An Algorithm for finding the Branch Numbers of Invertible Boolean Matrices

---

Vladislav Fedchenko
(Belarusian State University, Minsk)

June 4–7, 2019 CTCrypt'2019 Rump–Session

Well Known Definitions

$V_{mk} = \mathrm{GF}(2)^{mk}$ — row-vectors, V^*_{mk} — column-vectors, $m, k \in \mathbb{N}$

$[x] \in \{0,1,\ldots,k\}$ — count of nonzero m-vectors in $x \in V^{(*)}_{mk}$, weight

$M \in \mathrm{GL}(mk, 2)$ — linear transform, invertible $(mk \times mk)$-matrix

$$\mathfrak{B}_L(M) = \min_{L'' \in V^*_{mk} \setminus \{0\}} \big([M \cdot L''] + [L'']\big)$$ — linear branch number

$$\mathfrak{B}_D(M) = \min_{D' \in V_{mk} \setminus \{0\}} \big([D'] + [D' \cdot M]\big)$$ — differential branch number

Well Known Definitions

$V_{mk} = \mathrm{GF}(2)^{mk}$ — row-vectors, V^*_{mk} — column-vectors, $m, k \in \mathbb{N}$

$[x] \in \{0,1,\ldots,k\}$ — count of nonzero m-vectors in $x \in V^{(*)}_{mk}$, weight

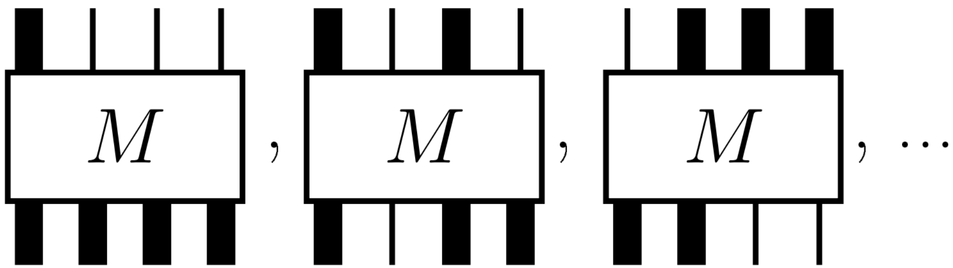
$M \in \mathrm{GL}(mk, 2)$ — linear transform, invertible $(mk \times mk)$-matrix

$$\mathfrak{B}_L(M) = \min_{L'' \in V^*_{mk} \setminus \{0\}} \big([M \cdot L''] + [L'']\big)$$ — linear branch number

$$\mathfrak{B}_D(M) = \min_{D' \in V_{mk} \setminus \{0\}} \big([D'] + [D' \cdot M]\big)$$ — differential branch number

Lin. (L', L'') and diff. (D', D'') relations, truncated representation:

D' $\qquad$ $L' = M \cdot L''$



$D'' = D' \cdot M$ $\qquad$ L''

Motivation

1. Criteria of **maximality** ($\mathfrak{B}_{(\cdot)}(\cdot) = k+1$, e.g. MDS) is known.

Motivation

1. Criteria of **maximality** ($\mathfrak{B}_{(\cdot)}(\cdot) = k+1$, e.g. MDS) is known.
2. How to evaluate the branch numbers for non-MDS matrices?

Motivation

1. Criteria of **maximality** ($\mathfrak{B}_{(\cdot)}(\cdot) = k+1$, e.g. MDS) is known.
2. How to evaluate the branch numbers for non-MDS matrices?
3. The question is **practical** (`Crypton`, `Midori` etc.).

Motivation

1. Criteria of **maximality** ($\mathfrak{B}_{(\cdot)}(\cdot) = k+1$, e.g. MDS) is known.
2. How to evaluate the branch numbers for non-MDS matrices?
3. The question is **practical** (`Crypton`, `Midori` etc.).
4. It seems nothing was published.

Notation

$$L'' = \begin{pmatrix} l_1 \\ \vdots \\ l_k \end{pmatrix} \in V_{mk}^* \qquad L' = \begin{pmatrix} l_{k+1} \\ \vdots \\ l_{2k} \end{pmatrix} \in V_{mk}^* \qquad l_j \in V_m^*$$

$$D' = (d_1, \ldots, d_k) \in V_{mk} \quad D'' = (d_{k+1}, \ldots, d_{2k}) \in V_{mk} \quad d_j \in V_m$$

Notation

$$L'' = \begin{pmatrix} l_1 \\ \vdots \\ l_k \end{pmatrix} \in V_{mk}^* \qquad L' = \begin{pmatrix} l_{k+1} \\ \vdots \\ l_{2k} \end{pmatrix} \in V_{mk}^* \qquad l_j \in V_m^*$$

$$D' = (d_1, \ldots, d_k) \in V_{mk} \quad D'' = (d_{k+1}, \ldots, d_{2k}) \in V_{mk} \quad d_j \in V_m$$

O_m — zero matrix, $m \times m$
E_m — identity matrix, $m \times m$

$$T_i := (\overset{1}{O_m}, \ldots, \overset{i-1}{O_m}, \overset{i}{E_m}, \overset{i+1}{O_m}, \ldots, \overset{2k}{O_m})$$

Notation

$$L'' = \begin{pmatrix} l_1 \\ \vdots \\ l_k \end{pmatrix} \in V_{mk}^* \qquad L' = \begin{pmatrix} l_{k+1} \\ \vdots \\ l_{2k} \end{pmatrix} \in V_{mk}^* \qquad l_j \in V_m^*$$

$$D' = (d_1, \ldots, d_k) \in V_{mk} \quad D'' = (d_{k+1}, \ldots, d_{2k}) \in V_{mk} \quad d_j \in V_m$$

O_m — zero matrix, $m \times m$

E_m — identity matrix, $m \times m$

$$T_i := (\overset{1}{O_m}, \ldots, \overset{i-1}{O_m}, \overset{i}{E_m}, \overset{i+1}{O_m}, \ldots, \overset{2k}{O_m})$$

$$W^M_{j_1, j_2, \ldots, j_t} := \begin{pmatrix} M, E_{mk} \\ T_{i_1} \\ T_{i_2} \\ \vdots \\ T_{i_{2k-t}} \end{pmatrix}$$

where $\{i_1, i_2 \ldots, i_{2k-t}\} = \{1, 2, \ldots, 2k\} \setminus \{j_1, j_2, \ldots, j_t\}$

Main Observation

Theorem. Nontrivial linear relation (L', L'') has no more than $t \in \mathbb{N}$, $2 \leqslant t \leqslant k+1$, nonzero m-vectors $l_j \in V_m^* \setminus \{0\}$, with indices $j \in \{j_1, j_2, \ldots, j_t\}$, $1 \leqslant j_1 < j_2 < \ldots < j_t \leqslant 2k$, iff rank $W^M_{j_1, j_2, \ldots, j_t} < 2mk$.

$$\mathfrak{B}_L(M) = \mathfrak{B}_D(M^\top)$$

Similarly for differential relations using $M^\top$ instead of M

Algorithm & Complexity

Input: $M \in \mathrm{GL}(mk, 2)$, $m, k \in \mathbb{N}$
Output: $\mathfrak{B}_L(M)$

for all $t = 2, 3, \ldots, k$
  for all $j_1, \ldots, j_t : 1 \leqslant j_1 < \ldots < j_t \leqslant 2k, j_1 < k+1, j_t > k$
    if $\operatorname{rank} W^M_{j_1, j_2, \ldots, j_t} < 2mk$ **than**
      return t
return $k + 1$

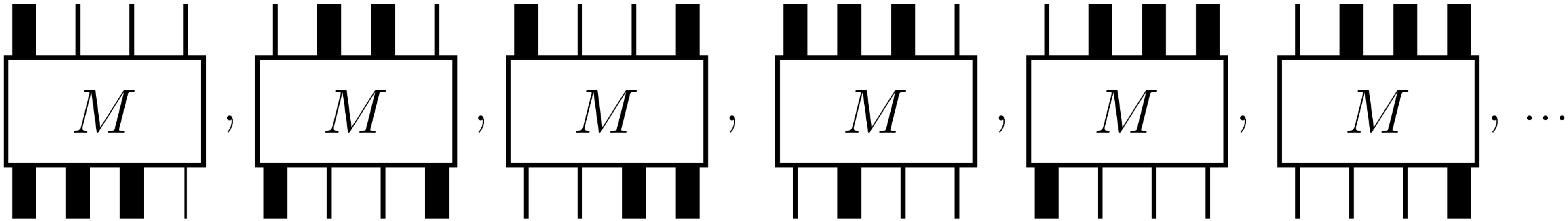
Similarly for differential branch number using $M^\top$ instead of M

$T_{\max} < (3mk)^2 \cdot 2^{2k}$ of $2mk$-bitwise XORs (extremely rough)

$m = 8$, $k = 16$, i.e. (128×128)-matrix: $<$ $\mathbf{2^{49}}$ (**feasible on PC**)

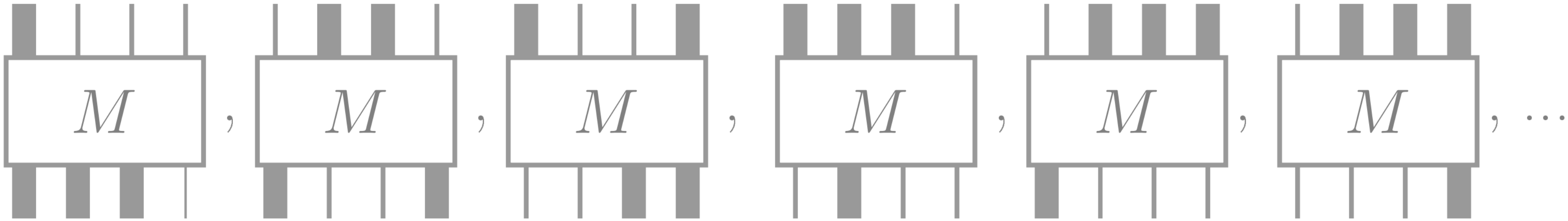
Extended Applications

Moreover, we can find all the **valid** minimal truncated relations

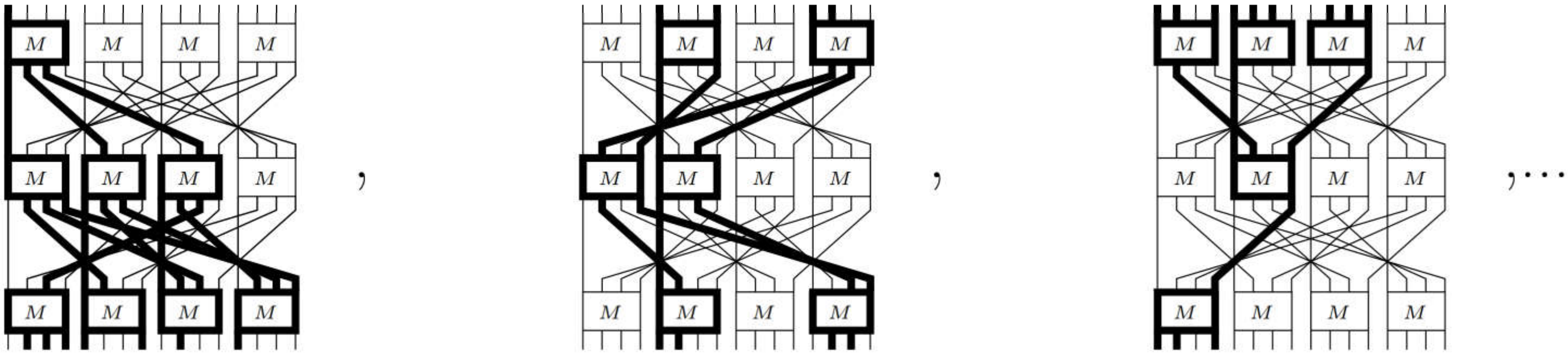


Extended Applications

Moreover, we can find all the **valid** minimal truncated relations



and use them while analyzing linear or differential **trails**:



Thank you for your attention!

An Algorithm for finding the Branch Numbers of Invertible Boolean Matrices

Vladislav Fedchenko
(Belarusian State University, Minsk)

June 4–7, 2019 CTCrypt'2019 Rump–Session