Magic in Hyperspace

Ehrhard Behrends

Abstract. We fix an integer $d \geq 1$: the dimension in the space where we are going to present our magic trick is $d+1$. A prime number p is also chosen, the elements of the field $\mathbb{Z}_p$ wil be represented by colours.

Now a "pyramid" in $\mathbb{R}^{d+1}$ is built as follows. The first layer consists of n^d coloured $(d+1)$-dimensional cubes of unit length, where n is an integer. They are arranged as the first layer of a pyramid in $\mathbb{R}^{d+1}$, the $d+1$ lengths of the sides of this layer are $n, n, \ldots, n, 1$. The second layer consists of $(n-1)^d$ coloured cubes. The colours of the new cubes are determined by the colours of the cubes of the first layer in a simple way, and the second layer is placed "on" the first one. (Admittedly, this is not easy to imagine if $d > 2$.) In this way one continues, a pyramid grows in d+1 dimensions, and after $n-1$ steps we arrive at its top that consists of a single cube. The problem is to predict the colour of this final cube in a simple way from the first layer. We will characterize the numbers n where this is possibe. It will turn out that in most cases the "good" n are precisely the integers of the form $p^s + 1$ when the rules of the game are based on the algebraic operations in the field $\mathbb{Z}_p$. This can be used as a prediction trick by magicians in hyperspace.

Our proofs are somehow technical, but elemenary. The key idea is to find the relevant quantities by counting the number of certain walks. Also Ram's result on the properties of binomial coefficients modulo a prime number will play a crucial role. AMS-classification: 00A08, 00A09, 05A10;

keywords: Ram's theorem, mathematical magical tricks, little Fermat theorem, binomial coefficients.

Introduction

In the sequel $(\Delta, +)$, our set of "colours", will be a nontrivial finite abelian group, and $d \geq 1$ will be a fixed integer. We will be concerned with hyperpyramids in $\mathbb{R}^{d+1}$ that are built from coloured $(d+1)$-dimensional unit cubes.

Given an integer m we define $A_{d,m}$ to be the collection of d-dimensional arrays $(x_{i_1,\ldots,i_d})_{i_1,\ldots,i_d=0,\ldots,m-1}$ with $x_{i_1,\ldots,i_d} \in \Delta$. For $d=1$ (resp. $d=2$) the set $A_{d,m}$ is the collection of m-tupels (resp. $m \times m$-matrices) with entries from Δ.

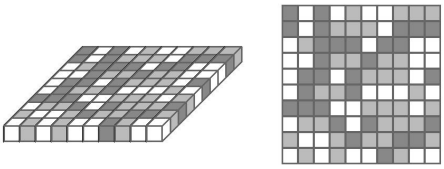
We will think of the elements of $A_{d,m}$ as follows. First we will associate with the $x \in \Delta$ colours such that different x correspond to different colours. And then $(x_{i_1,\ldots,i_d})_{i_1,\ldots,i_d=0,\ldots,m-1} \in A_{d,m}$ is a family of coloured unit cubes in $\mathbb{R}^{d+1}$ that are arranged such that they fill the set $[\,0,n\,] \times \cdots \times [\,0,n\,] \times [\,0,1\,]$ or a translation of it.

Let us illustrate this with $\Delta = \mathbb{Z}_3$. We choose the following colours:

$$0 = \text{white};\ 1 = \text{light gray};\ 2 = \text{dark gray}.$$

A typical element of $A_{1,m}$ is a row of coloured squares. Here is an example with $m = 10$.

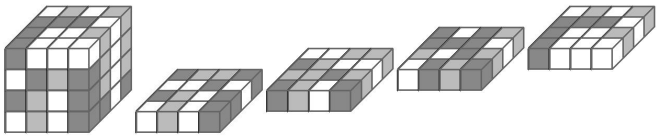
In the case $d = 2$ we are in $\mathbb{R}^3$ and the elements of $A_{2,m}$ can be thought of as square arrangements of unit cubes. Here one sees a 10×10-square for the preceding Δ:



An element of $A_{2,10}$: in $\mathbb{R}^3$ (left) and seen from the top (right)

(The left cube in the back row has colour $x_{0,0} = 2 =$ dark gray .) Seen from the top – in the picture on the right – this array is just a coloured checkerboard.

Needless to say that the case $d = 3$ is more difficult since we are working in four dimensions. If we drop one dimension an m-layer $(x_{i_1,i_2,i_3})_{i_1,i_2,i_3=0,\dots,m-1}$ in $\mathbb{R}^4$ could be represented as a threedimensional cube made of m^3 little cubes as in the following picture on the left. (Here is $m = 4$.)



An element of $A_{3,10}$ in $\mathbb{R}^4$: a 3D projection (left)
and the separated layers of the cube (right).

The 3D projection corresponds to the way how we saved one dimension for layers in $\mathbb{R}^3$ just before.

Fourdmensional beings could see the inside colours, and this will be important in the sequel. However, *we* cannot. But we have the possibility to show all colours by representing the big cube by m layers of height 1. In the preceding picture on the right one looks inside the cube: the first layer is the bottom layer etc.

This could be generalized: each element of $A_{d,m}$ could be visualized for us by m^{d-2} elements of $A_{2,m}$.

The next step is to build new arrays. To this end we fix a family $\alpha = (\alpha_{j_1,\dots,j_d})_{j_1,\dots,j_d=0,1}$ with $\alpha_{j_1,\dots,j_d} \in \mathbb{Z}$, and we define $\Phi_m : A_{d,m} \to A_{d,m-1}$ as follows: $\Phi_m\big((x_{i_1,\dots,i_d})_{i_1,\dots,i_d=0,\dots,m-1}\big)$ is the array $(y_{i_1,\dots,i_d})_{i_1,\dots,i_d=0,\dots,m-2} \in A_{d,m-1}$, where

$$y_{i_1,\dots,i_d} := \sum_{j_1,\dots,j_d=0,1} \alpha_{j_1,\dots,j_d} x_{i_1+j_1,\dots,i_d+j_d}.$$

(Note that every group allows a natural multiplication by elements of $\mathbb{Z}$.)
To state it otherwise, we have a map $\phi_\alpha : A_{d,2} \to \Delta$ that is defined by

$$(z_{j_1,\ldots,j_d})_{j_1,\ldots,j_d=0,1} \mapsto \sum_{j_1,\ldots,j_d=0,1} \alpha_{j_1,\ldots,j_d} z_{j_1,\ldots,j_d},$$

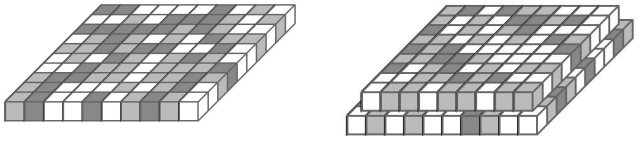
and ϕ_α is applied to every collection of 2^d adjacent hypercubes to produce the new colour.

By Φ_m we obtain a smaller layer of a "hyperpyramid in $\mathbb{R}^{d+1}$". This is just a shorter row of squares in the case $d = 1$ and a smaller quadratic array of unit cubes in the case $d = 2$.

Let us illustrate this in the case of the above examples. In the first one ($d = 1$) we choose $\alpha_0 = \alpha_1 = -1$. Here one sees the original row of squares and – on top of them – the new shorter row.

One can rephrase the rule as follows: put on the top of two adjacent squares with colours x, y one with colour $-x - y$. We note that this definition was the starting point of the present investigations (see [?]). It has the remarkable property that it can be reformulated without using the algebraic structure of $\mathbb{Z}_3$: "If the colours x, y coincide, use the same colour; if not, use the colour that is missing."

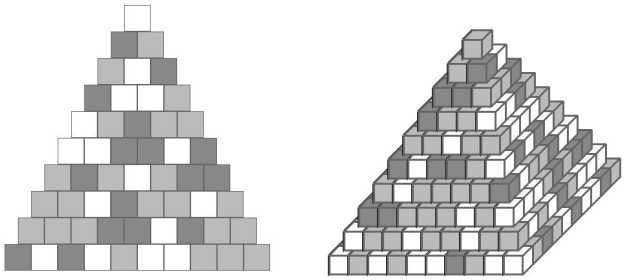
And here is the example with $d = 2$ where we chose $\alpha_{0,0} = \alpha_{1,0} = 1$ and $\alpha_{0,1} = \alpha_{1,1} = -1$. The following picture shows the original and the first two layers.



(Here is an example how the new colours are determined: The right cube in the back row of the new layer is green since

$$1 \cdot x_{0,0} - \cdot x_{0,1} + \cdot x_{1,0} - \cdot x_{1,1} = 1 \cdot 2 - 0 + 1 \cdot 2 - 0 = 1.$$

It is natural to continue this process by using the same rule for the new layers again and again until one finally arrives at a single cube in $\mathbb{R}^{d+1}$. Here are the completed examples, a triangle and a pyramid:



Can we easily predict the colour on the top from the starting configuration? The investigations in [?] started (in one dimensions) with the observation that – for certain widths of the starting layer – the final colour can be obtained by using the general rule for the colours of the extreme squares (the left and the right), and these investigations were continued in [?]. This happens in the preceding examples: the top colour of the triangle is white, and this colour would also be the result if we applied the rule to the left and right colours of the first row.

And the top of the pyramid is light gray, the same as the resulting colour of the corner colours of the first layer.

We will show that similar predictions are possible in hyperspace.

The notation will be similar as in [?] and [?]:

- Fix an integer $n \geq 2$ and define $\Psi_n : A_{d,n} \to A_{d,1} = \Delta$ by

$$\Psi_n := \Phi_2 \circ \Phi_3 \circ \cdots \circ \Phi_n.$$

  Ψ_n associates to a first layer the top colour.

- Call n ϕ_α-*simple* if

$$\Psi_n\big((x_{i_1,\ldots,i_d})\big) = \phi_\alpha\big((x_{j_1(n-1),\ldots,j_d(n-1)})_{j_1,\ldots,j_d\in\{0,1\}}\big).$$

  In other words: the top colour is the ϕ_α-result of the corner colours of the starting layer, and with the preceding examples we illustated the fact that $n = 10$ is ϕ_α-simple for the α under consideration.

We will characterize the ϕ_α-simple integers in the next sections, the main result is theorem 1 below. Since the investigations are rather technical we will treat the case $d = 2$ first. In this way we can present the relevant ideas much simpler than for the general situation.

The paper closes with some proposals for magicians in hyperspace.

The case $d = 2$: "ordinary" pyramids in $\mathbb{R}^3$

Our main result will be prepared by a number of lemmas. We start with some definitions.

The S-arrays and a characterization

In this section we will work with $d = 2$. Let $n \geq 2$ and $\alpha = (\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1})$ in $\mathbb{Z}^4$ be fixed. For $x \in \Delta$ and $i_1, i_2 \in \{0, \ldots, n-1\}$ we denote by $S^{n,x}_{i_1,i_2}$ the array in $A_{2,n}$ that is x at position (i_1, i_2) and zero at all other positions. We put $\sigma^{n,x}_{i_1,i_2} := \Psi_n(S^{n,x}_{i_1,i_2})$: this is the colour of the top cube if the bottom layer is simple: colour x at (i_1, i_2), the other cubes have the trivial colour.

Lemma 1: *n is ϕ_α-simple iff the following two properties hold:*
(i) $\sigma^{n,x}_{0,0} = \alpha_{0,0}x$, $\sigma^{n,x}_{0,n-1} = \alpha_{0,1}x$, $\sigma^{n,x}_{n-1,0} = \alpha_{1,0}x$, $\sigma^{n,x}_{n-1,n-1} = \alpha_{1,1}x$ for all x.
(ii) $\sigma^{n,x}_{i_1,i_2} = 0$ for all x and all (i_1, i_2) that do not lie in the set of corners $\mathcal{C} := \{(0,0), (0,n-1), (n-1,0), (n-1,n-1)\}$.

Proof: This assertion follows immediately from the formula

$$\Psi_n\big((x_{i_1,i_2})_{i_1,i_2=0,\dots,n-1}\big) = \sum_{i_1,i_2=0,\dots,n-1} \sigma_{i_1,i_2}^{n,x_{i_1,i_2}}$$

which is true by the additivity of the operations under consideration. □

Integers that are zero relative to Δ

The elements of our group Δ are multiplied by integers. For $k \in \mathbb{Z}$ we will write $k =_\Delta 0$ if $kx = 0$ for all $x \in \Delta$. In the following lemma we collect some elementary properties of this definition:

Lemma 2: (i) $\{k \mid k =_\Delta 0\}$ is an ideal in $\mathbb{Z}$ and thus of the fom $\beta\mathbb{Z}$.

(ii) The most general nontrivial finite abelian group Δ is a product of groups of type $(\mathbb{Z}_{p_\rho})^{t_\rho}$ for different primes p_ρ and $t_\rho \in \mathbb{N}$ $(\rho = 1, \dots, r)$. In this case β is the product of the p_ρ. In particular we have $\beta = p$ for $\Delta = (\mathbb{Z}_p)^t$.

The coefficients $C_{i_1,i_2}^{n,\eta}$

In order to apply lemma 1 we have to investigate the $\sigma_{i_1,i_2}^{n,x}$ more carefully. A recursion formula is easily established, one only has to check what happens with $S_{i_1,i_2}^{n,x}$ in the second layer:

$$\sigma_{i_1,i_2}^{n,x} = \alpha_{0,0}\sigma_{i_1,i_2}^{n-1,x} + \alpha_{0,1}\sigma_{i_1,i_2-1}^{n-1,x} + \alpha_{1,0}\sigma_{i_1-1,i_2}^{n-1,x} + \alpha_{0,0}\sigma_{i_1-1,i_2-1}^{n-1,x}.$$

(Here we put $\sigma_{i_1,i_2}^{m,x} := 0$ for all m if $i_1 = -1$ or $i_2 = -1$.)

It follows that there are $N_{i_1,i_2}^n \in \mathbb{Z}$ such that $\sigma_{i_1,i_2}^{n,x} = N_{i_1,i_2}^n x$, and N_{i_1,i_2}^n is a homogeous polynomial in $\alpha_{0,0}, \alpha_{0,1}, \alpha_{1,0}, \alpha_{1,1}$. In view of lemma 1 we have to check whether $N_{(n-1)j_1,j_2(n-1)}^n - \alpha_{j_1,j_2} =_\Delta 0$ for $j_1, j_2 = 0, 1$ and $N_{i_1,i_2}^n =_\Delta 0$ for $(i_1, i_2) \notin \mathcal{C}$. For some i_1, i_2 it is easy to find formulas for N_{i_1,i_2}^n. For example, if $(i_1, i_2) = (j_1(n-1), j_2(n-1))$ (with $j_1, j_2 = 0, 1$) lies in $\mathcal{C}$, then $N_{i_1,i_2}^n = \alpha_{j_1,j_2}^{n-1}$, but for the i_1, i_2 "in the middle" it seems hopeless to find easy explicit expressions.

N_{i_1,i_2}^n is a homogeneous polynomial af degree $n-1$ in the components of α. To describe it in more detail we introduce the following notation:

- By $\mathcal{E}_{n-1}$ we denote the collection of possible multi-exponents:

$$\mathcal{E}_{n-1} := \left\{(\eta_{0,0}, \eta_{0,1}, \eta_{1,0}, \eta_{1,1}) \mid \eta_{j_1,j_2} \in \mathbb{N}_0, \sum_{j_1,j_2=0,1} \eta_{j_1,j_2} = n-1\right\}.$$

- For $\eta = (\eta_{0,0}, \eta_{0,1}, \eta_{1,0}, \eta_{1,1}) \in \mathcal{E}_{n-1}$ the expression α^η means the integer $\alpha_{0,0}^{\eta_{0,0}} \cdot \alpha_{0,1}^{\eta_{0,1}} \cdot \alpha_{1,0}^{\eta_{1,0}} \cdot \alpha_{1,1}^{\eta_{1,1}}$. (For example, in the case $\eta = (1,3,4,0)$ and $\alpha = 10, 5, -2, 3)$ we have $\alpha^\eta = 10^1 \cdot 5^3 \cdot (-2)^4 \cdot 3^0$.)

With this notation it is possible to write N_{i_1,i_2}^n as

$$N_{i_1,i_2}^n = \sum_{\eta \in \mathcal{E}_{n-1}} C_{i_1,i_2}^{n,\eta} \alpha^\eta$$

for suitable $C^{n,\eta}_{i_1,i_2} \in \mathbb{N}_0$. We will find explicit expressions for these numbers.

In this way the $C^{n,\eta}_{i_1,i_2}$ are defined for $0 \leq i_1, i_2 \leq n-1$ and $\eta \in \mathcal{E}_{n-1}$. It will be convenient to extend the definition to all integers i_1, i_2 with $-1 \leq i_1, i_2$ and η with components in $\{-1, 0, 1, 2, \ldots\}$: the C for the new i_1, i_2, η are defined to be zero.

Lemma 3: *The $C^{n,\eta}_{i_1,i_2}$ satisfy the following conditions:*
(i) For $n = 2$ we have

$$C^{2,(1,0,0,0)}_{0,0} = C^{2,(0,1,0,0)}_{0,0} = C^{2,(0,0,1,0)}_{0,0} = C^{2,(0,0,0,1)}_{0,0} = 1$$

and all other $C^{2,\eta}_{i_1,i_2}$ are zero.
(ii) The following recursion formula holds:

$$\begin{aligned} C^{n,\eta}_{i_1,i_2} \;=\; & C^{n-1,(\eta_{0,0}-1,\eta_{0,1},\eta_{1,0},\eta_{1,1})}_{i_1,i_2} + C^{n-1,(\eta_{0,0},\eta_{0,1}-1,\eta_{1,0},\eta_{1,1})}_{i_1,i_2-1} + \\ & C^{n-1,(\eta_{0,0},\eta_{0,1},\eta_{1,0}-1,\eta_{1,1})}_{i_1-1,i_2} + C^{n-1,(\eta_{0,0},\eta_{0,1},\eta_{1,0},\eta_{1,1}-1)}_{i_1-1,i_2-1}. \end{aligned}$$

Proof: (i) This is an easy consequence of the definition of Φ_2. For example, $\sigma^{2,x}_{0,1} = \alpha_{0,1}\, x$ so that $N^n_{0,1} = \alpha_{0,1}$. Consequently $C^{2,(0,1,0,0)}_{0,1} = 1$ and the other $C^{2,\eta}_{0,1}$ vanish.
(ii) How can one arrive at a summand of type $\alpha^\eta x$ for the top colour after $n-1$ steps if one starts with $S^{n,x}_{i_1,i_2}$? The second layer has entry $\alpha_{0,0} \cdot x$ (resp. $\alpha_{0,1} \cdot x$ resp. $\alpha_{1,0} \cdot x$ resp. $\alpha_{1,1} \cdot x$) at position (i_1, i_2) (resp. $(i_1, i_2 - 1)$ resp. $(i_1 - 1, i_2)$ resp. $(i_1 - 1, i_2 - 1)$). Position i_1, i_2 will contribute to $\alpha^\eta \cdot x$ in $n-2$ further steps precisely $C^{n-1,(\eta_{0,0}-1,\eta_{0,1},\eta_{1,0},\eta_{1,1})}_{i_1,i_2}$ times, and taking into account the other three positions as well we arrive at the recursion formula. □

Walks

We now turn to the study of certain walks. There is a useful connection to the $C^{n,\eta}_{i_1,i_2}$, this will be crucial for the determination of ϕ_α-simple integers.

We will consider walks on $\mathbb{Z}^2$: they start at $(0,0)$, they terminate at (i_1, i_2) (where $0 \leq i_1, i_2$ are fixed), their length is $n-1$ and the allowed steps are $(0,0), (0,1), (1,0)$ and $(1,1)$. More precisely we define two-dimensioanl vectors v_{j_1,j_2} by $v_{j_1,j_2} := (j_1, j_2)$ for $j_1, j_2 = 0, 1$, and we are interested in sequences $v_1, v_2, \ldots, v_{n-1} \in \{v_{0,0}, v_{0,1}, v_{1,0}, v_{1,1}\}$ such that $\sum_{i=1}^{n-1} v_i = (i_0, j_0)$.

In fact, our investigations will have to be more subtly. Let $\eta \in \mathcal{E}_{n-1}$ be given. By $W^{n-1,\eta}_{i_1,i_2}$ we denote the number of walks of the above kind where among the $v_1, \ldots, v_{n-1}$ one finds η_{j_1,j_2} vectors v_{j_1,j_2} $(j_1, j_2 = 0, 1)$.

Remarks and examples: 1. $W^{n-1,\eta}_{i_1,i_2}$ will be different from zero if and only if $\sum_{j_1,j_2=0,1} \eta_{j_1,j_2} v_{j_1,j_2} = (i_1, j_1)$.
2. Suppose that $(i_1, i_2) = (0,0)$. There is only one walk that terminates there, namely the walk $v_{0,0}, \ldots, v_{0,0}$. This means that $W^{n-1,(n-1,0,0,0)}_{0,0} = 1$, and all other $W^{n-1,\eta}_{0,0}$ vanish.

3. Now we consider $(i_1, i_2) = (0, i)$ for some $i \in \{1, \ldots, n-2\}$. In order to arrive there we must use only the vectors $v_{0,0}$ and $v_{0,1}$. More precisely: one needs i vectors $v_{0,1}$ and $(n-1)-i$ vectors $v_{0,0}$. There are $\binom{n-1}{i}$ possibilities to do this, and this means that $W_{0,i}^{n-1,((n-1)-i,i,0,0)} = \binom{n-1}{i}$, and the other $W_{0,i}^{n-1,\eta}$ are zero.

4. In the preceding examples only one $W_{i_1,i_2}^{n-1,\eta}$ was different from zero. This occurs rarely: Suppose, e.g., that $(i_1, i_2) = (2, 2)$ and $n = 5$. How can we walk from $(0, 0)$ to $(2, 2)$ in four steps? There are several possibilities:

- Use two $v_{0,0}$ and two $v_{1,1}$.
- Use $v_{0,0}$, $v_{1,0}$, $v_{0,1}$, $v_{1,1}$, each of them once.
- etc.

It follows that $W_{2,2}^{4,\eta}$ does not vanish for $\eta = (2, 0, 0, 2), (1, 1, 1, 1), \ldots$.

5. It will be convenient to extend the definition by allowing that i_1 or i_2 or both are -1. Since in this case there are no walks that start at $(0, 0)$ and terminate there the associated W is defined to be zero.

The $W_{i_1,i_2}^{n-1,\eta}$ can be determined recursively. Suppose we want to arrive at (i_1, i_2) after $n-1$ steps subject to the condition that we use η_{j_1,j_2} times the vector v_{j_1,j_2} $(j_1, j_2 = 0, 1)$. Our first step will us lead to $(0, 0), (0, 1), (1, 0)$ or $(1, 1)$. Suppose that we are then at $(0, 1)$. To come to (i_1, i_2) we must continue with a walk of length $n-2$ from $(0, 0)$ to $(i_1, i_2 - 1)$. Similarly one can deal with the other three positions after the first step.

This leads to the recursion

$$\begin{aligned} W_{i_1,i_2}^{n-1,\eta} \;=\; & W_{i_1,i_2}^{n-2,(\eta_{0,0},\eta_{0,1},\eta_{1,0},\eta_{1,1})} + W_{i_1,i_2-1}^{n-2,(\eta_{0,0},\eta_{0,1}-1,\eta_{1,0},\eta_{1,1})} + \\ & W_{i_1-1,i_2}^{n-2,(\eta_{0,0},\eta_{0,1},\eta_{1,0}-1,\eta_{1,1})} + W_{i_1-1,i_2-1}^{n-2,(\eta_{0,0},\eta_{0,1},\eta_{1,0},\eta_{1,1}-1)}. \end{aligned}$$

And how many walks are there for $n = 1$? Only the $\eta = (1, 0, 0, 0), (0, 1, 0, 0)$, $(0, 0, 1, 0), (0, 0, 0, 1)$ will have to be considered. There is only one walk associated with each such η, and they terminate at $(0, 0), (0, 1), (1, 0), (1, 1)$, respectively. In other words:

$$W_{0,0}^{1,(1,0,0,0)} = W_{0,0}^{1,(0,1,0,0)} = W_{0,0}^{1,(0,0,1,0)} = W_{0,0}^{1}, (0, 0, 0, 1) = 1$$

and all other W_{i_1,i_2}^{2}, η are zero.

A formula for the $C_{i_1,i_2}^{n,\eta}$

Now we can calculate the $C_{i_1,i_2}^{n,\eta}$. We only have to combine the following two facts:

- The $C_{i_1,i_2}^{n,\eta}$ satisfy the same recursion formula as the $W_{i_1,i_2}^{n-1,\eta}$, and we have seen that the initial conditions are also the same. Thus $C_{i_1,i_2}^{n,\eta} = W_{i_1,i_2}^{n-1,\eta}$.

- $W^{n-1,\eta}_{i_1,i_2}$ can be determined with the help of elementary combinatorics: given $\eta \in \mathcal{E}_{n-1}$ such that $\sum_{j_1,j_2=0,1} \eta_{j_1,j_2} v_{j_1,j_2} = (i_1, i_2)$ we ask for the number of possibilities to put η_{j_1,j_2} vectors v_{j_1,j_2} in a sequence of $n-1$ vectors (all $(j_1, j_2 = 0, 1)$). There are $\binom{n-1}{\eta_{0,0}}$ possibilities to place $v_{0,0}$, there remain $(n-1) - \eta_{0,0}$ places for the $v_{0,1}$ $(= \binom{(n-1)-\eta_{0,0}}{\eta_{0,1}}$ possibilities) etc. It follows that $W^{n-1,\eta}_{i_1,i_2}$ is the product of $\binom{n-1}{\eta_{0,0}}$, $\binom{n-1-\eta_{0,0}}{\eta_{0,1}}$, $\binom{n-1-\eta_{0,0}-\eta_{0,1}}{\eta_{1,0}}$ and $\binom{n-1-\eta_{0,0}-\eta_{0,1}-\eta_{1,0}}{\eta_{1,1}}$. (The last factor is $\binom{\eta_{1,1}}{\eta_{1,1}} = 1$.)

In our argument we started with $\eta_{0,0}$, then we used $\eta_{0,1}$ etc. But any other order to deal with the components of η would work as well. For the sake of easy reference we formulate this observation as

Lemma 4: *Let e_1, e_2, e_3, e_4 be any enumeration of the components of η. Then*

$$\begin{aligned} C^{n,\eta}_{i_1,i_2} &= W^{n-1,\eta}_{i_1,i_2} \\ &= \binom{n-1}{e_1}\binom{n-1-e_1}{e_2}\binom{n-1-e_1-e_2}{e_3}. \end{aligned}$$

The main theorem

Our preparations are nearly complete. It only remains to remind the reader to Balak Ram's result [?] on binomial coefficients:

- Let p be a prime and m an integer. Then all $\binom{m}{l}$ for $l = 1, \ldots, m-1$ are divisible by p iff there is an s such $m = p^s$.
- Let m, r be integers such that $m > r > 1$. If r divides all $\binom{m}{l}$ for $l = 1, \ldots, m-1$ then r is a prime and – by the first part – m is of the form r^s.

A proof can be found in [?] and [?] (for a far-reaching generalization see [?]).

The following theorem summarizes our main results:

Theorem: *Let p be prime number and Δ the group $\mathbb{Z}_p^t$ for an integer t. Further let $\alpha = (\alpha_{j_1,j_2})_{j_1,j_2=0,1}$ with $\alpha_{j_1,j_2} \in \mathbb{Z}$ be given.*

(i) Suppose that $\alpha_{j_1,j_2} = 0 \bmod p$ for all j_1, j_2. Then all $n > 2$ are ϕ_α-simple.

(ii) Suppose that all but one $\alpha_{j_1 j_2}$ are zero modulo p. We will call this nonzero component γ. Denote by π the order of γ in the group of invertible elements of $\mathbb{Z}_p$, i.e., the smallest m in $\mathbb{N}$ such that $\gamma^m = 1$. Then an integer $n > 2$ is ϕ_α-simple iff $(n-1) \bmod \pi = 1$. In particular the numbers of the form $p^s + 1$ are ϕ_α-simple.

(iii) Now suppose that there are at least two $\alpha_{j_1 j_2}$ that are not zero modulo p. Then an integer $n > 2$ is ϕ_α-simple iff it is of the form $p^s + 1$ for some $s \in \mathbb{N}$.

Proof: (i) This is obvious.

(ii) Suppose, for example, that $\gamma = \alpha_{0,0} \neq 0 \bmod p$ and the others are zero. Then $\sigma^{n,x}_{0,0} = \gamma^{n-1}\, x$ and the other $\sigma^{n,x}_{i_1,i_2}$ are zero. Thus, by lemma 1, an integer n will be ϕ_α-simple iff $\gamma^{n-1} - \gamma =_\Delta 0$. And this is obviously the case iff $(n-1) \bmod \pi = 1$

(iii) Suppose that n is of the form p^s+1. We have to check whether the conditions of lemma 1 are satisfied. That $\alpha^{n-1}_{j_1(n-1),j_2(n-1)} = \alpha_{j_1(n-1),j_2(n-1)}$ for all $j_1, j_2 = 0, 1$ follows from the little Fermat theorem. What about the second condition of lemma 1? Let (i_1, i_2) be a tuple that does not lie in the corner set $\mathcal{C}$. Suppose, e,g, that i_1 lies strictly between 0 and $n-1$. Let us consider the $W^{n-1,\eta}_{i_1,i_2}$. If this number is different from zero we have $\eta_{0,1,0,0} + \eta_{0,0,0,1} = i_1$ so that one of the components of η must lie strictly between 0 and $n-1$. With the help of lemma 4 we may conclude from Ram's theorem that $W^{n-1,\eta}_{i_1,i_2} = C^{n,\eta}_{i_1,i_2} = 0 \bmod p$. And this proves that $\sigma^{n,x}_{i_1,i_2} = 0$.

Now suppose that $n-1$ is *not* of the form p^s. We will show that there are (i_1, i_2) that do not lie in the corner set $\mathcal{C}$ and an $x \in \mathbb{Z}_p$ such that $\sigma^{n,x}_{i_1,i_2} \neq 0$ so that, by lemma 1, n is not ϕ_α-simple.

Case 1: There are two α_{j_1,j_2} that are not zero in $\mathbb{Z}_p$ and for which the j_1 or j_2 coincide. Suppose, for example, that $\alpha_{0,0}, \alpha_{0,1} \neq 0 \bmod p$.

By the second part of Ram's theorem there is a $k \in \{1, \ldots, n-2\}$ such that $\binom{n-1}{k} \neq 0 \bmod p$. We consider $(i_1, i_2) := (0, k)$. The only η such that $C^{n,\eta}_{0,k}$ is different from zero is $\eta' = (n-1-i, i, 0, 0)$, and $C^{n,\eta'}_{0,k} = \binom{n-1}{k}$ so that $\sigma^{n,x}_{0,k} = \binom{n-1}{k}\alpha^{n-1-k}_{0,0} \cdot \alpha^k_{0,1}\, x$. This number is different from zero for every $x \neq 0$ in $\mathbb{Z}^t_p$ since $\mathbb{Z}_p$ is a field.

Case 2: Case 1 does not hold. Then the two nonzero components of α are either $\alpha_{0,0}, \alpha_{1,1}$ or $\alpha_{0,1}, \alpha_{1,0}$. Suppose that $\alpha_{0,0}, \alpha_{1,1} \neq 0 \bmod p$.

This time we work with $(i_1, i_2) = (k, k)$, where k is as in case 1. From $\alpha_{0,1} = \alpha_{1,0} = 0$ we conclude that $\sigma^{n,x}_{k,k} = \binom{n-1}{k}\alpha^{n-1-k}_{0,0} \cdot \alpha^k_{1,1}\, x$, and this number is different from zero for every $x \neq 0$. □

In order to generalize this theorem to the case of arbitrary finite abelian groups one only has to combine the following three facts:

- Suppose that Δ' is a subgroup of Δ. If n is ϕ_α-simple when working with Δ it will be also ϕ_α-simple with respect to Δ'.
- If $\Delta = \Delta_1 \times \Delta_2$ is a product group an n is ϕ_α-simple for Δ iff it is ϕ_α-simple for Δ_1 and for Δ_2 simultaneously.
- Every nontrivial finite abelian group Δ is of the form $\prod_{\rho=1,\ldots,r}(\mathbb{Z}_{p_\rho})^{t_\rho}$ for different primes p_ρ and $t_\rho \in \mathbb{N}$.

In this way we can characterize the ϕ_α-simple n for all Δ. One only has to check how many α_{j_1,j_2} vanish modulo $p_1, p_2, \ldots, p_r$, respectively. We only mention an interesting consequence: suppose that there are at least two p among the p_ρ such that there are at least two α_{j_1,j_2} that are not zero modulo p. (This is, for example true if $r > 1$ and all α_{j_1,j_2} lie in $\{-1, 1\}$.) Then there are no ϕ_α-simple $n > 2$. For a proof one only has to note that it is not possible for an integer to be of the form $p^s + 1$ for two different p simultaneously.

The case of arbitrary d: hyperpyramids in $\mathbb{R}^{d+1}$

Fortunately one needs no new ideas to treat the case of arbitrary d. Only the number of indices will increase. Therefore we will restrict ourselves to a rough sketch how to proceed.

1. Choose Δ as before and fix $d \in \mathbb{N}$ and α as in the introduction.

2. For $x \in \Delta$ we denote by $S^{n,x}_{i_1,\ldots,i_d} \in A_{d,n}$ the element where $(i_1,\ldots,i_d)$ has colour x and all other colours are zero. And $\sigma^{n,x}_{i_1,\ldots,i_d}$ is the top colour when starting with $S^{n,x}_{i_1,\ldots,i_d}$ as the first layer.

3. $N^n_{i_1,\ldots,i_d}$, $\mathcal{E}_{n-1} \subset \mathbb{N}_0^{2^d}$ and $C^{n,\eta}_{i_1,\ldots,i_d}$ denote the natural generalizations of the $N^n_{i_1,i_2}$, $\mathcal{E}_{n-1} \subset \mathbb{N}_0^4$ and $C^{n,\eta}_{i_1,i_2}$ of the previous section.

4. It will then be crucial to see that $C^{n,\eta}_{i_1,\ldots,i_d}$ can be calculated as the number of walks in $\mathbb{Z}^d$ of length $n-1$ from the origin to $(i_1,\ldots,i_d)$ that use $\eta_{j_1,\ldots,j_d}$ steps of type $(j_1,\ldots,j_d)$ for all $j_1,\ldots,j_d = 0,1$.

5. In this way one obtains a formula for $C^{n,\eta}_{i_1,\ldots,i_d}$. The most important consequence is that these numbers vanish modulo p for the $(i_1,\ldots,i_d)$ "in the middle" if $\Delta = (\mathbb{Z}_p^t)$ and n is of the form p^s+1.

6. This is the essential ingredient to prove a generalization of theorem 1 for the case of arbitrary d and $\Delta = (\mathbb{Z}_p)^t$. Not much further work is necessary for a complete proof:

- That condition (i) of lemma 1 is satisfied for $n = p^s+1$ follows again from the little Fermat theorem.

- For the reverse implication (only the $n = p^s+1$ are ϕ_α-simple if there are at least two nontrivial $\alpha_{j_1,\ldots,j_2}$) we argue as follows.

  Suppose that at least two $\alpha_{j_1,\ldots,j_d}$ are nonzero modulo p. Without loss of generality $\alpha_{0,0,\ldots,0}$ is one of them. Now choose an $\alpha_{j_1,\ldots,j_d} \neq 0 \bmod p$ in the collection of remaining nonzero (modulo p) $\alpha_{j_1,\ldots,j_d}$ such that $\{\kappa \mid j_\kappa = 0\}$ has the maximal number of elements[1]. Without loss of generality we may assume that we chose $\alpha_{1,1,\ldots,1,0,\ldots,0}$ (δ 1's followed by $d-\delta$ zeros, where $1 \leq \delta \leq d$.) Then we know that $\alpha_{j_1,\ldots,j_\delta,0,\ldots,0} = 0$ unless $j_1 = \cdots = j_\delta = 1$. And now we can copy the proof of the second half of (iii) in theorem 1: If n is not of the form p^s+1 choose $k \in \{1,\ldots,n-1\}$ with $\binom{n-1}{k} \neq 0 \bmod p$. Then one has

  $$\sigma^{n,x}_{k,\ldots,k,0,\ldots,0} = \binom{n-1}{k} \alpha^{n-1-k}_{0,\ldots,0} \cdot \alpha^k_{1,\ldots,1,0,\ldots,0}\, x,$$

  and this is not zero for $x \neq 0$. By lemma 1, n is not ϕ_α-simple.

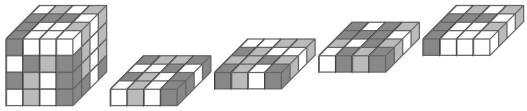
Some proposals for magicians in hyperspace

[1] More precisely, let us denote by $K \subset \{0,1\}^d \setminus (0,\ldots,0)$ the collection of $(j_1,\ldots,j_d)$ with $\alpha_{j_1,\ldots,j_d} \neq 0 \bmod p$. The map $\tau : K \to \{0,\ldots,d-1\}$ counts the number of zeros, and we choose a $(j_1,\ldots,j_d)$ where τ is maximal

Dear magician in $\mathbb{R}^{d+1}$ with $d > 2$! It is to be hoped that you have an audience that likes lengthy calculations. If you start with a ϕ_α-simple n they will have to select n^d colours from $\mathbb{Z}_p$ for the first layer. Each new colour for the little cubes of the further layers necessitates the calculation of a sum of 2^d numbers, and this has to be done $(n-1)^d + (n-2)^d + \cdots + 1$ times. But at such an occasion you can present your spectacular magic trick: immediately after the choice of the first layer you can write down your prediction of the top colour, and this will turn out to be true!

Suppose that you work in four dimensions, please allow us to see you in action. For simplicity you work with $\mathbb{Z}_3$ with the colour convention of the first section, and with α defined by $\alpha_{0,0,0} := 2$ and $\alpha_{j_1,j_2,j_3} := 1$ for the other components of α you choose the modest ϕ_α-admissible number $n = 4$ for your trick.

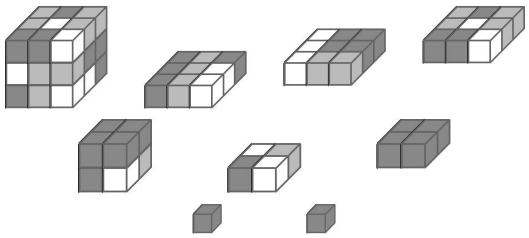
Someone in the audience proposes a starting pattern. For us who live in $\mathbb{R}^3$ we represent it as a cube, and since we want to have a look inside we even sketch the four layers of it separately.



Now it is your turn: the corner colours are $x_{0,0,0} = 2$, $x_{0,0,3} = 2{,}0, 2, 0, 1, 2, 0$[2], and by the choice of α you have to calculate two times the first colour plus the sum of the remaining ones: $2 \cdot 2 + 2 + 0 + 2 + 0 + 1 + 2 + 0 = 2$. Thus your prediction of the final colour is "dark gray".

Now your visitors will have to work. Wherever 8 little four-dimensional cubes meet they have to put "on top" of them a cube with a new colour. In our case it is the sum of the 8 colours, but the colour of the left/back/bottom-cube counts twice. They do this $3^3 + 2^3 + 1^3 = 36$ times, and then they have built a little pyramid in $\mathbb{R}^4$. The top colour really is "dark gray" as predicted.

In the following pictures there are depicted the intermediate steps of this construction:



We close this section with two advices for an audience of non-mathematicians: it might happen that they don't like the calculations in $\mathbb{Z}_p$.

[2]Recall that $x_{0,0,0}$ is in the back to the left of the bottom layer, $x_{0,1,0}$ is the second cube from the left in the back row of the bottom layer etc.

- Choose the simplest group, $\Delta = \mathbb{Z}_2$, and represent 0 and 1 by colours, e.g. by white (for 0) and green (for 1). The admissible n are the numbers $2^s + 1$ and there are in fact not many choices for the $\alpha_{j_1,\ldots,j_d}$. Suppose that you decided that all of them are 1. Then the audience simply will have to calculate a sum in $\mathbb{Z}_2$, and this can be translated as follows:

  > Suppose that you see j green cubes among the adjacent 2^d cubes that determine the new colour c. Choose c such that the total number of green cubes is now even. (In other words, c is green if j is odd and red otherwise.)

- Also rather simple is the case $\Delta = \mathbb{Z}_3$ together with α where all $\alpha_{j_1,\ldots,j_d}$ equal 2. You work with three colours, e.g. with white (for 0), light gray (for 1) and dark gray (for 2). It will be necessary to calculate expressions $-a_1 - a_2 - \cdots - a_k$ in $\mathbb{Z}_3$. This can be done by using the following rules:
  - Cancel all red colours, then all pairs blue/green, and then each three of the same colour.
  - There will remain: no colour / a single colour / a pair of the same color.
  - In the first case chooose white as the new colour, in the second the other one in the pair light gray/dark gray and in the third the colour of the pair.

  E.g., if your visitors have to treat w,w,lg,dg,dg,dg,lg,lg,lg,lg,lg,dg,dg,w,lg during your presentation in $\mathbb{R}^5$ they will arrive at "dg" after the first step so that the new colour is light gray .

Good luck for your performances!

References

[1] E. Behrends, St. Humble. *Triangle Mysteries.*. The Mathematical Intelligencer, 35 (2013). pp. 10 – 15.

[2] E. Behrends. *Pyramid Mysteries.*. To appear in the Mathematical Intelligencer.

[3] H. Joris, C. Oestreicher, and J. Steinig. *The greatest common divisor of certain sets of binomial coefficients.* J. Number Theory, 21 (1985). pp. 101 -119.

[4] Balak Ram. *Common Factors of* $\frac{n!}{m!(n-m)!}$, $m = 1, \ldots, n-1$. Journal of the Indian Mathematical Club, 1 (1909). pp. 39 – 43.

Ehrhard Behrends
Mathematisches Institut, Freie Universität Berlin
Arnimallee 6
D-14 195 Berlin
Germany
e-mail: behrends@math.fu-berlin.de