J_{v, \varphi^t(v)}. \tag{29}$$

This follows inductively from the fact that any pair of "neighboring cubes" e_j

$$\lfloor \varphi^{t'}(v), \varphi^{t'+1}(v) \rceil \quad \text{and} \quad \lfloor \varphi^{t'+e_j}(v), \varphi^{t'+e_j+1}(v) \rceil\,, \quad \text{where } e_j := (0,\dots,0,1,0,\dots,0), \tag{30}$$

"overlaps and cancels" in one side $\lfloor \varphi^{t'+e_j}(v), \varphi^{t'+1}(v) \rceil$, they "add up" to a "bigger cuboid" $\lfloor \varphi^{t'}(v), \varphi^{t'+e_j+1}(v) \rceil$. More precisely,

$$J_{\varphi^{t'}(v),\varphi^{t'+1}(v)} + J_{\varphi^{t'+e_j}(v),\varphi^{t'+e_j+1}(v)} \;=\; J_{\varphi^{t'}(v),\varphi^{t'+e_j+1}(v)}. \tag{31}$$

In the simplest case $t := (2,1,\dots,1) = e_1 + 1$

$$\sum_{0\le t'\le t-1} J_{\varphi^{t'}(v),\varphi^{t'+1}(v)} \;=\; J_{\varphi^{0}(v),\varphi^{1}(v)} + J_{\varphi^{e_1}(v),\varphi^{e_1+1}(v)} \;=\; J_{\varphi^{0}(v),\varphi^{e_1+1}(v)} \;=\; J_{v,\varphi^{t}(v)}. \tag{32}$$

□

4 Second Normal Form

Here we present another normal form based on the following definition:

Definition 4.1. We say that a pattern $U \in \mathbb{Z}^I$ has *vanishing row sums*, respectively *modulo* $r \geq 2$ *vanishing row sums*, if for all $v \in I$ and $j = 1,\dots,n$

$$\sum_{x\in v\restriction j} U(x) \;=\; 0, \quad \text{respectively} \quad \sum_{x\in v\restriction j} U(x) \;\equiv\; 0 \pmod r.$$

Only certain modular cases will be nice enough for our applications in part two of this paper. Therefore, we state the following lemma only for the modulo r case:

Lemma 4.2. *Assume* $a \in I := I_1 \times I_2 \times \cdots \times I_n$ *, and let* $r \geq 2$ *. To any pattern* $U \in \mathbb{Z}^I$*, there exists exactly one* $\bar{U} \in \mathbb{Z}^I$ *with*

(i) $\bar{U}|_{I\Bbbk a} = U|_{I\Bbbk a}$.

(ii) $0 \leq \bar{U}(x) \leq r-1$ *for all* $x \in I \setminus (I\Bbbk a)$.

(iii) $\bar{U}$ *has modulo* r *vanishing row sums.*

In particular, in $\mathrm{AB}_r(k_1,k_2,\dots,k_n)$ *, there are exactly* $r^{(k_1-1)(k_2-1)\cdots(k_n-1)}$ *patterns with vanishing row sums.*

Proof. Let, w.l.o.g., $a := 0 \in I$. After setting $\bar{U}(x) := U(x)$ for $x \in I\Bbbk 0$, there is only one way to choose the values $\bar{U}(x)$ for points x of weight $n-1$. If, say, $x_j = 0$ then we have to choose $\bar{U}(x)$ such that the sum over $x\restriction j$ vanishes, and the summands $\bar{U}(x')$ with $x' \in (x\restriction j)\backslash x$ are already fixed. Now, if x has weight $n-2$, say

$$x_{j_1} \;=\; x_{j_2} \;=\; 0,\;\; j_1 \neq j_2, \tag{33}$$

we have to choose $\bar{U}(x)$ such that the sum over the plane $x\restriction\{j_1, j_2\}$ vanishes. Only then any of the two row sums

$$\sum_{x'\in x\restriction j_1} \bar{U}(x') \quad \text{and} \quad \sum_{x'\in x\restriction j_2} \bar{U}(x') \tag{34}$$

will vanish, as the plane $x\restriction\{j_1, j_2\}$ is already made up of "vanishing parallels" to $x\restriction j_1$, respectively $x\restriction j_2$. Proceeding in this manner, we come to points x of lower and lower weight. The very last step will be to choose $U(0) := -\sum_{x\neq 0} U(x)$, so that the sums over the coordinate axes will vanish as all parallel rows will have vanishing sums already. □

For simplicity, we work from here on only over the boards I of size $k \times k \times \cdots \times k$. We present the following somehow more symmetric normal form:

Theorem 4.3 (Second Normal Form)**.** *Let r be coprime to k, and $t\,(-k)^n \equiv 1 \pmod{r}$. Any light pattern $U \in \mathbb{Z}_r^I$ in $\mathrm{AB}_r^n(k)$ can be transformed into a pattern $N(U)$ with vanishing row sums. This* normal form *$N(U)$ of U is uniquely determined, and the group endomorphism $N\colon U \longmapsto N(U)$ is given by*

$$N(\{u\}) \;=\; t \sum_{J\subseteq\{1,\ldots,n\}} (-k)^{n-|J|}(u\restriction J) \;\in\; \mathbb{Z}_r^I,$$

In other words, for $v \in I$,

$$N(\{u\})(v) \;=\; t\,(1-k)^{|\{i\mid v_i=u_i\}|} \;\in\; \mathbb{Z}_r.$$

Under the stronger assumption that r divides $k-1$ we have

$$N(\{u\}) \;=\; (-1)^n(I\setminus u) \quad \textit{and} \quad N(U)(v) \;=\; (-1)^n \sum_{u\in I\setminus v} U(u).$$

Proof. Provided that a normal form $N\colon \mathbb{Z}_r^I \longrightarrow \mathbb{Z}_r^I$ exists, the uniqueness follows immediately from the fact that, by Lemma 4.2 and Theorem 3.1, there are only as many patterns with vanishing row sums as there are equivalence classes. However, it is straightforward to check that the suggested patterns

$$N(\{u\}) \;:=\; \sum_{J\subseteq\{1,\ldots,n\}} t\,(-k)^{n-|J|}(u\restriction J) \tag{35}$$

have vanishing row sums, and are in second normal form. If, e.g., we sum along the line $(*, v_2, \ldots, v_s, u_{s+1}, \ldots, u_n)$, where $(v_2, \ldots, v_s) \equiv\!\!\!\!/\; (u_2, \ldots, u_s)$, then we have to sum up for each possible first coordinate $v_1 \neq u_1$ the value

$$\sum_{J\supseteq\{1,\ldots,s\}} t\,(-k)^{n-|J|} \;=\; t\,(1-k)^{n-s} \tag{36}$$

and for $v_1 = u_1$ the value

$$\sum_{J\supseteq\{2,\ldots,s\}} t\,(-k)^{n-|J|} = \sum_{J\supseteq\{1,\ldots,s\}} t\,(-k)^{n-|J|} + \sum_{1\notin J\supseteq\{2,\ldots,s\}} t\,(-k)^{n-|J|} \;=\; t\,(1-k)^{n-s} + \; t\,(-k)(1-k)^{n-s}, \tag{37}$$

which makes a total of

$$(k-1)\,t\,(1-k)^{n-s} \;+\; t\,(1-k)^{n-s} \;+\; t\,(-k)(1-k)^{n-s} \;=\; 0. \tag{38}$$

Furthermore, all summands in $N(\{u\})$ are switchable, except the one to $J=\emptyset$, which is

$$t\,(-k)^n\{u\} \;=\; \{u\} \;\in\; \mathbb{Z}_r^I \tag{39}$$

Hence, modulo r our $N(\{u\})$ is a switchable pattern plus $\{u\}$. This means that $\{u\}$ can be transformed into $N(\{u\})$, so that, indeed, the group endomorphism

$$N\colon U \longmapsto N(U), \quad N(\{u\}) \;:=\; \sum_{J\subseteq\{1,\ldots,n\}} t\,(-k)^{n-|J|}(u{\upharpoonright}J) \tag{40}$$

is a normal form.

Our pointwise formula follows from this, similarly as in Equation (36) above, since for any fixed point $v \in I$

$$v \in u{\upharpoonright}J \quad\Longleftrightarrow\quad J \supseteq \{i \,\mathrel{\rlap{\smash{\,\vdots}}}\, v_i \neq u_i\}. \tag{41}$$

Under the stronger assumption that r divides $k-1$, the values of this formula at points $v \notin I\setminus\!\!\setminus u$ vanish, so that

$$N(\{u\}) \;=\; t\,(I\setminus\!\!\setminus u) \;=\; (-1)^n(I\setminus\!\!\setminus u) \;\in\; \mathbb{Z}_r^I, \tag{42}$$

and

$$N(U)(v) \;=\; \sum_{u\in U} N(\{u\})(v) \;=\; \sum_{u\in I} U(u)\,(-1)^n(I\setminus\!\!\setminus u)(v) \;=\; (-1)^n \sum_{u\in I\setminus\!\!\setminus v} U(u). \tag{43}$$

□

We obtain the following obvious corollary:

Corollary 4.4 (Switchability Criterion)**.** *Let $U \in \mathbb{Z}^I$ be a pattern on a $k\times k\times\cdots\times k$ board I. If r divides $k-1$, the following statements are equivalent:*

(i) U can be switched off modulo r.

(ii) $\sum_{u\in I\setminus\!\!\setminus v} U(u) \;\equiv\; 0 \pmod r$ for all $v \in I$.

5 Polynomials as Light Patterns

This section contains the original idea behind this paper. It reveals a connection between polynomial maps and affine Berlekamp $\mathrm{AB}(k_1,\ldots,k_n)$, which we play on the board [k)

k

$$I \;=\; [\mathrm{k}) \;:=\; [k_1)\times\cdots\times[k_n)\;, \quad \mathrm{k} \;:=\; (k_1,\ldots,k_n), \tag{44}$$

where $[n)$

$(n]$

$$[n) \;=\; [0,n) \;:=\; \{0,1,\ldots,n-1\} \quad \text{and} \quad (n] \;=\; (0,n] \;:=\; \{1,2,\ldots,n\}. \tag{45}$$

More precisely, we always work with polynomial maps on what we call a *Berlekamp* (k−1)-*Domain*. That is a Cartesian product $\mathfrak{X}$

$$\mathfrak{X} \;:=\; \mathfrak{X}_1 \times \cdots \times \mathfrak{X}_n \;\subseteq\; \mathbb{F}^n, \quad |\mathfrak{X}_j| = k_j{-}1 \quad \text{for} \quad j \in (n] \,, \tag{46}$$

over a field $\mathbb{F}$, with the property that

$$L_{\mathfrak{X}_j,s} \;:=\; (-1)^s \sum_{\substack{S\subseteq\mathfrak{X}_j \\ |\mathfrak{X}_j\setminus S|=s}} \prod S \;\neq\; 0 \quad \text{ for all } \; j \in (n] \text{ and } s \in [k_j) \,, \tag{47}$$

where $\prod S := \prod_{\sigma\in S} \sigma$. In other words, $\prod S$ $L_{\mathfrak{X},v}$

$$L_v \;=\; L_{\mathfrak{X},v} \;:=\; \prod_{j=1}^{n} L_{\mathfrak{X}_j,v_j} \;\neq\; 0 \quad \text{for all } \; v \in [\mathrm{k}) \,. \tag{48}$$

Note that the k-board $[\mathrm{k})$ is bigger than the (k−1)-domain $\mathfrak{X}$, $|[k_j)| > |\mathfrak{X}_j|$ for all $j \in (n]$. Therefore, each map $\mathfrak{X} \longrightarrow \mathbb{F}$ can be described by different polynomials $\mathbb{F}[X^{<\mathrm{k}}]$

$$P \;\in\; \mathbb{F}[X^{<\mathrm{k}}] \;:=\; \{\, P \in \mathbb{F}[X_1, \ldots, X_n] \;\vert\; \deg_j(P) < k_j, \; j \in (n] \,\}. \tag{49}$$

However, we will see that such interpolation polynomials P are unique up to a “switchable part”. In this respect, the map $\Psi = \Psi_{\mathfrak{X}}$

$$\Psi = \Psi_{\mathfrak{X}} : \; \mathbb{Z}^{[\mathrm{k})} \;\longrightarrow\; \mathbb{F}[X^{<\mathrm{k}}], \quad U \longmapsto \Psi_{\mathfrak{X}}(U) \;:=\; \sum_{v\in[\mathrm{k})} L_{\mathfrak{X},v} U(v) X^v, \tag{50}$$

with $X^v := X_1^{v_1} X_2^{v_2} \cdots X_n^{v_n}$, is of central interest. The most important case is when the $\mathfrak{X}_j$ are made up of k_j^{th} roots of unity different from 1 over $\mathbb{F} = \mathbb{C}$, i.e., X^v $\mathfrak{X}(k_j)$

$$\mathfrak{X}_j \;=\; \mathfrak{X}(k_j) \;:=\; \{\, \xi_{k_j}^{\,t} \;\vert\; t = 1, 2, \ldots, k_j - 1 \,\} \quad \text{ where } \quad \xi_{k_j} := e^{2\pi\sqrt{-1}/k_j} \in \mathbb{C}. \tag{51}$$

In this case, for all $v \in [\mathrm{k})$, $\mathfrak{X}(\mathrm{k})$

$$L_v \;=\; L_{\mathfrak{X}(\mathrm{k}),v} = \; 1 \quad \text{ where } \quad \mathfrak{X}(\mathrm{k}) \;:=\; \mathfrak{X}(k_1) \times \cdots \times \mathfrak{X}(k_n), \tag{52}$$

as

$$\sum_{s\in[k_j)} L_{\mathfrak{X}(k_j),s} x^s \;=\; (x - \xi_{k_j}^{\,1}) \cdots (x - \xi_{k_j}^{\,k_j-1}) \;=\; \frac{x^{k_j} - 1}{x - 1} \;=\; \sum_{s\in[k_j)} x^s, \tag{53}$$

i.e., we end up with the simpler $\mathbb{Z}$-module isomorphism

$$\Psi_{\mathfrak{X}(\mathrm{k})} : \; \mathbb{Z}^{[\mathrm{k})} \;\longrightarrow\; \mathbb{Z}[X^{<\mathrm{k}}], \quad U \longmapsto \Psi_{\mathfrak{X}(\mathrm{k})}(U) \;:=\; \sum_{v\in[\mathrm{k})} U(v) X^v. \tag{54}$$

Via this isomorphism, we may view light patterns in $\mathbb{Z}^{[\mathrm{k})}$ and polynomials $\mathbb{Z}[X^{<\mathrm{k}}]$ as the same thing. However, polynomials P over $\mathbb{Z}$ also give rise to polynomial maps

$P|_{\mathfrak{X}(\mathrm{k})}: \mathfrak{X}(\mathrm{k}) \longrightarrow \mathbb{C}$, $x \longmapsto P(x)$, and these maps are important in applications and structural examinations, as we will see. In what follows, we work over general Berlekamp (k−1)-Domains $\mathfrak{X}$, and examine the composed map $P|_{\mathfrak{X}(\mathrm{k})}$

$$\begin{aligned} \mathbb{Z}^{[\mathrm{k})} &\longrightarrow \mathbb{F}[X^{<\mathrm{k}}] \longrightarrow \mathbb{F}^{\mathfrak{X}} \\ U &\longmapsto \Psi_{\mathfrak{X}}(U) \longmapsto \Psi_{\mathfrak{X}}(U)|_{\mathfrak{X}}, \end{aligned} \tag{55}$$

where $|_{\mathfrak{X}}$ denotes restriction to polynomial maps on $\mathfrak{X}$. Our first main result shows that Berlekamp's game can be used to decide if, for polynomials $P = \Psi_{\mathfrak{X}}(U)$, the polynomial map $P|_{\mathfrak{X}}$ describes the zero map: $|_{\mathfrak{X}}$

Theorem 5.1. *Let $\mathfrak{X} \subseteq \mathbb{F}^n$ be a Berlekamp* (k−1)*-Domain. For patterns $U \in \mathbb{Z}^{[\mathrm{k})}$ the following statements are equivalent:*

(i) U can be switched off.

(ii) $\Psi_{\mathfrak{X}}(U)|_{\mathfrak{X}} \equiv 0$.

Proof. We examine the one-to-one correspondence

$$\Psi = \Psi_{\mathfrak{X}}: \mathbb{Z}^{[\mathrm{k})} \longrightarrow \mathbb{F}[X^{<\mathrm{k}}], \quad U \longmapsto \sum_{v \in [\mathrm{k})} L_v U(v) X^v. \tag{56}$$

What happens on the right side of this correspondence if we add a move $v{\upharpoonright}j$ on the left side? Well, if w.l.o.g. $v_j = 0$, then

$$\begin{aligned} \Psi(v{\upharpoonright}j) &= \sum_{v \in v{\upharpoonright}j} L_v X^v = \sum_{s \in [k_j)} L_{v+se_j} X^{v+se_j} = \sum_{s \in [k_j)} (\prod_{i \neq j} L_{\mathfrak{X}_i, v_i}) L_{\mathfrak{X}_j, s} X^v X^{se_j} \\ &= (\prod_{i \neq j} L_{\mathfrak{X}_i, v_i}) X^v \prod_{x \in \mathfrak{X}_j} (X_j - x), \end{aligned} \tag{57}$$

and this polynomial vanishes on $\mathfrak{X}$. Therefore, the right side does not change when we perform an elementary move $v{\upharpoonright}j$,

$$\Psi(U \pm (v{\upharpoonright}j))|_{\mathfrak{X}} = \Psi(U)|_{\mathfrak{X}}. \tag{58}$$

Consequently, we also come off clear with many moves, and may apply our first normal form N_a with $a := \mathrm{k} - 1$. We obtain

$$\Psi(N_{\mathrm{k}-1}(U))|_{\mathfrak{X}} = \Psi(U)|_{\mathfrak{X}}, \tag{59}$$

but also

$$\deg_j(N_{\mathrm{k}-1}(\Psi(U))) < k_j - 1 \quad \text{for all } j \in (n]. \tag{60}$$

By the Interpolation Theorem, see e.g. [Scha1, Section 2] or [AlTa, Lemma 2.1], there is only one interpolation polynomial with such restricted partial degrees to any map on $\mathfrak{X}$, i.e., $\Psi(N_{\mathrm{k}-1}(U))$ is uniquely determined by $\Psi(U)|_{\mathfrak{X}}$. Based on this uniqueness, we can conclude as follows,

$$\Psi(U)|_{\mathfrak{X}} \equiv 0 \iff \Psi(N_{\mathrm{k}-1}(U)) = 0 \iff N_{\mathrm{k}-1}(U) \equiv 0 \overset{3.1}{\iff} U \text{ is switchable.} \tag{61}$$

□

The last theorem is important since it builds a bridge from Berlekamp to many applications. However, it also provides some insights about the game itself. Since two patterns U_1 and U_2 are equivalent if and only if their difference $U_1 - U_2$ is switchable, we obtain the following corollary:

Corollary 5.2. *Let $\mathfrak{X} \subseteq \mathbb{F}^n$ be a Berlekamp* (k−1)*-Domain. The group homomorphism $\mathbb{Z}^{[k)} \longrightarrow \mathbb{F}^{\mathfrak{X}}$, $U \longmapsto \Psi_{\mathfrak{X}}(U)|_{\mathfrak{X}}$ is a complete invariant for the equivalence classes of Affine Berlekamp $\mathrm{AB}([k_1), \ldots, [k_n))$, i.e., two patterns U_1 and U_2 are equivalent if and only if $\Psi_{\mathfrak{X}}(U_1)|_{\mathfrak{X}} = \Psi_{\mathfrak{X}}(U_2)|_{\mathfrak{X}}$.*

We also have the following modular corollary:

Corollary 5.3. *Let $\mathfrak{X} \subseteq \mathbb{F}^n$ be a Berlekamp* (k−1)*-Domain. For patterns $U \in \mathbb{Z}^{[\mathrm{k})}$ and any $r \in \mathbb{N}$ the following holds:*

$$U \text{ can be switched off modulo } r \quad \Longrightarrow \quad \Psi_{\mathfrak{X}}(U)|_{\mathfrak{X}} \equiv 0 \pmod{r\mathbb{Z}[\textstyle\bigcup_j \mathfrak{X}_j\,]}.$$

Proof. The pattern U can be switched off modulo r if and only if there is a switchable pattern $\widehat{U}$ such that $U - \widehat{U}$ is everywhere zero modulo r, i.e., if and only if

$$U = r\mathring{U} + \widehat{U} \quad \text{with } \mathring{U}, \widehat{U} \in \mathbb{Z}^I \text{ and } \widehat{U} \text{ switchable.} \tag{62}$$

Therefore,

$$\Psi(U)|_{\mathfrak{X}} = r\Psi(\mathring{U})|_{\mathfrak{X}} + \Psi(\widehat{U})|_{\mathfrak{X}} \overset{5.1}{\equiv} 0 \pmod{r\mathbb{Z}[\textstyle\bigcup_j \mathfrak{X}_j\,]}. \tag{63}$$

□

6 The Polynomial Algebra of Light Patterns

In the rest of the paper we examine $\mathrm{AB}(\mathbb{Z}_{k_1}, \mathbb{Z}_{k_2}, \ldots, \mathbb{Z}_{k_n})$, i.e., Berlekamp on the board I

$$I := \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n} = \langle e_1, e_2, \ldots, e_n \rangle, \tag{64}$$

where the e_j are the standard basis vectors of the $\mathbb{Z}$-module I. This setting is general enough to allow all possible board sizes $k_1 \times k_2 \times \cdots \times k_n$, just as the board [k) used in the last section, but it also provides an additive structure on the board I. Since we already have an additive structure on the set of light patterns $\mathbb{Z}^I$, we have to be careful. Subsets of I are usually viewed as 0-1 patterns in $\mathbb{Z}^I$ and added in $(\mathbb{Z}^I, +)$, while elements of I are always added in $(I, +)$. We also provide a multiplicative copy $(X^I, \cdot)$ of the additive group $(I, +)$. We write X^v for the copy of an element $v \in I$, and set e_j X^I, X^v

$$X^u X^v = X^u \cdot X^v := X^{u+v}, \tag{65}$$

i.e.,

$$(I, +) \cong (X^I, \cdot) := (\{ X^v \mid v \in I \}, \cdot) \qquad \text{via} \qquad v \longmapsto X^v. \tag{66}$$

We will work in the group algebra $\mathbb{Z}X^I \subseteq \mathbb{Q}X^I$ of X^I over $\mathbb{Z}$, i.e., the set of all formal $\mathbb{Z}X^I$

linear combinations of elements of X^I, with coefficients in $\mathbb{Z}$, and with distributively extended multiplication. When we study subsets and subgroups $U \subseteq I$, the notation ΣX^U

$$\Sigma X^U := \sum_{u \in U} X^u, \tag{67}$$

and the following folkloric lemma will be helpful:

Lemma 6.1. *Let U_1 and U_2 be subgroups of $I := \mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \cdots \times \mathbb{Z}_{k_n}$, with set-theoretic sum $U_1 + U_2 := \{ u_1 + u_2 \mid u_1 \in U_1,\, u_2 \in U_2 \}$. In $\mathbb{Q}X^I$ it holds that*

$$\frac{\Sigma X^{U_1}}{|U_1|}\,\frac{\Sigma X^{U_2}}{|U_2|} \;=\; \frac{\Sigma X^{U_1+U_2}}{|U_1+U_2|}\,, \quad \textit{in particular,} \quad \frac{\Sigma X^{U_1}}{|U_1|} \quad \textit{is an idempotent.} \tag{68}$$

Our $\mathbb{Z}$-algebra $\mathbb{Z}X^I$ is a free $\mathbb{Z}$-module with basis X^I isomorphic to the $\mathbb{Z}$-module of light patterns $\mathbb{Z}^I$, Ψ_{k}

$$\mathbb{Z}^I \;\cong\; \mathbb{Z}X^I \qquad \text{via} \qquad \Psi_{\mathrm{k}} :\, U \longmapsto \sum_{v \in I} U(v)\, X^v. \tag{69}$$

Based on this isomorphy, we may view $\mathbb{Z}X^I$ as our set of light patterns, where the axis-parallel moves have the form $\Sigma X^{v \upharpoonright j}$. In what follows we will show that the isomorphism $\Sigma X^{v \upharpoonright j}$ map Ψ_{k} is basically the same as the map $\Psi_{\mathfrak{X}(\mathrm{k})}$ in Equation (54), and that $\mathbb{Z}X^I$ and $\mathbb{Z}[X^{<\mathrm{k}}]$ are isomorphic $\mathbb{Z}$-modules. We start by setting X_j

$$X_j := X^{e_j}. \tag{70}$$

With this, the elements of the algebra can be written as polynomials in $X_1, \ldots, X_n$, as the elements of I can be written as $\mathbb{Z}$-linear combinations of the e_j. The elements of the algebra can even uniquely be written as polynomials in $X_1, \ldots, X_n$, if we use elements of $\mathbb{Z}_{k_j}$ as exponents of X_j, $j = 1, \ldots, n$, and define

$$X_j^{(z + k_j\mathbb{Z})} := X_j^z, \tag{71}$$

which is well defined as

$$X_j^{k_j} \;=\; X^{k_j e_j} \;=\; X^0 \;=\; 1. \tag{72}$$

Therefore, the group algebra $\mathbb{Z}X^I$ is nothing else but the polynomial $\mathbb{Z}$-algebra $\mathbb{Z}[X_1, \ldots, X_n]$ with elements of $\mathbb{Z}_{k_1} \times \mathbb{Z}_{k_2} \times \ldots \times \mathbb{Z}_{k_n}$ as exponents and multiindex notation,

$$X^{(v_1, \ldots, v_n)} \;=\; X_1^{v_1} X_2^{v_2} \cdots X_n^{v_n}. \tag{73}$$

More precisely, if we denote the representative of an element $z \in \mathbb{Z}_{k_j}$ in $[k_j)$ by $\hat{z}$, i.e. $z = \hat{z} + k_j\mathbb{Z}$, and extend this notation to an operation on I and $\mathbb{Z}X^I$ by defining

$$\widehat{(v_1, \ldots, v_n)} := (\hat{v}_1, \ldots, \hat{v}_n) \qquad \text{and} \qquad \widehat{\sum_{v \in I} P_v X^v} := \sum_{v \in I} P_v X^{\hat{v}}, \tag{74}$$

then each $P \in \mathbb{Z}X^I$ corresponds to an ordinary polynomial $\widehat{P} \in \mathbb{Z}[X_1, \ldots, X_n]$ with partial degrees $\deg_j \widehat{P} < k_j$. The diagram $\widehat{P}$

$$\begin{array}{ccc} \mathbb{Z}^I & \xrightarrow{\Psi_{\mathrm{k}}} & \mathbb{Z}X^I \ni P \\ & \searrow^{\Psi_{\mathfrak{X}(\mathrm{k})}} \circlearrowleft & \downarrow \qquad \updownarrow \\ & & \mathbb{Z}[X^{<\mathrm{k}}] \ni \widehat{P} \end{array} \tag{75}$$

of group isomorphisms commutes. The advantage of the new structure is that it is closed under multiplication, $\mathbb{Z}[X^{<\mathrm{k}}]$ is not. By identifying all three structures we obtain a multiplication on the set of light patterns, which we will study in Section 8. We are also able to substitute numbers $\zeta_1, \ldots, \zeta_n \in \mathbb{C}$ into our new kind of polynomials $P \in \mathbb{Z}X^I$,

$$P(\zeta_1, \ldots, \zeta_n) \;=\; P|_{X=(\zeta_1,\ldots,\zeta_n)} \;:=\; \widehat{P}(\zeta_1, \ldots, \zeta_n). \tag{76}$$

In particular,

$$(\zeta_1, \ldots, \zeta_n)^v \;=\; X^v|_{X=(\zeta_1,\ldots,\zeta_n)} \;:=\; \zeta_1^{\hat{v}_1} \cdots \zeta_n^{\hat{v}_n}. \tag{77}$$

Usually, this substitution does not go well together with the multiplication in $\mathbb{Z}X^I$. However, as

$$\zeta_j^{\hat{v}_j + \hat{w}_j} \;=\; \zeta_j^{\widehat{v_j + w_j}} \quad \text{if} \quad \zeta_j^{k_j} = 1\,, \tag{78}$$

we have the following important special case:

Proposition 6.2. *If, for* $j = 1, \ldots, n$ *,* ζ_j *is a* k_j^{th} *root of unity, then substitution* $\mathbb{Z}X^I \longrightarrow \mathbb{C}$ *,* $P \longmapsto P(\zeta_1, \ldots, \zeta_n)$ *is a* $\mathbb{Z}$*-algebra homomorphism.*

Actually, the $k_1 k_2 \cdots k_n = |I|$ possible substitution homomorphisms are exactly the irreducible characters of the commutative group I .

7 Switchable Subspaces

In this section we study $\mathrm{AB}^n(\mathbb{Z}_k)$, $2 \le k \in \mathbb{N}$, and the switchability of subgroups $U \le I := \mathbb{Z}_k^n$ as 0-1 light patterns. Surprisingly, the switchability of a subgroup can be characterized in terms of orthogonality relations, which suddenly involves the multiplicative structure on $\mathbb{Z}_k$. Based on this fact, we speak about subspaces U rather than subgroups. Actually, any subgroup of $\mathbb{Z}_k^n$ is already a subspace (submodule) of $\mathbb{Z}_k^n$ viewed as a free $\mathbb{Z}_k$-module. We define *orthogonality* for elements $v, w \in I$ and subsets $U \subseteq I$ by $I := \mathbb{Z}_k^n$ $(v \cdot w)$ $v \perp U$

$$v \perp w \quad :\Longleftrightarrow \quad (v \cdot w) := \sum_{j \in (n]} v_j w_j = 0 \qquad \text{and} \qquad v \perp U \quad :\Longleftrightarrow \quad \forall\, u \in U : v \perp u, \tag{79}$$

and make the following important observation:

Theorem 7.1. *Let* $k \ge 2$ *,* $\xi := e^{2\pi\sqrt{-1}/k} \in \mathbb{C}$ *,* $f \in \mathbb{Z}_k^n$ *and* $\xi^f := (\xi^{f_1}, \xi^{f_2}, \ldots, \xi^{f_n})$ *. For subspaces* $U \le \mathbb{Z}_k^n$ *, and* $r \in \mathbb{N}$ *not dividing* $|U|$ *, the following statements are equivalent:* ξ^f

(i) $f \perp U$.

(ii) $\Sigma X^U|_{X=\xi^f} \neq 0$.

(iii) $\Sigma X^U|_{X=\xi^f} \not\equiv 0 \pmod{r\mathbb{Z}[\xi]}$.

(iv) $\Sigma X^U|_{X=\xi^f} = |U|$.

Proof. In view of Lemma 6.1, it is enough to prove the equivalence of statement (i), (ii) and (iv) only for cyclic subspaces U, $U =: \langle u \rangle$. Using the univariate polynomial

$$S(x) := x^0 + x^1 + \cdots + x^{k-1} = \frac{x^k - 1}{x - 1} = (x - \xi^1)(x - \xi^2) \cdots (x - \xi^{k-1}), \tag{80}$$

we see that

$$\tfrac{1}{|U|} \Sigma X^U = \tfrac{1}{k} \sum_{\lambda \in \mathbb{Z}_k} X^{\lambda u} = \tfrac{1}{k} S(X^u) , \tag{81}$$

so that

$$\tfrac{1}{|U|} \Sigma X^U|_{X=\xi^f} = \tfrac{1}{k} S((\xi^f)^u) = \tfrac{1}{k} S(\xi^{(f\cdot u)}) \tag{82}$$

as

$$(\xi^f)^u = (\xi^{f_1}, \ldots, \xi^{f_n})^{(u_1, \ldots, u_n)} = \xi^{f_1 u_1} \cdots \xi^{f_n u_n} = \xi^{f_1 u_1 + \cdots + f_n u_n} = \xi^{(f\cdot u)}. \tag{83}$$

It follows that

$$\begin{array}{lcl} \Sigma X^U|_{X=\xi^f} \neq 0 \iff S(\xi^{(f\cdot u)}) \neq 0 & \searrow & \\ & & \xi^{(f\cdot u)} = 1 \iff (f \cdot u) = 0 \iff f \perp U. \\ \Sigma X^U|_{X=\xi^f} = |U| \iff S(\xi^{(f\cdot u)}) = k & \nearrow & \end{array} \tag{84}$$

Therefore, statements (i), (ii) and (iv) are equivalent for any subspace $U \leq \mathbb{Z}_k^n$. Now, obviously, statement (iii) implies statement (ii) and its equivalent (iv), which, conversely, entails statement (iii) since

$$|U| \notin r\mathbb{Z}[\xi], \tag{85}$$

as

$$|U| \notin r\mathbb{Z} = r(\mathcal{O}_{\mathbb{C}} \cap \mathbb{Q}) \supseteq r(\mathbb{Z}[\xi] \cap \mathbb{Q}) = r\mathbb{Z}[\xi] \cap \mathbb{Q}, \tag{86}$$

where $\mathcal{O}_{\mathbb{C}}$ is the set of algebraic integers, see e.g. [DuFo]. ☐

The connection to orthogonality is the crucial point. It is important with respect to the following definition, which plays a fundamental role in the second part of this article:

Definition 7.2. A *(nowhere-zero) flow* $f = (f_1, \ldots, f_n) \in \mathbb{Z}_k^n$ of a subspace $U \leq \mathbb{Z}_k^n$ is a nowhere-zero vector (i.e. $f_j \neq 0$ for $j = 1, 2, \ldots, n$) orthogonal to U, $f \perp U$.

We can now prove our core theorem:

Theorem 7.3. *For subspaces $U \leq \mathbb{Z}_k^n$, and $r \in \mathbb{N}$ not dividing $|U|$, the following statements are equivalent:*

(i) *U does not have a flow.*

(ii) *U can be switched off.*

(iii) *U can be switched off modulo r.*

Proof. We start with the proof of $(i) \Rightarrow (ii)$. If U has no flow, then

$$\Psi_{\mathrm{k}}(U)|_{\mathfrak{X}(k)^n} \;=\; \Sigma X^U|_{\mathfrak{X}(k)^n} \;\equiv\!= \; 0, \tag{87}$$

by Theorem 7.1, and, with Theorem 5.1, this means that U can be switched off.

The implication $(ii) \Rightarrow (iii)$ is trivial. We are left with the proof of $(iii) \Rightarrow (i)$. However, if U is switchable modulo r, then

$$\Sigma X^U|_{\mathfrak{X}(k)^n} \;\equiv\; 0 \pmod{r\mathbb{Z}[e^{2\pi\sqrt{-1}/k}]}, \tag{88}$$

by Corollary 5.3, and, with Theorem 7.1, this implies that U has no flow. □

We are currently working on a purely combinatorial proof of this fact over finite fields, which will nicely fit together with our planned description of Projective Berlekamp. But, first, let us collect everything that we need in the second part of this article in the following theorem. With $U\setminus\!\!\setminus v := \{\, u \in U \mid u \equiv\!\neq v \,\}$ and the pattern $J_{a,v} \colon I = \mathbb{Z}_k^n \longrightarrow \{-1, 0, 1\}$ $U\setminus\!\!\setminus v$
from Equation (20) the following holds: $J_{a,v}$

Theorem 7.4. *Let $a \in \mathbb{Z}_k^n$ and $b \in (\mathbb{Z}_k \setminus 0)^n$, e.g. $a \equiv\!= 0$ and $b \equiv\!= 1$. Let $U \leq \mathbb{Z}_k^n$ be a subspace, and assume that $r \geq 2$ does not divide $|U|$, and that $r' \geq 2$ divides $k-1$. Then the following statements are equivalent:*

(i) *U does not have a flow.*

(ii) $\sum_{x \in U} J_{a,v}(x) \;=\; 0$ *for all* $v \in \mathbb{Z}_k^n \setminus\!\!\setminus a$.

(iii) $\sum_{x \in U} J_{a,v}(x) \;\equiv\; 0 \pmod{r}$ *for all* $v \in \mathbb{Z}_k^n \setminus\!\!\setminus a$.

(iv) $\sum_{x \in U} J_{0,b}(x - v) \;=\; 0$ *for all* $v \in \mathbb{Z}_k^n \setminus\!\!\setminus 0$.

(v) $\sum_{x \in U} J_{0,b}(x - v) \;\equiv\; 0 \pmod{r}$ *for all* $v \in \mathbb{Z}_k^n \setminus\!\!\setminus 0$.

(vi) $\bigl|U\setminus\!\!\setminus v\bigr| \;\equiv\; 0 \pmod{r'}$ *for all* $v \in \mathbb{Z}_k^n$.

Proof. This follows from Theorem 7.3 together with Theorem 3.3 and Corollary 4.4. Only point (iv) and (v) may look a bit unexpected. However, if we use $\varphi(x) := x + b$ and $a \equiv 0$ in Theorem 3.3, we will arrive at the term

$$\sum_{x \in I} J_{v,\varphi(v)}(x)\, U(x) \;=\; \sum_{x \in U} J_{v,v+b}(x) \;=\; \sum_{x \in U} J_{0,b}(x - v), \tag{89}$$

which is exactly the expression in these two parts of our theorem. □

8 Wedderburn Decomposition

In this short section we discus the Wedderburn Decomposition of our game. This is not required for the other sections, but it seems to be an interesting question. Since we have no further applications, we restrict ourselves to an example, and do not present detailed proofs. Why Wedderburn Decomposition? Well, the isomorphism Ψ

$$\Psi\colon \mathbb{Z}^I \;\xrightarrow{\sim}\; \mathbb{Z}X^I, \qquad U \longmapsto \sum_{v \in I} U(v)\, X^v, \tag{90}$$

from the last section pulls back a multiplicative structure on our set of patterns. With this multiplication $\mathbb{Z}^I$ is a group algebra. If we view only the classical modulo 2 case, with the two states *ON* and *OFF*, this becomes the group algebra $\mathbb{Z}_2^I \cong \mathbb{F}_2 X^I$ over the field $\mathbb{F}_2 = \mathbb{Z}_2$. If we further choose $I := \mathbb{Z}_3^n$, which is an important case with respect to the Four Color Problem and the Three Flow Conjecture, as we will see, the group algebra

$$\mathbb{Z}_2^{\mathbb{Z}_3^n} \;\cong\; \mathbb{F}_2 X^{\mathbb{Z}_3^n} \tag{91}$$

fulfills the Maschke Condition. Therefore, it is isomorphic to a direct product of extension fields of $\mathbb{F}_2$. It turns out that

$$\mathbb{Z}_2^{\mathbb{Z}_3^n} \;\cong\; \mathbb{F}_2 \times \mathbb{F}_4 \times \mathbb{F}_4 \times \cdots \times \mathbb{F}_4, \tag{92}$$

with the single factor $\mathbb{F}_2$ corresponds to the trivial representation. Where can these fields be found inside $\mathbb{Z}_2^{\mathbb{Z}_3^n}$? Well, they are given by the following types of sets of patterns:

$$\{\emptyset, \mathbb{Z}_3^n\} \;\cong\; \mathbb{F}_2 \quad \text{and} \quad \{\emptyset, \overline{H}, v{+}\overline{H}, -v{+}\overline{H}\} \;\cong\; \mathbb{F}_4, \tag{93}$$

where $\overline{H} := \mathbb{Z}_3^n \setminus H$ is the complement of a hyperplanes H, and $\pm v{+}\overline{H}$ is $\overline{H}$ shifted by an arbitrary $v \in \overline{H}$. The complements $\overline{H}$ are, together with the all-1 pattern $\mathbb{Z}_3^n$, the primitive idempotents of $\mathbb{Z}_2^{\mathbb{Z}_3^n}$. For details, we refer the reader to [Wa, Sections 9.1-9.4], and the detailed example $\mathbb{Z}_2^{\mathbb{Z}_5^2}$ on page 837 of this book. Using Theorem 7.3, one can further show that the subspace (ideal) of switchable patterns is the product of the first factor $\{\emptyset, I\} \cong \mathbb{F}_2$ and those $\mathbb{F}_4$-factors corresponding to hyperplanes $H = h^\perp$ with a 0-entry in $h \in \mathbb{Z}_3^n$.

Part II

Nowhere Zero Conditions in Graph Theory and Combinatorics

We initially work in the general framework of finite commutative rings R with $1 \neq 0$, $k := |R|$, but soon come back to $\mathbb{Z}_k := \mathbb{Z}/k\mathbb{Z}$. Our objective is to apply Theorem 7.4 about switchable subspaces $U \leq \mathbb{Z}_k^n$ to graphs and matrices. Therefore, we have to consider subspaces U related to these combinatorial structures. In all cases U will be defined with the help of (incidence) matrices. We use the following convention for vector-matrix and matrix-vector multiplication, based on matrix-matrix multiplication:

R, k $\mathbb{Z}_k$ uA

Av

$$uA := [u]^t A \quad \text{and} \quad Av := A[v] \quad \text{for} \quad A \in R^{m\times n},\ u \in R^m,\ v \in R^n, \tag{94}$$

where $[u] \in R^{m\times 1}$ is the usual interpretation of $u \in R^m$ as a column-matrix, and $[u]^t$ is its transposed in $R^{1\times m}$ (transposition is not defined in R^m).

$[u]^t$

9 Nowhere Zero Flows

We repeat and extend the definition of a flow of a subspace from the first part of this article. A *subspace* or a *linear code* or a *chain-group* on a set N over the ring R is a submodule U of the free R-module R^N. Mostly, we use $N := \{1, 2, \ldots, n\}$ and work in R^n. It is also worth mentioning that linear codes are basically the same as *linear matroids*, see e.g. [Ca]. We prefer here the term *subspace* even though the term *code* would emphasize the relative position of the subspace U to the coordinate axes $\langle e_j \rangle$. Actually, this should be emphasized, as our definition of subspace flows will depend on coordinates. Again, we write "$f \equiv\!\!\!\!\!\!\neq 0$" if $f = (f_1, f_2, \ldots, f_n) \in R^n$ has full weight, and "$v \perp w$" if $\sum_j v_j w_j = 0$. With this the following definition generalizes nowhere-zero flow of graphs:

$\langle e_j \rangle$ $f \equiv\!\!\!\!\!\!\neq 0$ $\perp$

Definition 9.1 (Flows)**.**

(i) A *(nowhere-zero) flow* $f \in R^n$ of a subset $U \subseteq R^n$ is a tuple $f \equiv\!\!\!\!\!\!\neq 0$ orthogonal to U, $f \perp U$. Such an f is then automatically a flow of the whole span $\langle U \rangle$.

(ii) A *(nowhere-zero right) flow* of a matrix $A \in R^{m\times n}$ (an A*-flow*) is a flow $f \in R^n$ of the row space $\mathrm{RS}(A)$ of A, i.e., $f \equiv\!\!\!\!\!\!\neq 0$ and $Af \equiv\!\!\!\!\!= 0$.

RS

(iii) A *(nowhere-zero) left flow* of a matrix $A \in R^{m\times n}$ is a flow $f \in R^m$ of the column space $\mathrm{CS}(A)$ of A, i.e., $f \equiv\!\!\!\!\!\!\neq 0$ and $fA \equiv\!\!\!\!\!= 0$.

CS

A *nowhere-zero R-flow* of a directed graph $\vec{G} = (\mathcal{V}, \mathcal{E}, \to)$ is nothing else but a left flow $f \in R^{\mathcal{E}}$ of its arc-vertex incidence matrix $\mathrm{AV}_R(\vec{G}) \in \{-1, 0, 1\}^{\mathcal{E}\times\mathcal{V}}$ over R. It is

$\vec{G}$ $\mathrm{AV}_R(\vec{G})$

known that the existence of such a flow depends neither on the orientation of the graph nor on the structure of R, only on $k := |R|$. Therefore, we may say that the underlying graph $G = (\mathcal{V}, \mathcal{E})$ *has a nowhere zero k-flow* if such a flow exists. G

One also says that a flow $f \in R^{\mathcal{E}}$ of a directed graph $\vec{G} = (\mathcal{V}, \mathcal{E}, \rightarrow)$ is a flow *through* the edges ε of $\vec{G}$. In accordance with this, we could say that a flow $f \in R^n$ of a subspace $U \leq R^n$ is a flow through the *standard basis* vectors $e_1, e_2, \ldots, e_n$ of R^n. The *nowhere-zero condition* $f \equiv\!\neq 0$ just means e_j

$$f \not\angle e_j \quad \text{for } j = 1, 2, \ldots, n\,; \tag{95}$$

and

$$f \perp U \tag{96}$$

is the *flow condition.*

The column space $\mathrm{CS}(\mathrm{AV}_R(\vec{G})) \leq R^{\mathcal{E}}$ of the arc-vertex incidence matrix $\mathrm{AV}_R(\vec{G})$ of $\vec{G}$ is also called the *R-bond space* or *coboundary module* of $\vec{G}$. We abbreviate $\mathcal{B}_k$

$$\mathcal{B}_R(\vec{G}) := \mathrm{CS}(\mathrm{AV}_R(\vec{G})) \quad \text{and} \quad \mathcal{B}_k(\vec{G}) = \mathcal{B}_{\mathbb{Z}_k}(\vec{G}). \tag{97}$$

The R-bond space is the subspace of all potential differences in the *edge space* $R^{\mathcal{E}}$ of $\vec{G}$, i.e., its elements $u = (u_\varepsilon)_{\varepsilon \in \mathcal{E}}$ are of the form

$$u \;=\; \big(\lambda(\varepsilon^{\rightarrow}) - \lambda(\varepsilon^{\leftarrow})\big)_{\varepsilon \in \mathcal{E}} \quad \text{with} \quad \lambda \in R^{\mathcal{V}} \tag{98}$$

(where $\varepsilon^{\rightarrow}$ and $\varepsilon^{\leftarrow}$ are the target and the source of the edge ε, respectively). These *coboundaries* $u \in \mathcal{B}_R(\vec{G})$ are also called *tensions*, *R-coflows* or *dual R-flows*, as the signed sum of arc values on each circuit of $\vec{G}$ is zero. A nowhere-zero coflow u exists if and only if a proper vertex coloring λ exists. Summarizing, we see that the concept of flows of subspaces generalizes the graph-theoretic one: $\varepsilon^{\rightarrow}, \varepsilon^{\leftarrow}$

Proposition 9.2. *Assume $|R| = k$. A graph $G = (\mathcal{V}, \mathcal{E})$ has a nowhere-zero k-flow if and only if the R-bond space $\mathcal{B}_R(\vec{G}) \leq R^{\mathcal{E}}$ of an oriented version $\vec{G}$ of G has a flow.*

With this proposition we have a connection to nowhere-zero flows of graphs, and obtain the following new equivalents; where again $U \setminus\!\!\setminus a := \{\, u \in U \mid u \equiv\!\neq a \,\}$, and $J_{a,g}(x)$ is nonzero and equal to $(-1)^{|\{j \,\mid\, x_j = a_j\}|}$ only if $x_j \in \{a_j, g_j\}$ for all j, as in Equation (20): $U \setminus\!\!\setminus a$ $J_{a,g}(x)$

Theorem 9.3. *Let $\vec{G} = (\mathcal{V}, \mathcal{E}, \rightarrow)$ be a connected directed graph, $a \in \mathbb{Z}_k^{\mathcal{E}}$ and $b \in (\mathbb{Z}_k \setminus 0)^{\mathcal{E}}$, e.g. $a \equiv\!= 0$ and $b \equiv\!= 1$. Assume that $r \geq 2$ does not divide $k^{|\mathcal{V}|-1}$, and that $r' \geq 2$ divides $k - 1$. Then the following six statements are equivalent:*

(i) *$\vec{G}$ has a nowhere-zero k-flow.*

(ii) *There is a $g \in \mathbb{Z}_k^{\mathcal{E}} \setminus\!\!\setminus a$ with $\sum_{x \in \mathcal{B}_k(\vec{G})} J_{a,g}(x) \neq 0$.*

(iii) *There is a* $g \in \mathbb{Z}_k^{\mathcal{E}} \setminus\!\setminus a$ *with* $\sum_{x \in \mathcal{B}_k(\vec{G})} J_{a,g}(x) \not\equiv 0 \pmod{r}$.

(iv) *There is a* $g \in \mathbb{Z}_k^{\mathcal{E}} \setminus\!\setminus 0$ *with* $\sum_{x \in \mathcal{B}_k(\vec{G})} J_{0,b}(x-g) \neq 0$.

(v) *There is a* $g \in \mathbb{Z}_k^{\mathcal{E}} \setminus\!\setminus 0$ *with* $\sum_{x \in \mathcal{B}_k(\vec{G})} J_{0,b}(x-g) \not\equiv 0 \pmod{r}$.

(vi) *There is a* $g \in \mathbb{Z}_k^{\mathcal{E}}$ *with* $\left|\mathcal{B}_k(\vec{G}) \setminus\!\setminus g\right| \not\equiv 0 \pmod{r'}$.

Proof. By [Tu, Theorem VIII.46], $U := \mathcal{B}_k(\vec{G})$ has $k^{|\mathcal{V}|-1}$ many elements so that Theorem 7.4 applies. □

This theorem generalizes a result by Onn [Onn, Theorem 1.2], which is the special case $a \equiv\!\!= -1$ of the first equivalence, $(i) \Leftrightarrow (ii)$. Onn also applied his result in [Onn, Corollary 1.4] to bridgeless triangulated (chordal) graphs, where he showed that such graphs have a 4-flow. The inductive proof uses the fact that, on a cyclically directed triangle, the trivial edge labelling $x \equiv\!\!= 0$ is the only $\mathbb{Z}_4$-coflow contributing a nonvanishing summand $J_{a,g}(x)$, if $a \equiv\!\!= -1$ and $g \equiv\!\!= 0$.

By Tutte's 5-Flow Conjecture, bridges in $\vec{G}$ should be the only obstruction against the existence of k-flows with $k \geq 5$. Since bridges ε correspond to coordinate axes $\langle e_\varepsilon \rangle$ contained in $\mathcal{B}_k(\vec{G})$, one could conjecture that every subspace $U \subseteq \mathbb{Z}_k^n$ not containing a coordinate axes possesses a flow. However, this is wrong. There is a 4-dimensional subspace of the 6-dimensional space $\mathbb{Z}_5^6$ which is a counterexample. More generally, if k is prime, the row space $\mathrm{RS}(A)$ of the matrix

$$A := \left[\begin{array}{cccc|cc} 1 & & \cdots & 0 & 1 & 1 \\ & 1 & & \vdots & 1 & 2 \\ \vdots & & \ddots & & \vdots & \vdots \\ 0 & \cdots & & 1 & 1 & k-1 \end{array}\right], \tag{99}$$

as matrix over $\mathbb{Z}_k$, is a simple counterexample (as can be seen by using the nowhere-zero point equivalent in Lemma 10.2). The point is that if we could prove that such counterexamples do not arise from directed graphs, we would have found a proof of Tutte's 5-Flow Conjecture.

Moreover, the generalized definition of a flow does not just capture flows of graphs. A classical theorem by Heawood [Ai, Theorem 7.61] reveals a connection to edge 3-colorings. Let $G = (\mathcal{V}, \mathcal{E})$ be a connected 3-regular planar graph. Then G can be edge colored with 3 colors if and only if there is a vertex labelling with the numbers $+1$ and -1 , such that for each face F of G , the sums over all labels of vertices which lie on the border of F is zero modulo 3 . In our notation, this ± 1-labelling is a right flow of the face-vertex incidence matrix of G over $\mathbb{Z}_3$ and, again, a flow of a subspace:

Proposition 9.4. *Let $G = (\mathcal{V}, \mathcal{E})$ be a connected 3-regular planar graph. Then G can be edge colored with 3 colors if and only if the row space $\mathrm{RS}(\mathrm{FV}(G))$ of the face-vertex incidence matrix $\mathrm{FV}(G) \in \{0,1\}^{\mathcal{F}\times\mathcal{V}}$ of G, as matrix over $\mathbb{Z}_3$, has a flow.*

By Appel and Haken's Four Color Theorem [ApHa], in Tait's edge coloring formulation [Ai, Theorem 7.61], such a *Tait Coloring* exists if and only if the graph has no bridge. We present the following new equivalents which also may be of interest if one wants to find a short proof of the Four Color Theorem:

Theorem 9.5. *Let $G = (\mathcal{V}, \mathcal{E}, \mathcal{F})$ be a connected 3-regular planar graph with $\mathcal{F}$ as set of faces, $\mathrm{RS}(\mathrm{FV}(G))$ the row space of its face-vertex incidence matrix $\mathrm{FV}(G) \in \{0,1\}^{\mathcal{F}\times\mathcal{V}}$, as matrix over $\mathbb{Z}_3$, $a \in \mathbb{Z}_3^{\mathcal{V}}$ and $b \in (\mathbb{Z}_3\backslash 0)^{\mathcal{V}}$, e.g. $a \equiv 0$ and $b \equiv 1$. Then for $r \in \mathbb{N}$ not dividing $3^{|\mathcal{F}|-1}$, the following statements are equivalent:*

(i) G *can be* edge colored *with* 3 *colors.*

(ii) *There is a* $g \in \mathbb{Z}_3^{\mathcal{V}} \setminus a$ *with* $\displaystyle\sum_{x\in\mathrm{RS}(\mathrm{FV}(G))} J_{a,g}(x) \neq 0\,.$

(iii) *There is a* $g \in \mathbb{Z}_3^{\mathcal{V}} \setminus a$ *with* $\displaystyle\sum_{x\in\mathrm{RS}(\mathrm{FV}(G))} J_{a,g}(x) \not\equiv 0 \pmod r\,.$

(iv) *There is a* $g \in \mathbb{Z}_3^{\mathcal{V}} \setminus 0$ *with* $\displaystyle\sum_{x\in\mathrm{RS}(\mathrm{FV}(G))} J_{0,b}(x-g) \neq 0\,.$

(v) *There is a* $g \in \mathbb{Z}_3^{\mathcal{V}} \setminus 0$ *with* $\displaystyle\sum_{x\in\mathrm{RS}(\mathrm{FV}(G))} J_{0,b}(x-g) \not\equiv 0 \pmod r\,.$

(vi) *There is a* $g \in \mathbb{Z}_3^{\mathcal{V}}$ *with* $\big|\mathrm{RS}(\mathrm{FV}(G)) \setminus g\big| \not\equiv 0 \pmod 2\,.$

Proof. The subspace $U := \mathrm{RS}(\mathrm{FV}(G))$ has dimension $|\mathcal{F}|-1$ and $3^{|\mathcal{F}|-1}$ many elements. Therefore, Theorem 7.4 can be applied. □

Heawood's Theorem is based on the fact that the face cycles of a planar graph G span the whole $\mathbb{Z}_2$-cycle space $\mathcal{C}_2(G) \subseteq \mathbb{Z}_2^{\mathcal{E}}$ of the graph. However, this property is not lost if we remove one face cycle, so that our results also hold if we delete one row in the examined matrix. It is also known that even two rows may be deleted if they correspond to two adjacent faces of G. Even three rows, corresponding to the three faces around a common border vertex, can be removed. This can be proven using a double counting argument, or as in [Tu, Theorem IX.53].

Furthermore, all this can be generalized to non-planar 3-regular graphs. We just need a set of cycles that span the cycle space of G, and any distinguished cyclic order on the three edges around each vertex. With respect to these orders, the generating cycles usually will not turn to the same side all the time, they will dipsy-doodle through the vertices. Therefore, the corresponding incidence matrix usually will contain the entry -1 as well.

10 Nowhere Zero Colorings of Matrices

In this section we study nowhere-zero colorings of matrices. These results are then also used in the succeeding section about graph colorings. We need the following definition:

Definition 10.1 (Nowhere Zero Colorings)**.**

(i) A *(nowhere-zero) coflow* $f \in R^n$ of a subset $U \subseteq R^n$ is a tuple $f \equiv\neq 0$ in $\langle U \rangle$. Such an f is then automatically a coflow of the whole subspace $\langle U \rangle$.

(ii) A *(nowhere-zero right) coflow* of a matrix $A \in R^{m \times n}$ (an A-*coflow*) is a coflow $f \in R^n$ of the column space $\mathrm{CS}(A)$ of A, i.e., $f \equiv\neq 0$ and $f = Ag$ for a $g \in R^n$. CS

(iii) A *(proper right) coloring* of a matrix $A \in R^{m \times n}$ (an A-*coloring*) is a tuple $g \in R^n$ with $Ag \equiv\neq 0$, i.e., Ag is a coflow of A.

(iv) A *nowhere-zero (proper right) coloring* or *nowhere zero point* of $A \in R^{m \times n}$ is a tuple $g \in R^n$ with $g \equiv\neq 0$ and $Ag \equiv\neq 0$.

The following lemma builds the bridge from nowhere-zero points to flows and contains another connection to colorings:

Lemma 10.2. *Let $A \in R^{m \times n}$ and $f \in R^n$, then the following statements are equivalent:*

(i) g is a nowhere-zero point of A.

(ii) $\binom{Ag}{-g}$ is a flow of (I_m, A).

(iii) g is a coloring of $\binom{A}{\mathrm{I}_n}$, or equivalently of $\binom{-A}{\mathrm{I}_n}$.

In particular, since any right flow of (I_m, A) necessarily has the form $\binom{Ag}{-g}$, the following existence statements are equivalent:

(i′) A has a nowhere-zero point.

(ii′) (I_m, A) has a flow.

(iii′) $\binom{A}{\mathrm{I}_n}$, or equivalently $\binom{-A}{\mathrm{I}_n}$, has a coloring.

Proof. It is easy to see that $(i) \Leftrightarrow (ii)$ and $(i) \Leftrightarrow (iii)$. □

In terms of subspaces this connection between nowhere-zero points and flows can be stated as follows:

Proposition 10.3. *A matrix $A \in R^{m \times n}$ has a nowhere-zero point if and only if the row space $\mathrm{RS}(\mathrm{I}_m, A) \leq R^{m+n}$ of (I_m, A) has a flow.*

With this we obtain new equivalents to the existence of nowhere-zero points:

Theorem 10.4. *Let* $A \in \mathbb{Z}_k^{m\times n}$*,* $a \in \mathbb{Z}_k^{m+n}$ *and* $b \in (\mathbb{Z}_k\backslash 0)^{m+n}$*, e.g.* $a \equiv 0$ *and* $b \equiv 1$*. Assume that* $r \geq 2$ *does not divide* k^m*, and that* $r' \geq 2$ *divides* $k-1$*. Then the following statements are equivalent:*

(i) A *has a nowhere-zero point.*

(ii) There is a $v \in \mathbb{Z}_k^{m+n}\backslash\!\backslash a$ *such that* $\sum_{x\in\mathbb{Z}_k^m} J_{a,v}(x, xA) \neq 0$*.*

(iii) There is a $v \in \mathbb{Z}_k^{m+n}\backslash\!\backslash a$ *such that* $\sum_{x\in\mathbb{Z}_k^m} J_{a,v}(x, xA) \not\equiv 0 \pmod r$*.*

(iv) There is a $w \in \mathbb{Z}_k^n$ *such that* $\sum_{x\in\mathbb{Z}_k^m} J_{0,b}(x, xA - w) \neq 0$*.*

(v) There is a $w \in \mathbb{Z}_k^n$ *such that* $\sum_{x\in\mathbb{Z}_k^m} J_{0,b}(x, xA - w) \not\equiv 0 \pmod r$*.*

(vi) There is a $w \in \mathbb{Z}_k^n$ *such that* $\left|\mathrm{RS}(\mathrm{I}_m, A)\backslash\!\backslash w\right| \not\equiv 0 \pmod{r'}$*.*

Proof. With Theorem 7.4 in mind we set $U := \mathrm{RS}(\mathrm{I}_m, A) \subseteq \mathbb{Z}_k^{m+n}$. Our matrix A has a nowhere zero point if and only if there is a flow of U. Therefore, Theorem 7.4 yields the equivalence $(i) \Leftrightarrow (vi)$, and, together with the observation

$$\sum_{x\in\mathbb{Z}_k^m} J_{a,v}(x, xA) \;=\; \sum_{u\in U} J_{a,v}(u), \tag{100}$$

it proves the equivalences $(i) \Leftrightarrow (iii)$ and $(i) \Leftrightarrow (ii)$. In order to prove $(i) \Leftrightarrow (iv)$ and $(i) \Leftrightarrow (v)$, we split each $v \in \mathbb{Z}_k^{m+n}$ into $v_1 \in \mathbb{Z}_k^m$ and $v_2 \in \mathbb{Z}_k^n$, $v = (v_1, v_2)$. If

$$w \;=\; v_2 - v_1 A, \tag{101}$$

then

$$\sum_{x\in\mathbb{Z}_k^m} J_{0,b}(x, xA - w) \;=\; \sum_{y\in\mathbb{Z}_k^m} J_{0,b}(y - v_1, yA - v_2) \;=\; \sum_{u\in U} J_{0,b}(u - v) \;=\; \sum_{u\in U} J_{v,v+b}(u), \tag{102}$$

by substituting $y = x + v_1$ and $u = (y, yA)$, so that, again, Theorem 7.4 does the job. □

Corollary 10.5. *Let* p *be an odd prime. Then a matrix* $A \in \mathbb{Z}_p^{m\times n}$ *has a nowhere-zero point if and only if the rows and columns of* A *can be multiplied with nonvanishing scalars in such a way that the resulting matrix* $\tilde{A}$ *has the following property:*

There are altogether an odd number of zero-one combinations of the rows of $\tilde{A}$ *resulting in a zero-one vector. In other words, oddly many* $x \in \{0,1\}^m$ *with* $x\tilde{A} \in \{0,1\}^n$*.*

Proof. We set $r := 2$ and $a := 0 \in \mathbb{Z}_p^{m+n}$. If A has a nowhere-zero flow then there is a $v = (v_1, \ldots, v_{m+n}) \equiv\!\!\not\; 0$ as in part (iii) of the last theorem. Now the matrix

$$\tilde{A} \;:=\; \mathrm{Diag}(v_1, \ldots, v_m)\, A\, \mathrm{Diag}(v_{m+1}^{-1}, \ldots, v_{m+n}^{-1}) \tag{103}$$

has the property that

$$\sum_{x\in\mathbb{Z}_p^m} J_{0,1}(x, x\tilde{A}) \;=\; \sum_{y\in\mathbb{Z}_p^m} J_{0,v}(y, yA) \not\equiv 0 \pmod 2, \tag{104}$$

as

$$(x, x\tilde{A})\,\mathrm{Diag}(v_1,\ldots,v_{m+n}) \;=\; (y, yA) \quad \text{if} \quad y \;=\; (v_1x_1,\ldots,v_mx_m). \tag{105}$$

This singles out odd many $x \in \{0,1\}^m$ with $x\tilde{A} \in \{0,1\}^n$, and proves one direction of the equivalence. The other direction is proven similarly. □

This corollary may be of interest with respect to Jaeger's Conjecture:

> "Non-singular square matrices A over finite fields $\mathbb{F}_q$ with $q > 3$ elements have a nowhere-zero point."

Only the prime field case, $\mathbb{F}_q = \mathbb{Z}_p$, is still open. A very nice proof, in the case of proper prime powers, $q = p^k$ ($k > 1$), was given by Alon and Tarsi in [AlTa2].

11 Colorings of Graphs

In this section we present our new equivalents for the colorability of graphs. A *coloring* of a directed graph $\vec{G} = (\mathcal{V}, \mathcal{E}, \rightarrow)$ with colors taken from R, respectively from $R\backslash 0$, is nothing else but a coloring, respectively a nowhere-zero coloring, $g \in R^{\mathcal{V}}$ of the arc-vertex incidence matrix $\mathrm{AV}_R(\vec{G}) \in \{-1,0,1\}^{\mathcal{E}\times\mathcal{V}}$ of $\vec{G}$ over R. Obviously the existence of such colorings neither depend on the orientation of the graph nor on the structure of R, only on $k := |R|$. Therefore, we may say that the underlying graph $G = (\mathcal{V}, \mathcal{E})$ *has a k-coloring*, respectively *a $(k-1)$-coloring*, if such a coloring exists.

$\vec{G}$ AV_R G

Before we explain connections to flows, we want to mention some of the different terminologies used in literature, mainly in the case of finite fields, $R := \mathbb{F}_q$. With respect to graph theory, a coflow also could be called a nowhere-zero *coboundary*. If a matrix A has a coloring g then this vector g is not orthogonal to any row of A, so that no row of A is contained in $g^{\perp}$. Conversely, if the rows of A form no 1-*blocking set*, i.e., if there is a hyperplane $g^{\perp}$ avoiding the rows of A, then A has a coloring g (see e.g. [We]). Equivalently, one can say that the set of rows of A has *critical exponent* at most 1. Some authors would say that the linear matroid of these rows is 1-*colorable* over $\mathbb{F}_q$. Furthermore, one could generalize the concept of colorings and flows by allowing tuples $f_1,\ldots,f_t \in R^n$ with the property that to any index $j \le n$ at least one of the f_i does not vanish at the j^{th} coordinate, as e.g. in [Ai, Theorem 7.55]. Flows also can be defined for orientable matroids, see e.g. [HoNi].

From our definition we see that a k-coloring of a graph exists if and only if the bond space $\mathcal{B}_R(\vec{G}) := \mathrm{CS}(\mathrm{AV}_R(\vec{G}))$ of $\vec{G}$ has a coflow. Equivalently, its orthogonal space $\mathcal{C}_R(\vec{G}) := \mathrm{CS}(\mathrm{AV}_R(\vec{G}))^{\perp}$, the *$R$-cycle space* (or *cycle module*) of $\vec{G}$, has a flow. This equivalence is not quite obvious over rings, as for subspaces $U \le R^n$ it does not always hold that $(U^{\perp})^{\perp} = U$. However, by [Tu, Theorem VIII.42], it does hold for $U := \mathcal{B}_R(\vec{G})$. We have:

$\mathcal{C}_R$

Proposition 11.1. *Assume* $|R| = k$ *. A graph* $G = (\mathcal{V}, \mathcal{E})$ *has a vertex k-coloring if and only if the cycle space* $\mathcal{C}_R(\vec{G}) \leq R^{\mathcal{E}}$ *of an oriented version* $\vec{G}$ *of* G *has a flow.*

From this we derive the following result, where $\mathcal{C}_k(\vec{G}) = \mathcal{C}_{\mathbb{Z}_k}(\vec{G})$: $\mathcal{C}_k$

Theorem 11.2. *Let* $\vec{G} = (\mathcal{V}, \mathcal{E}, \rightarrow)$ *be a connected directed graph,* $a \in \mathbb{Z}_k^{\mathcal{E}}$ *and* $b \in (\mathbb{Z}_k \backslash 0)^{\mathcal{E}}$ *, e.g.* $a \equiv 0$ *and* $b \equiv 1$ *. Assume that* $r \geq 2$ *does not divide* $k^{|\mathcal{E}|-|\mathcal{V}|+1}$*, and that* $r' \geq 2$ *divides* $k-1$ *. Then the following statements are equivalent:*

(i) G *is k-colorable.*

(ii) There is a $g \in \mathbb{Z}_k^{\mathcal{E}} \backslash\backslash a$ *with* $\sum_{x \in \mathcal{C}_k(\vec{G})} J_{a,g}(x) \neq 0$ *.*

(iii) There is a $g \in \mathbb{Z}_k^{\mathcal{E}} \backslash\backslash a$ *with* $\sum_{x \in \mathcal{C}_k(\vec{G})} J_{a,g}(x) \not\equiv 0 \pmod{r}$ *.*

(iv) There is a $c \in \mathbb{Z}_k^{\mathcal{V}}$ *with* $\sum_{x:\, x\,\mathrm{AV}(\vec{G}) = c} J_{0,b}(x) \neq 0$ *.*

(v) There is a $c \in \mathbb{Z}_k^{\mathcal{V}}$ *with* $\sum_{x:\, x\,\mathrm{AV}(\vec{G}) = c} J_{0,b}(x) \not\equiv 0 \pmod{r}$ *.*

(vi) There is a $g \in \mathbb{Z}_k^{\mathcal{E}}$ *with* $\left|\mathcal{C}_k(\vec{G}) \backslash\backslash g\right| \not\equiv 0 \pmod{r'}$ *.*

Proof. By [Tu, Theorem VIII.46], the bond space $\mathcal{B}_k(\vec{G})$ has $k^{|\mathcal{V}|-1}$ many elements so that $\mathcal{C}_k(\vec{G}) \cong \mathbb{Z}^{\mathcal{E}} / \mathcal{B}_k(\vec{G})$ has cardinality $k^{|\mathcal{E}|-|\mathcal{V}|+1}$, and Theorem 7.4 applies. For the two equivalences $(i) \Leftrightarrow (iv)$ and $(i) \Leftrightarrow (v)$ we also need that, if

$$c = -v\,\mathrm{AV}(\vec{G}), \tag{106}$$

then

$$\sum_{x:\, x\,\mathrm{AV}(\vec{G}) = c} J_{0,b}(x) \;=\; \sum_{x:\, (x+v)\,\mathrm{AV}(\vec{G}) = 0} J_{0,b}(x) \;=\; \sum_{y \in \mathcal{C}_k(\vec{G})} J_{0,b}(y - v) \;=\; \sum_{y \in \mathcal{C}_k(\vec{G})} J_{v,v+b}(y). \tag{107}$$

□

The equivalence $(i) \Leftrightarrow (v)$, in the special case $b \equiv 1$, $r = 2$ and k an odd prime, was also obtained by Balázs Szegedy in [Sz, Proposition 30].

The condition in part (ii), with $a \equiv 0$ and $g \equiv 1$, generalizes Alon and Tarsi's widely known sufficient condition [AlTa, Theorem 1.1] for the existence of list colorings. Alon and Tarsi's Theorem is more special in that it assumes that the maximal outdegree $\Delta^+(\vec{G})$ is strictly smaller than k . It is not difficult to see that, under this additional assumption, the nonvanishing summands $J_{0,1}(x)$ in part (ii) correspond to Eulerian subgraphs $x \in \mathcal{C}_k(\vec{G}) \cap \{0,1\}^{\mathcal{E}}$. It follows that

$$\sum_{x \in \mathcal{C}_k(\vec{G})} J_{0,1}(x) \; = \; |EE(\vec{G})| - |EO(\vec{G})|, \tag{108}$$

where $EE(\vec{G})$, resp. $EO(\vec{G})$, is the set of even, resp. odd, Eulerian subgraphs, as in Alon and Tarsi's sufficient condition

$$|EE(\vec{G})| \; \neq \; |EO(\vec{G})|. \tag{109}$$

However, as already said, Alon and Tarsi's Theorem is more general in that it guarantees the existence of list colorings. Even *k-paintability* follows under their additional assumptions $\Delta^{+}(\vec{G}) < k$, as we showed in [Scha2].

The condition in part (ii), again with $a \equiv 0$ and $g \equiv 1$, also contains Yuri Matiyasevich's earlier found sufficient condition in [Ma1]. Matiyasevich's condition for the existence of ordinary k-colorings is similar to Alon and Tarsi's condition, but does not require that the maximal outdegree $\Delta^{+}(\vec{G})$ is strictly smaller than k. Without this requirement Equation (108) still holds, but one has to allow all subgraphs that are "Eulerian modulo k". By flipping around the edges in such a subgraph one obtains a new orientation of $\vec{G}$ that has modulo k the same outdegrees as $\vec{G}$. These kind of orientations are in one-to-one correspondence with the modulo k Eulerian subgraphs. Therefore, the condition in part (ii) (with $a \equiv 0$ and $g \equiv 1$) can be stated as a statement about certain equivalence classes of orientations, exactly as in [Ma1].

Matiyasevich also provided in [Ma1] a necessary condition. This condition follows from the condition in part (v), with $b \equiv 1$. Now, the x with nonvanishing summands $J_{0,1}(x)$ correspond to subgraphs with an outdegree sequence that differs form its indegree sequence by the given sequence c modulo k. So, if we flip around the edges in such a subgraph, we obtain a new orientation of $\vec{G}$ that has certain determined outdegrees modulo k. From this we can derive Matiyasevich's necessary condition in terms of equivalence classes of such orientations.

Analogously, it should be possible to derive the similar result [Go, Theorem 18] by Goodall. Moreover, if we apply part (v), with $b \equiv 1$, to the line graph of a plane triangulation we further can deduce [Ma2, Theorem 7].

We also make the following observation, where $\mathrm{AV}_k(\vec{G}) = \mathrm{AV}_{\mathbb{Z}_k}(\vec{G})$: AV_k

Proposition 11.3. *Assume $|R| = k$, $G = (\mathcal{V}, \mathcal{E})$ is a graph and $\mathrm{AV}_k(\vec{G}) \in \{-1,0,1\}^{\mathcal{E}\times\mathcal{V}}$ is the arc-vertex incidence matrix of a directed version $\vec{G}$ of G. Then G can be vertex colored with $k-1$ colors if and only if $\mathrm{RS}(\mathrm{I}_{\mathcal{E}}, \mathrm{AV}_k(\vec{G})) \leq R^{\mathcal{E}\uplus\mathcal{V}}$ has a flow.*

Proof. This is a special case of Proposition 10.3. □

From this we derive the following graph coloring theorem:

Theorem 11.4. *Let* $a \in \mathbb{Z}_k^{\mathcal{E} \uplus \mathcal{V}}$ *and* $b \in (\mathbb{Z}_k \backslash 0)^{\mathcal{E} \uplus \mathcal{V}}$*, e.g.* $a \equiv 0$ *and* $b \equiv 1$ *. Further, let* $\mathrm{AV}_k(\vec{G}) \in \{-1, 0, 1\}^{\mathcal{E} \times \mathcal{V}} \subseteq \mathbb{Z}_k^{\mathcal{E} \times \mathcal{V}}$ *be the arc-vertex incidence matrix of a directed version* $\vec{G}$ *of a graph* G *. Assume that* $r \geq 2$ *does not divide* $k^{|\mathcal{E}|}$*, and that* $r' \geq 2$ *divides* $k-1$ *. Then the following statements are equivalent:*

(i) G *is* $(k-1)$*-colorable.*

(ii) There is a $g \in \mathbb{Z}_k^{\mathcal{E} \uplus \mathcal{V}} \backslash\!\backslash a$ *with* $\sum_{x \in \mathbb{Z}_k^{\mathcal{E}}} J_{a,g}(x, x\,\mathrm{AV}_k(\vec{G})) \neq 0$ *.*

(iii) There is a $g \in \mathbb{Z}_k^{\mathcal{E} \uplus \mathcal{V}} \backslash\!\backslash a$ *with* $\sum_{x \in \mathbb{Z}_k^{\mathcal{E}}} J_{a,g}(x, x\,\mathrm{AV}_k(\vec{G})) \not\equiv 0 \pmod{r}$ *.*

(iv) There is a $c \in \mathbb{Z}_k^{\mathcal{V}}$ *with* $\sum_{x \in \mathbb{Z}_k^{\mathcal{E}}} J_{0,b}(x, x\,\mathrm{AV}_k(\vec{G}) - c) \neq 0$ *.*

(v) There is a $c \in \mathbb{Z}_k^{\mathcal{V}}$ *with* $\sum_{x \in \mathbb{Z}_k^{\mathcal{E}}} J_{0,b}(x, x\,\mathrm{AV}_k(\vec{G}) - c) \not\equiv 0 \pmod{r}$ *.*

(vi) There is a $g \in \mathbb{Z}_k^{\mathcal{E} \uplus \mathcal{V}}$ *with* $\left|\mathrm{RS}(\mathrm{I}_{\mathcal{E}}, \mathrm{AV}_k(\vec{G})) \backslash\!\backslash g\right| \not\equiv 0 \pmod{r'}$ *.*

Proof. The new corollary is just a reformulation of Theorem 10.4 in the special case $A := \mathrm{AV}_k(\vec{G})$. The nowhere-zero points of this matrix are the colorings of the given graph $\vec{G}$ with $\mathbb{Z}_k \backslash 0$ as color set. □

The same holds for hypergraphs if a kind of incidence matrix with vanishing row sums is used, as in [Scha3, Section 2].

Acknowledgement:
We are grateful to Ayub Khan for his help. Furthermore, the author gratefully acknowledges the support provided by the King Fahd University of Petroleum and Minerals under the project numbers JF090005 and FT090010.

References

[Ai] M. Aigner: Combinatorial Theory. *Springer, Berlin 1979.*

[Al] N. Alon: Restricted Colorings of Graphs. *In:* Surveys in combinatorics, 1993. *London Math. Soc. Lecture Notes Ser. 187, Cambridge Univ. Press, Cambridge 1993, 1–33.*

[AlTa] N. Alon, M. Tarsi: Colorings and Orientations of Graphs. *Combinatorica 12 (1992), 125–134.*

[AlTa2] N. Alon, M. Tarsi: A Nowhere-zero Point in Linear Mappings. *Combinatorica 9 (1989), 393–395.*

[ApHa] K. I. Appel, W. Haken, J. Koch: Every planar map is four colorable. *Illinois J. Math. 21 (1977), 429–567.*

[Ca] P. J. Cameron: Notes on Matroids and Codes. `http://www.maths.qmw.ac.uk/~pjc/comb/matroid.ps`

[CaSt] J. Carlson , D. Stolarski: The Correct Solution to Berlekamp's Switching Game. *Discrete Mathematics 287 (2004), 145–150.*

[DuFo] D. S. Dummit, R. M. Foote: Abstract Algebra. *John Wiley and Sons, 2004.*

[FiSl] P. C. Fishburn, N. J. A. Sloane: The Solution to Berlekamp's Switching Game. *Discrete Math. 74 (1989), 263–290.*

[Go] A. J. Goodall: Some new evaluation of the Tutte polynomial. *J. Combin. Theory Ser. B 96 (2) (2006), 207–224.*

[HoNi] W. Hochstättler and R. Nickel: The flow lattice of oriented matroids. *Contrib. Discrete Math. 2 (2007), 68–86.*

[Ma1] Yu. V. Matiyasevich: A Criterion for Vertex Colorability of a Graph Stated in Terms of Edge Orientations. *(in Russian) Discrete Analysis (Novosibirsk), 26, (1974), 65–71. URL of translation:* *http://logic.pdmi.ras.ru/~yumat/papers/22_paper/22_home.html*

[Ma2] Yu. V. Matiyasevich: A Polynomial Related to Colourings of Triangulation of Sphere. *http://logic.pdmi.ras.ru/~yumat/Journal/Triangular/triang.htm*

[Onn] S. Onn: Nowhere-zero Flow Polynomials. *J. Combin. Theory Ser. A 108 (2004), 205–215.*

[RoVi] R. M. Roth, K. Viswanathan: On the Hardness of Decoding the Gale-Berlekamp Code. *IEEE Trans. Inform. Theory, 54 (2008), 1050–1060.*

[Scha1] U. Schauz: Algebraically Solvable Problems: Describing Polynomials as Equivalent to Explicit Solutions *Electron. J. Combin. 15 (2008), #R10.*

[Scha2] U. Schauz: Flexible Color Lists in Alon and Tarsi's Theorem, and Time Scheduling with Unreliable Participants. *Electron. J. Combin. 17 (2010), #R13.*

[Scha3] U. Schauz: A Paintability Version of the Combinatorial Nullstellensatz, and List Colorings of k-partite k-uniform Hypergraphs. *Submitted.*

[Sz] B. Szegedy: Coverings of Abelian Groups and Vector Spaces. *J. Combinatorial Theory A 114 (2007), 20–34.*

[Tu] W. T. Tutte: Graph Theory. *Cambridge University Press, Camebridge 2001.*

[Ve] O. Veblen: An application of modular equations in analysis situs. *Annals Math. 14 (1912), 86–94.*

[Wa] H.N. Ward: Quadratic residue codes and divisibility. *In:* V. Pless, W.C. Huffman (eds.): Handbook of Coding Theory. *Vol. 1, 827-870. Elsevier, Amsterdam 1998.*

[We] D. J. A. Welsh: Matroids: Fundamental Concepts. *In:* R.L. Graham, M. Grötschel and L. Lovász (eds.): The Handbook of Combinatorics. *Vol. 1, 481-526. MIT Press, Cambridge, MA, 1995.*