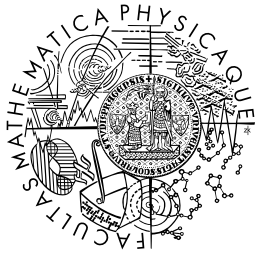

FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

**BACHELOR THESIS**

Nikita Edward Carulkov

# Multiplication in a finite field of characteristic 2 and XOR-metrics

Department of Algebra

Supervisor of the bachelor thesis: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.

Study programme: Mathematics

Study branch: Mathematics for Information Technologies

Prague 2020

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In ..... date .....  .....

Author's signature

I would like to thank the supervisor of this bachelor thesis, Jan Žemlička, for his patience, guidance, and valuable comments.
I would like to thank my parents and my family for a kind and tolerant support.

Title: Multiplication in a finite field of characteristic 2 and XOR-metrics

Author: Nikita Edward Carulkov

Department: Department of Algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of Algebra

Abstract: XOR-counts measure the efficiency of multiplication in finite fields of characteristic 2. In the first chapter we define two XOR-counts (the direct XOR-count and the sequential XOR-count) and present detailed proofs of some propositions from the paper from Lukas Kolsch about the XOR-counts of inverse matrices and permutation similar matrices. It seems that the case when the direct XOR-count is lower than the sequential XOR-count is rare. We will explore those cases in the second chapter. Some of them were already described in the paper from Lukas Kolsch and we prove that they occur only for matrices with order higher or equal to six.

Keywords: lightweight cryptography, XOR-count, multiplication in a finite field of characteristic 2

# Obsah

# Introduction

## Notation

We denote the field with two elements (i.e. binary field) by $\mathbb{F}_2$ in this thesis. By $\mathbb{F}_2^m$ we denote field with $2^m$ elements, which can be represented by polynomials of degree at most $m-1$. By XOR operation we mean addition in a binary field.

## Motivation

In recent years, with the emerge of the Internet of Things (i.e. IoT), the need for performing cryptography on devices with restricted computation capacity grew. Many devices such as RFID tags, sensor networks, or any small appliances with the connection to the Internet do not have enough computing power to perform standard cryptographical algorithms. Therefore new branch of cryptography developed — lightweight cryptography. Lightweight cryptography is a compromise between security and computing power needed to perform cryptography primitives. The goal of the lightweight cryptography is the minimization of the resources needed to perform a cryptography operation.

The security aspects usually do not depend on the specific implementation of some cryptographic operations [Köl19, BKL16]. Therefore, it is an interesting task to investigate, which representation of finite field elements uses fewer resources.

Linear layers (e.g. `Mix Columns` in AES) are usually linear mappings $\mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n,\ n, m \in \mathbb{N}$, which can be represented with a matrix of order $n$ with entries from $\mathbb{F}_{2^m}$. By exchanging each entry of this matrix for a companion matrix (see the definition 1.10) we get a matrix of order $m \cdot n$ with entries from $\mathbb{F}_2$. And thus resources that are used by some implementation are dependent on the number of XOR operations (i.e. additions in the binary field). Therefore it is of interest to us to determine the number of XOR operations needed to perform matrix multiplication.

In this thesis, we present two XOR-metrics — sequential XOR-count and direct XOR-count. In the first chapter, we define both XOR-metrics and prove observations and theorems regarding XOR-counts of matrix and its inverse. In the second chapter, we further explore matrices with direct XOR-count lower than sequential XOR-count.

# 1. Determining XOR-counts

In this chapter, we will properly define the s-XOR-count and the d-XOR-count. Then we will explore what are their differences and what they represent. We will prove some lemmas and observations regarding their relationship and regarding their relationship with permutations. At the end of this chapter, we will present and prove a theorem that allows us to determine the s-XOR-count of the inverse matrix $M^{-1}$ given the s-XOR-count of $M$ and some additional assumptions.

Most of the definitions, examples, and theorems in this chapter are inspired the by article [Köl19]. Our proofs are conducted similarly and often they are more detailed.

**Definition 1.1.** The direct XOR-count *(the d-XOR-count)* of an **invertible** $n \times n$ matrix $M$ over $\mathbb{F}_2$, denoted by $wt_d(M)$ is

$$wt_d(M) = \omega(M) - n$$

where $\omega(M)$ denotes the number of ones in the matrix $M$.

Notice that the d-XOR-count is always non-negative because the minimal number of ones in an invertible matrix of order $n$ is $n$ (fewer ones would mean that some columns of the matrix have only zeros in them, which would mean that the matrix is singular and therefore not invertible) and thus according to the previous definition $wt_d(M) \geq n - n = 0$.

Now we define the sequential XOR-count metric, which helps us determine how many row additions we need to perform when transforming a matrix into a permutation matrix. But first, let us define the addition matrix.

**Definition 1.2.** Let $I_n$ be the identity matrix of order $n$ and $E_{i,j}$ matrix that has exactly one '1' in the i-th row and in the j-th column. Then matrix

$$A_{i,j} = I_n + E_{i,j}, \quad i \neq j$$

is called the *addition matrix*. Let us further denote a set of all addition matrices of order $n$ as $\mathcal{A}(n)$.

Notice that left multiplication with an addition matrix $A_{i,j}$ adds j-th row to i-th row, right multiplication with addition matrix adds the i-th column to the j-th column and that the addition matrix $A_{i,j}$ is involutory (i.e. self-inverse).

**Definition 1.3.** Let $\sigma \in S_n$ be a permutation of $n$ elements. We define the *permutation matrix* $P_\sigma$ as a matrix that permutes rows of an arbitrary matrix according to the permutation $\sigma$, in other words

$$P_\sigma = \begin{pmatrix} e^n_{\sigma(1)} \\ e^n_{\sigma(2)} \\ \vdots \\ e^n_{\sigma(n)} \end{pmatrix}$$

where $e^n_i$ denotes row of dimension n with exactly one '1' on the $i$-th position and with other entries equal to '0'. We will denote the set of all permutation matrices of order $n$ by $\mathcal{P}(n)$. We define the *permutation similarity* of matrices $M_1$ and $M_2$ as

$$\exists P_\sigma \in \mathcal{P}(n) : P_\sigma^{-1} M_1 P_\sigma = M_2$$

and denote as $M_1 \approx M_2$.

**Definition 1.4.** An **invertible** matrix $M$ over $\mathbb{F}_2$ has the sequential XOR-count (*the s-XOR-count*) of $t$, if $t$ is the minimal number such that

$$M = P_\sigma \prod_{k=1}^{t} A_{i_k,j_k}$$

where $P_\sigma \in \mathcal{P}(n)$ and $A_{i_k,j_k} \in \mathcal{A}(n)$. Such representation of $M$ is called the *s-XOR-representation* of $M$ and the s-XOR-representation with $wt_s(M)$ addition matrices is called the *optimal s-XOR-representation*.

We now show an example in which we illustrate two XOR-counts we just defined.

**Example 1.5.** The d-XOR-count of the matrix $M$ equals to 6 ($wt_d(M) = \omega(M) - n = 10 - 4 = 6$), but at the same time multiplication with this matrix can be implemented with only 3 XOR operations, since the results of previous steps can be reused.

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_1 + a_2 \\ (a_1 + a_2) + a_3 \\ ((a_1 + a_2) + a_3) + a_4 \end{pmatrix}$$

Notice that $wt_s(M) = 3$ and the optimal s-XOR-representation is $M = I_4 \cdot A_{4,3} \cdot A_{3,2} \cdot A_{2,1}$, which is exactly how vector on the right side is constructed.

Now we know that the s-XOR-count gives us information about how the matrix was constructed. More precisely, the minimal number of row addition operations we used to construct the matrix. While the d-XOR-count rather gives us information about how the matrix looks like and how the construction turned out. More precisely, how many entries of the vector $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 \end{pmatrix}^T$ we added to other rows of the same vector. Although this is yet to be proven, empirically speaking, it seems that most matrices will have the s-XOR-count lower than the d-XOR-count, but there are relatively rare cases when the d-XOR-count is indeed lower than the s-XOR-count, which we will explore in the second chapter.

Let us prove the following observation which we use to prove some theorems.

**Observation 1.6.** *For any $P_\sigma \in \mathcal{P}(n)$ and any $A_{i,j} \in \mathcal{A}$ holds*

$$P_\sigma A_{\sigma(i),\sigma(j)} = A_{i,j} P_\sigma.$$

*Důkaz.* Let $P_\sigma \in \mathcal{P}(n)$ with '1's on positions $(i, \sigma(i))$ and $(j, \sigma(j))$. Then $A_{i,j}P_\sigma$ has '1's on positions $(i, \sigma(i))$, $(j, \sigma(j))$ and $(i, \sigma(j))$, because we added $j$-th row of $P_\sigma$ to the $i$-th row. Now let us consider $P_\sigma A_{\sigma(i),\sigma(j)}$. In this case we add $\sigma(i)$-th column of $P_\sigma$ to the $\sigma(j)$-th column of $P_\sigma$. That means that $P_\sigma$ has '1's on position $(i, \sigma(i))$, $(j, \sigma(j))$ and $(i, \sigma(j))$. And thus $P_\sigma A_{\sigma(i),\sigma(j)} = A_{i,j} P_\sigma$.

$$P_\sigma = \begin{array}{c} \begin{matrix} \sigma(i) & & \sigma(j) \end{matrix} \\ \begin{pmatrix} & & \\ & & 1 \\ & & \\ 1 & & \\ & & \end{pmatrix} \end{array} \begin{matrix} \\ \\ j \\ \\ i \\ \\ \end{matrix}, A_{i,j} \cdot P_\sigma = \begin{array}{c} \begin{matrix} \sigma(i) & & \sigma(j) \end{matrix} \\ \begin{pmatrix} & & \\ & & 1 \\ & & \\ 1 & & 1 \\ & & \end{pmatrix} \end{array} \begin{matrix} \\ \\ j \\ \\ i \\ \\ \end{matrix} = P_\sigma \cdot A_{\sigma(i),\sigma(j)}$$

□

The following observations describe the relationship between the d-XOR-counts of permutation similar matrices.

**Observation 1.7.** *Let $M \in GL(n, \mathbb{F}_2)$. Then $wt_d(M) = wt_d(P_\sigma M P_\rho)$, where $P_\sigma, P_\rho \in \mathcal{P}(n)$.*

*Důkaz.* When the matrix $M$ is multiplied with $P_\sigma$ from the left side, it permutes rows of this matrix and when we use $P_\rho$ from the right side, it permutes columns of matrix $M$, therefore neither of those operations change the number of ones in the matrix $M$ and the order of the matrix $P_\sigma M P_\rho$ is the same as of the matrix $M$, which implies $wt_d(M) = wt(M) - n = wt(P_\sigma M P_\rho) - n = wt_d(P_\sigma M P_\rho)$. □

Similarly to the previous observation, the following lemma describes the relationship between the s-XOR-counts of permutation similar matrices.

**Lemma 1.8.** *Let $M \in GL(n, \mathbb{F}_2)$. Then $wt_s(M) = wt_s(P_\sigma M P_\rho)$, where $P_\sigma, P_\rho \in \mathcal{P}(n)$.*

*Důkaz.* Suppose that $wt_s(M) = t$. From Observation 1.6 we obtain second equality

$$\begin{aligned} P_\sigma M P_\rho &= P_\sigma \cdot P_\tau \prod_{k=1}^{t} A_{i_k, j_k} \cdot P_\rho \\ &= P_\sigma \cdot P_\tau \cdot P_\rho \prod_{k=1}^{t} A_{\rho(i_k), \rho(j_k)} \\ &= P_{\rho \circ \tau \circ \sigma} \prod_{k=1}^{t} A_{\rho(i_k), \rho(j_k)}, \end{aligned}$$

where $P_\tau \in \mathcal{P}(n)$. Furthermore, $P_{\rho\circ\tau\circ\sigma} \in \mathcal{P}(n)$, since the product of permutation matrices is also a permutation matrix. Thus $wt_s(P_\sigma M P_\rho) \leq t = wt_s(M)$. We prove that $wt_s(M) \leq wt_s(P_\sigma M P_\rho)$ by using the proven fact for $\tilde{M} = P_\sigma M P_\rho$ and $P_{\tilde{\sigma}} = P_{\sigma^{-1}}, P_{\tilde{\rho}} = P_{\rho^{-1}}$. We obtain $wt_s(\tilde{M}) \geq wt_s(P_{\tilde{\sigma}} \tilde{M} P_{\tilde{\rho}}) = wt_s(M)$, which implies desired equation $wt_s(M) = wt_s(P_\sigma M P_\rho)$. □

**Definition 1.9.** Let $M_1, ..., M_d$ be square matrices. We denote a block matrix consisting of these matrices by

$$\bigoplus_{k=1}^{d} M_k = \begin{pmatrix} M_1 & & & 0 \\ & M_2 & & \\ & & \ddots & \\ 0 & & & M_d \end{pmatrix}.$$

We call this matrix a *block diagonal matrix*.

**Definition 1.10.** Let $p$ be a polynomial such that $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_2[x]$. We define the *companion matrix* to a polynomial $p$ as

$$C_p = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & 0 & \cdots & 0 & a_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & a_{n-1} \end{pmatrix}.$$

**Definition 1.11.** Let $P_\sigma \in \mathcal{P}(n)$. We say that $P_\sigma$ is in the *cycle normal form* when $P_\sigma$ is permutation similar to $\bigoplus_{k=1}^{d} C_{x^{m_k}+1}$.

$$P_\sigma \approx \bigoplus_{k=1}^{d} C_{x^{m_k}+1}$$

for some $m_k$ which fulfill $\sum_{k=1}^{d} m_k = n$ and $m_1 \geq \cdots \geq m_d \geq 1$.

**Observation 1.12.** *Any permutation matrix is permutation-similar to a permutation matrix in a cycle normal form. And therefore*

$$P_\sigma \prod_{k=1}^{t} A_{i_k,j_k} \approx P_{\sigma'} \prod_{k=1}^{t} A_{\rho^{-1}(i_k),\rho^{-1}(j_k)}$$

*for permutation $\rho \in S_n$, where $\sigma' = \rho \circ \sigma \circ \rho^{-1}$ where $P_{\sigma'}$ is the cycle normal form of $P_\sigma$.*

*Důkaz.* Let $P_\rho \in \mathcal{P}(n)$ such that $P_\rho P_\sigma P_\rho^{-1} = P_{\rho'}$, thus $\rho \in S(n)$ must be such that $\sigma' = \rho^{-1} \circ \sigma \circ \rho$. Together we get

$$\begin{aligned} P_\sigma \prod_{k=1}^{t} A_{i_k,j_k} &\approx P_\rho P_\sigma \prod_{k=1}^{t} A_{i_k,J_k} P_\rho^{-1} \\ &= P_\rho P_\sigma P_\rho^{-1} \prod_{k=1}^{t} A_{\rho^{-1}(i_k),\rho^{-1}(i_k)} \\ &= P_{\sigma'} \prod_{k=1}^{t} A_{\rho^{-1}(i_k),\rho^{-1}(j_k)} \end{aligned}$$

□

To prove the theorem 1.14 we first need to prove the following observation, which describes the fundamental relation between the inverse matrix of the permutation matrix and transposed permutation matrix.

**Observation 1.13.** *For any $P_\sigma \in \mathcal{P}(n)$ holds that $(P_\sigma)^{-1} = (P_\sigma)^T$.*

*Důkaz.* $P_\sigma$ is invertible. From the definition we have

$$P_\sigma (P_\sigma)^T = \begin{pmatrix} e^n_{\sigma(1)} \\ e^n_{\sigma(2)} \\ \vdots \\ e^n_{\sigma(n)} \end{pmatrix} \cdot \left( (e^n_{\sigma(1)})^T \mid (e^n_{\sigma(2)})^T \mid \cdots \mid (e^n_{\sigma(n)})^T \right) = I_n$$

This yields that $(P_\sigma)^T$ is the right inverse of $P_\sigma$. □

The following theorem characterizes the relationship between the s-XOR-count of matrix and its inverse.

**Theorem 1.14.** *Let $M$ be an invertible matrix over $\mathbb{F}_2$ with $wt_s(M) = t$ and let us assume that*

$$M = P_\sigma \prod_{k=1}^{t} A_{i_k,j_k}$$

*where $P_\sigma \in \mathcal{P}(n)$ is in a cycle normal form. Then $wt_s(M^{-1}) = t$. Moreover,*

$$M^{-1} \approx P_\sigma \prod_{k=t}^{1} A_{\tau^{-1}(i_k),\tau^{-1}(j_k)} \tag{1.1}$$

*for some permutation $\tau \in S_n$ that depends only on $P_\sigma$.*

*Důkaz.* This proof has two parts. In the first one, we prove $wt_s(M^{-1}) = t$ indeed holds and in the second we prove equation 1.1.

For the inverse of $M$ we have

$$\begin{aligned} M^{-1} &= A_{i_t,j_t} \cdot A_{i_{t-1},j_{t-1}} \cdot \cdots \cdot A_{i_1,j_1} \cdot P_{\sigma^{-1}} \\ &\approx P_{\sigma^{-1}} \cdot A_{i_t,j_t} \cdot \cdots \cdot A_{i_1,j_1} \end{aligned}$$

which together with the assumption that $wt_s(M) = t$ and lemma 1.8 yields that $wt_s(M^{-1}) \leq wt_s(M)$. We prove that $wt_s(M) \leq wt_s(M^{-1})$, by using the proven fact on $\widehat{M} := M^{-1}$. This yields that $wt_s(M) = wt_s(\widehat{M}^{-1}) \leq wt_s(\widehat{M}) = wt_s(M^{-1})$. Together we get that $wt_s(M) = wt_s(M^{-1}) = t$.

Let us consider that $P_\sigma = \bigoplus_{k=1}^{d} C_{x^{m_k}+1}$. Notice that for the inverse of the matrix $P_\sigma$ we have $(P_\sigma)^{-1} \overset{1.13}{=} (P_\sigma)^T = \bigoplus_{k=1}^{d} C^T_{x^{m_k}+1}$ (transposing block diagonal matrix results in the transposition of all blocks).

Let us consider a matrix $P_{\rho_r}$ of order $n$ with ones on the positions $(i, r-i+1)$, zero otherwise (i.e. a counterdiagonal matrix of order $r$). We get that $P_{\rho_r} \in \mathcal{P}(r)$. We can conclude that

$$\rho_r = \begin{cases} (1 \quad r)(2 \quad r-1)\ldots(\frac{r}{2} \quad \frac{r}{2}+1), & \text{for } r \text{ even.} \\ (1 \quad r)(2 \quad r-1)\ldots(\lfloor\frac{r}{2}\rfloor \quad \lceil\frac{r}{2}\rceil), & \text{for } r \text{ odd.} \end{cases} \tag{1.2}$$

Let $P_\tau = \bigoplus_{k=1}^{d} P_{\rho_{m_k}} \in \mathcal{P}(n)$, where $\tau \in S_n$ and $\tau$ depends only on $P_\sigma$. Notice that matrices $P_\tau$ and $P_\sigma$ have blocks of the same size and in the same order. Another thing to notice is that rows of any matrix of order $r$ multiplied by $P_{\rho_r}$ from the left side are in the reverse order and columns of any matrix of order $j$ multiplied by $P_{\rho_r}$ from the right side are also in the reverse order.

$$\begin{aligned} P_\tau(P_\sigma)^{-1}(P_\tau)^{-1} = P_\tau(P_\sigma)^{-1}P_{\tau^{-1}} &= \bigoplus_{k=1}^{d} P_{\rho_{m_k}} \bigoplus_{k=1}^{d} (C_{x^{m_k}+1})^T (\bigoplus_{k=1}^{d} P_{\rho_{m_k}})^{-1} \\ &= \bigoplus_{k=1}^{d} P_{\rho_{m_k}} \bigoplus_{k=1}^{d} (C_{x^{m_k}+1})^T \bigoplus_{k=1}^{d} P^T_{\rho_{m_k}} \\ &= \bigoplus_{k=1}^{d} P_{\rho_{m_k}} \bigoplus_{k=1}^{d} (C_{x^{m_k}+1})^T \bigoplus_{k=1}^{d} P_{\rho_{m_k}} \\ &= \bigoplus_{k=1}^{d} P_{\rho_{m_k}} (C_{x^{m_k}+1})^T P_{\rho_{m_k}} \\ &= \bigoplus_{k=1}^{d} C_{x^{m_k}+1} = P_\sigma \end{aligned}$$

and together we get

$$\begin{aligned} M^{-1} &\approx P_{\sigma^{-1}} \prod_{k=t}^{1} A_{i_k,j_k} \\ &\approx P_\tau P_{\sigma^{-1}} \prod_{k=t}^{1} A_{i_k,j_k} P_{\tau^{-1}} \\ &= P_{\tau^{-1} \circ \sigma^{-1} \circ \tau} \prod_{k=t}^{1} A_{\tau^{-1}(i_k),\tau^{-1}(j_k)} \\ &= P_\sigma \prod_{k=t}^{1} A_{\tau^{-1}(i_k),\tau^{-1}(j_k)}. \end{aligned}$$

□

The following theorem shows the relationship of the s-XOR-count of the product of matrices and the s-XOR-counts of those particular matrices.

**Theorem 1.15.** *Let $M, N \in GL(n, \mathbb{F}_2)$ be invertible matrices with $wt_s(M) = t_M$ and $wt_s(N) = t_N$. Then $wt_s(M \cdot N) \leq t_M + t_N$. Moreover, $wt_s(M^k) \leq |k| t_M$ for all $k \in \mathbb{Z}$, if $M$ is in a cycle normal form.*

*Důkaz.* Suppose that $M = P_\sigma \prod_{k=1}^{t_M} A_{i_k,j_k}$ and $N = Q_\rho \prod_{l=1}^{t_N} B_{i_l,j_l}$. Then

$$MN \overset{1.6}{=} P_\sigma Q_\rho \prod_{k=1}^{t_M} A_{\rho(i_k),\rho(j_k)} \prod_{l=1}^{t_N} B_{i_l,j_l},$$

where $A_{i_k,j_k}, B_{i_l,j_l}$ are addition matrices. And thus $wt_s(MN) \leq t_M + t_N$. From here it is clear that even the statement $wt_s(M^k) \leq |k| t_M$ for $k \in \mathbb{Z}, k \geq 1$ holds.

Let $k < 0$. We use Theorem 1.14. More precisely, the fact that the s-XOR-counts of a matrix and its inverse are equal. We know that $wt_s(M^{-1}) = t_M$. Let us denote $l := -k,\ M^{-1} = A$. Then

$$wt_s(M^k) = wt_s((M^{-1})^l) = wt_s(A^l),\ l > 0,\ wt_s(A) = wt_s(M^{-1}) = t_M.$$

By applying the proved statement we get that $wt_s(A^l) \leq |l| t_M$. Thus

$$wt_s(M^k) = wt_s(A^l) \leq |l| t_M = |-k| t_M = |k| t_M.$$

For $k = 0$ we get $wt_s(M^0) = wt_s(I) = 0 \leq |k| t_M$. □

# 2. Relation of XOR-counts

In this chapter, we investigate the relation of XOR-counts. Specifically, we explore matrices which have the d-XOR-count lower than the s-XOR-count. We present an inductive construction of such matrices and prove correctness. We then prove that such a matrix of order $n$ exists if and only if $n \geq 6$.

**Definition 2.1.** The *Hamming weight* of a vector $v \in \mathbb{F}_2$ is the number of non-zero values in $v$. We denote it by $wt(v)$.

**Definition 2.2.** A *unit vector* is a vector with the Hamming weight equal to 1.

**Definition 2.3.** By *zero vector* we mean a vector $u$ that has only zeros in it, i.e. $wt(u) = 0$. Moreover, we shall denote the $i$-th row vector of the matrix $M$ by $M_i$ and the $i$-th entry of the vector $v$ by $v_i$. By $M_{i,j}$ we denote the entry in the row $i$ and columns $j$.

Let us first prove the following lemma about the Hamming weight of the sum of two vectors. We'll use this lemma in the proof of Observation 2.5.

**Lemma 2.4.** *For vectors $u, v$ of arbitrary length holds*

$$wt(u + v) = wt(u) + wt(v) - 2wt(u \cdot v).$$

*Hence if $u$ and $v$ have even weights, their sum has even weight too.*

*Důkaz.* Let us denote the set of indices of '1's in the vector $u$ by $I_u$ and the set of indices of '1's in the vector $v$ by $I_v$. We prove the statement by noticing that $wt(u+v)$ in fact denotes the cardinality of the symmetric difference of $I_u$ and $I_v$. The cardinality of this set equals to $|I_u| + |I_v| - 2 \cdot |I_u \cap I_v| = wt(u) + wt(v) - 2wt(u \cdot v)$. □

In the following propositions, we present matrices such that the sequential XOR-count is higher than the direct XOR-count. We start by introducing a matrix of order 6 and proving that the statemant holds. Later we generalize our construction for any order $n \geq 6$. Let

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(6, \mathbb{F}_2).$$

But first, we need to prove the following observation about a property of matrix $M$ that will help us prove that $wt_d(M) < wt_s(M)$.

**Observation 2.5.** *Matrix $M$ is invertible and is constructed in a way that the sum of any two or three rows doesn't add up to a unit vector. In other words, we have to perform at least three row additions to get a unit vector in a row of the matrix $M$.*

*Důkaz.* First, let us prove that $M$ is invertible. Let us switch the the first and the second row. Now, let's add the first, the second, and the third row to the sixth row and we get a matrix in a row echelon form, where all rows have at least one non-zero element and said matrix is in the upper triangular form. Thus our matrix has full rank and thus is invertible.

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Let us now prove that the sum of any two vectors isn't equal to a unit vector. Let us denote those two vectors by $i, k$ for brevity and begin by considering $i, k \in \{M_j | 1 \leq j \leq 5\}$. From Lemma 2.4 we have that their sum has even Hamming weight and therefore is not a unit vector. To get a unit vector from the sum of sixth vector and $i$, we would need $i$ to have ones in the same two columns as $l$ does. But we see that no choice of $i$ satisfies this condition. Therefore, the sum of any two rows of the matrix $M$ isn't equal to a unit vector.

Let us now prove that the sum of any three rows of $M$ isn't equal to a unit vector. From Lemma 2.4 we see that adding three vectors from rows $M_1, \ldots, M_5$ (which have even weights) doesn't give us a unit vector.

Let's consider adding $i, k \in \{M_1, \ldots, M_5\}$ to the row $M_6$. We can see that to get rid of the first entry of $M_6$ we must add $M_2$. To get rid of the third entry of $M_6$ we must add $M_3$ to it. To get rid of the sixth entry of $M_6$ we must add $M_5$ to it. Thus to get rid of two entries of $M_6$ simultaneously we must add two of those rows to $M_6$. So the only options of our interest are $M_2 + M_3 + M_6$, $M_2 + M_5 + M_6$, $M_3 + M_5 + M_6$. But each one of these options is of weight 3. Again, we see that no such rows $i, k$ exist in $M$. And thus, the sum of no three vectors from $M$ equals to a unit vector. In other words, two row additions can't give us a unit vector. □

The following idea was proposed for $n \geq 7$ [Köl19], my contribution is that this idea holds for all $n \geq 6$ and later we show that $\forall n < 6$ there is no matrix with the d-XOR-count lower than the s-XOR-count.

**Theorem 2.6.** *For every $n$ such that $n \geq 6$, exists an invertible matrix $M$ of order $n$ such that $wt_d(M) < wt_s(M)$.*

*Důkaz.* We start by proving that the statement holds for $n = 6$, then we'll generalize this statement for every $n > 6$.
Let us consider the matrix $M$ from Observation 2.5.

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(6, \mathbb{F}_2)$$

We have $wt_d(M) = 7$, since the number of ones in $M$ is equal to 13 and $n = 6$. Suppose that $wt_s(M) = t$, then a sequence of matrices $A_{i_k,j_k} \in \mathcal{A}$ and a permutation matrix $P_\sigma \in \mathcal{P}(n)$ exist such that $\prod_{k=1}^{t} A_{i_k,j_k} \cdot M = P_\sigma$.
According to Observation 2.5, $M$ is constructed in such a way that we need to perform at least three row additions to get a unit vector in $M$. Each of the remaining rows needs at least one row addition operation to become a unit vector. That yields that the lower bound for $wt_s(M) \geq 3 + 5 \cdot 1 = 8$. Hence $wt_d(M) < wt_s(M)$ and the statement holds for $n = 6$.

We construct a matrix of order $n > 6$ with the d-XOR-count lower than the s-XOR-count by having a block diagonal matrix with two blocks, where the first block is equal to $M$ and the second is equal to the identity matrix of order $(n-6)$. Let us denote this matrix by $M'$.

$$M' = \begin{pmatrix} M & \\ & Id_{n-6} \end{pmatrix} \in GL(n, \mathbb{F}_2)$$

We see that $wt_d(M') = wt_d(M) < wt_s(M) = wt_s(M')$. □

Now a new question arises. Is there such a matrix of order $n > 6$ that values of the d-XOR-count and the s-XOR-count differ from $wt_d(M)$ and $wt_s(M)$? Let us consider the matrix of order $n = 7$ denoted by $A$. Let

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \in GL(7, \mathbb{F}_2)$$

The matrix $A$ was derived from $M$ by adding the third row and extending all the other rows accordingly (we add the second column, see the generalization and inductive algorithm below). Similarly to $M$, $A$ has the property that the sum of any three row vectors isn't a unit vector. The proof of this fact is conducted similarly to the proof of Observation 2.5.

We notice that all rows but the last one have even Hamming weight and therefore we must use the last row to get a unit vector. We see that to get rid of some non-zero entry of $A_7$, we must add either $A_2$ or $A_4$ or $A_6$ to $A_7$. This means that only options are $A_2 + A_4 + A_7$, $A_2 + A_6 + A_7$ and $A_4 + A_6 + A_7$. But each option gives us a row with $wt(\cdot) = 3$.

Therefore we need to add together at least 4 rows to get a unit vector. Each remaining vector then needs to be updated at least once. And thus $wt_s(A) \geq 3 + 6 \cdot 1 = 9$ and $wt_d(A) = 8$. So $wt_d(A) < wt_s(A)$.

As mentioned before, matrices $M$ and $A$ can be extended accordingly even for $n > 7$. Let us denote matrix of order $n$ that is extended from $M$ by $M^n$ (this means $M^6 = M$ and $M^7 = A$). We construct $M^n$ from $M^{n-1}$. We do this by

- adding zero at the beginning of the $M_1^{n-1}$ and placing it as the first row
- adding zero at the end of $M_2^{n-1}, \ldots, M_{n-5}^{n-1}$ and placing those as rows $2, \ldots, n-5$, respectively

- adding new row vector with ones on positions $n-5, n-4$ as $n-4$-th row
- adding zero at the beginning of rows $M_{n-4}^{n-1}, M_{n-3}^{n-1}, M_{n-2}^{n-1}$ and placing those as rows $M_{n-3}^{n}, M_{n-2}^{n}, M_{n-1}^{n}$
- adding new row with ones on position $1, n-3, n$

Notice that when $n$ increases by 1, the s-XOR-count and the d-XOR-count also increase by 1, so their inequality holds. And thus we get that for any $n > 6$ we are able to construct a matrix so that $wt_s(A) = wt_d(A) + 1$. See below for a visual example of a matrix with such a property

$$A' = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

In the following theorem, we prove that matrices with the d-XOR-count lower than the s-XOR-count of order 5 or less do not exist. We conduct the proof by going over the cases $2 \leq n \leq 5$ and showing that all invertible matrices of order $n$ have the sequential XOR-count lower or equal to the direct XOR-count.

**Theorem 2.7.** *For every $n < 6$ and $A \in GL(n, \mathbb{F}_2)$ holds $wt_s(A) \leq wt_d(A)$.*

*Důkaz.* **Let $n = 2$.** Let us assume $wt_d(A) \geq 1$ (matrices with $wt_d(A) \leq 0$ are either singular or permutation matrices). Also let us assume that $wt_d(A) \leq 1$, because $wt_d(A) = 2$ yields that the $A$ is singular. This gives us that the only four possibilities are

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

For all such matrices holds that $wt_s(A) = wt_d(A) = 1$.

**Let $n = 3$.** Firstly, we will show that if $A$ has a row with the Hamming weight equal to 1 or 3, then $wt_s(A) \leq wt_d(A)$. This will give us that the only option left is that all rows of $A$ have the weight of 2, which is also not suitable.

Let us without loss of generality assume that $A_{1,1} = 1$ and $wt(A_1) = 1$. In case $A_{2,1} \neq 0$, we add $A_1$ to $A_2$. The same goes for $A_3$. By $k \in \{0, 1, 2\}$ we denote the number of those additions. We get a block diagonal matrix with the second block of order 2. Each addition of $A_1$ changed one non-zero entry to 0. From the case for $n = 2$ we get $1 + k = wt_s(A) \leq wt_d(A) = 1 + k$, where $k$ depends on how many times we added $A_1$ to $A_2, A_3$.

$$\begin{pmatrix} 1 & 0 & 0 \\ ? & ? & ? \\ ? & ? & ? \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & ? & ? \\ 0 & ? & ? \end{pmatrix}$$

Let $A$ consist of a row with the Hamming weight equal to 3. Let us without loss of generality assume that $wt(A_1) = 3,\ wt(A_2) = 2,\ wt(A_3) = 2$ and $A_{2,2} = 1,\ A_{2,3} = 1$. Then by adding $A_2$ to $A_1$ and $A_1$ to $A_3$ we get block diagonal matrix with $wt_s(A) = 2 + l \leq 4 = wt_d(A)$, where $l$ depends on whether we added $A_1$ to $A_3$.

$$\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ ? & ? & ? \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ ? & ? & ? \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & ? & ? \end{pmatrix}$$

This yields $wt(A_i) = 2,\ i = 1, 2, 3$. But in this case, every possible matrix is singular. Let us denote values of $wt_d(A),\ wt_s(A)$ as $wt_{d3},\ wt_{s3}$ for further purposes.

**Let $n = 4$.** Let rows of $A$ each have the Hamming weight of at least 2. Otherwise $A$ would be permutation similar to some block diagonal matrix with the first block of order 1 and the second block of order 3, which yields that $wt_s(A) \leq wt_d(A)$ from discussion of the case $n = 3$.

Moreover, there must exist $i \in \{1, 2, 3, 4, 5\}$ such that $wt(A_i) \geq 3$, otherwise $A$ is singular. We will first compute, how many vectors can we get by adding all possible combinations of at most three rows together.

$$|\{\sum_{k \in K} A_k,\ K \subseteq \{1, \ldots, 4\}\}| = \binom{4}{1} + \binom{4}{2} + \binom{4}{3} = 2^4 - 2.$$

This means that we can get a unit vector by performing two additions. Furthermore, to get such a unit vector, one of the terms of the sum must be a vector with the Hamming weight 3, because the sum of vectors with even Hamming weight can't have odd Hamming weight (see 2.4). Let us for the simplicity assume that the unit vector we get is without loss of generality $A'_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$ (where by $A'$ we denote newly derived matrix). If $A'_{2,1} \neq 0$, then we add $A'_1$ to $A'_2$. The same goes for $A'_{3,1}$ and $A'_{4,1}$. By $l$ we denote how many additions of this type we performed. At this point, we have a block diagonal matrix with the first block of order 1 and the second one of order 3.

$$\begin{pmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \overset{\text{2 additions}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{pmatrix} \overset{l \text{ additions}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & ? & ? & ? \\ 0 & ? & ? & ? \\ 0 & ? & ? & ? \end{pmatrix}$$

We get that $wt_s(A) \leq 2 + l + wt_{s3} \leq 2 + l + wt_{d3} \leq wt_d(A)$. Let us denote $wt_d(A) = wt_{d4}$ and $wt_s(A) = wt_{s4}$ for further purposes.

**Let $n = 5$.** By summing at most three distinct rows together we get

$$|\{\sum_{k \in K} A_k,\ K \subseteq \{1, \ldots, 5\}\}| = \binom{5}{1} + \binom{5}{2} + \binom{5}{3} = 25 = 2^5 - 7$$

different vectors. At the same time, we have $2^5 - 1$ different vectors in total (excluding zero vector). Thus matrix $A$ might be constructed in a way that the only the sum of four or five rows produces a unit vector. First, we will show that

such a matrix doesn't have the property that the d-XOR-count is lower than the s-XOR-count.

Let us denote such a matrix by $B$ in this part of the proof. We see that we get six distinct vectors by adding either four or five rows of $B$ together. They are distinct because $A$ is invertible. Five of them are unit vectors and one of them is some arbitrary (non-zero, non-unit) vector, which we shall denote by $v$ in this proof. Notice that $\binom{5}{1} + \binom{5}{2} + \binom{5}{3} + \binom{5}{4} = 2^5 - 2$, which means that by adding five rows together we get either a unit vector or $v$.

- First, consider the possibility that by adding all five rows we get $v$ (in other words, we get all five unit vectors by adding different quartets of rows). Without loss of generality, we may assume that by adding all rows but the first one, we get the unit vector $\begin{pmatrix}1 & 0 & 0 & 0 & 0\end{pmatrix}$ (we shall denote this equality by $\varepsilon_1$), by adding all rows but the second one, we get the unit vector $\begin{pmatrix}0 & 1 & 0 & 0 & 0\end{pmatrix}$ (we shall denote this equality by $\varepsilon_2$) — in general, adding all rows but the $k$-th one will result in the unit vector with the $k$-th value being non-zero (and we shall denote this equality by $\varepsilon_k$) for $1 \leq k \leq 5$.
  This yields matrix equality

  $$(J_5 - I_5) \cdot B = I_5,$$

  where $J_5$ is a matrix of order 5 with all entries equal to one and $I_5$ is the identity matrix of order 5. Matrix $J_5 - I_5$ is singular because the Hamming weight of each column is equal to 4 and by adding all rows together we get a zero vector. Thus even the matrix $(J_5 - I_5) \cdot B$ is singular. On the other side of equality, we have the invertible matrix $I_5$. This gives us a contradiction.

- Next, we will consider the possibility that by adding all five rows we'll get a unit vector $\begin{pmatrix}0 & 0 & 0 & 0 & 1\end{pmatrix}$ (let us denote this equation by $\varepsilon_5$). And similarly to the previous part, adding all rows but the $k$-th one will result in a unit vector with the $k$-th value being non-zero (we denote this equality by $\varepsilon_k$) for $1 \leq k \leq 4$. Adding all vectors but the fifth one gives us $v$.

  $$\begin{aligned}
  \varepsilon_1 &: B_2 + B_3 + B_4 + B_5 = \begin{pmatrix}1 & 0 & 0 & 0 & 0\end{pmatrix} \\
  \varepsilon_2 &: B_1 + B_3 + B_4 + B_5 = \begin{pmatrix}0 & 1 & 0 & 0 & 0\end{pmatrix} \\
  \varepsilon_3 &: B_1 + B_2 + B_4 + B_5 = \begin{pmatrix}0 & 0 & 1 & 0 & 0\end{pmatrix} \\
  \varepsilon_4 &: B_1 + B_2 + B_3 + B_5 = \begin{pmatrix}0 & 0 & 0 & 1 & 0\end{pmatrix} \\
  \varepsilon_5 &: B_1 + B_2 + B_3 + B_4 + B_5 = \begin{pmatrix}0 & 0 & 0 & 0 & 1\end{pmatrix} \\
  \varepsilon_6 &: B_1 + B_2 + B_3 + B_4 = v
  \end{aligned}$$

  These equations give us explicit form of $B$.

  $$\begin{aligned}
  \varepsilon_1 + \varepsilon_5 &: B_1 = \begin{pmatrix}1 & 0 & 0 & 0 & 1\end{pmatrix} \\
  \varepsilon_2 + \varepsilon_5 &: B_2 = \begin{pmatrix}0 & 1 & 0 & 0 & 1\end{pmatrix} \\
  \varepsilon_3 + \varepsilon_5 &: B_3 = \begin{pmatrix}0 & 0 & 1 & 0 & 1\end{pmatrix} \\
  \varepsilon_4 + \varepsilon_5 &: B_4 = \begin{pmatrix}0 & 0 & 0 & 1 & 1\end{pmatrix}
  \end{aligned}$$

And from that, we derive

$$v = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 \end{pmatrix},$$
$$\varepsilon_5 + \varepsilon_6 : B_5 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

And thus

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix} \overset{\text{4 additions}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \overset{\text{4 additions}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

From this, we get that $wt_s(B) = 8 = wt_d(B)$.

Now we know that we get at least one unit vector by performing at most two row addition operations. We continue similarly to the case for $n = 4$. If $A$ contains a unit vector, then $wt_s(A) \leq wt_d(A)$ from the case $n = 4$. Thus every row of $A$ has the Hamming weight of at least 2. If $A$ contains only rows with the Hamming weight equal to 2, then $A$ is singular. Therefore at least one row has the Hamming weight greater or equal to 3. This row must be one of the terms of the sum that gives us a unit vector. Without loss of generality, we assume this row is $A_1$. We again proceed as in $n = 4$. We first add some rows to $A_1$ to get $\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \end{pmatrix}$. If $A_{2,1} \neq 0$, we add $A_1$ to $A_2$. Same goes for $A_{3,1}, A_{4,1}, A_{5,1}$. By $l \in \{0, 1, 2, 3, 4\}$ we denote how many additions of this type we performed. We get a block diagonal matrix with the first block of order 1 and the second one of order 4.

$$\begin{pmatrix} ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \end{pmatrix} \overset{\leq 2 \text{ additions}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \\ ? & ? & ? & ? & ? \end{pmatrix} \overset{l \text{ additions}}{\sim} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & ? & ? & ? & ? \\ 0 & ? & ? & ? & ? \\ 0 & ? & ? & ? & ? \\ 0 & ? & ? & ? & ? \end{pmatrix}$$

We get that $wt_d(A) = wt_{d4} + 2 + l$ and $wt_s(A) = wt_{s4} + 2 + l$. Therefore $wt_s(A) \leq wt_d(A)$. □

This last corollary summarizes the relationship of the direct XOR-count and the sequential XOR-count, which we proved in theorem 2.6 and in theorem 2.7.

**Corollary 2.8.** *Invertible matrix $A$ of order $n$ with $wt_d(A) < wt_s(A)$ exists if and only if $n \geq 6$.*

*Důkaz.* In theorem 2.6 we showed that $\forall n \geq 6$ exists a matrix of order $n$ with the d-XOR-count lower than the s-XOR-count. In theorem 2.7 we showed that $\forall n \leq 5$ invertible matrices of order $n$ have the s-XOR-count lower than the d-XOR-count. □

# Conclusion

In the final corollary 2.8, we showed the characterization of the existence of matrices with direct XOR-count lower than sequential XOR-count based on the order of the matrix. Another problem that could be further researched is the *complete description* of the case when direct XOR-count is lower than the sequential XOR-count.

This characterization could lead to an inductive construction of matrices with the maximal difference of d-XOR-count and s-XOR-count. From this, we could derive the exact number of matrices of some order $n$ with d-XOR-count lower than s-XOR-count.

# Bibliography

[BKL16] Christof Beierle, Thorsten Kranz, and Gregor Leander. Lightweight multiplication in GF($2^n$) with applications to MDS matrices. In *Annual International Cryptology Conference*, pages 625–653. Springer, 2016.

[Köl19] Lukas Kölsch. XOR-counts and lightweight multiplication with fixed elements in binary finite fields. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 285–312. Springer, 2019.