Word oriented LFSR and construction of block companion matrices in a given conjugacy class

Gilles LACHAUD

Institut de Mathématiques de Luminy
CNRS/AMU, Marseille

Crypto'Puces 2013
May 27-31, Porquerolles

Introduction

LFSR : linear feedback shift register

The aims :

- to offer a good tradeoff between security and efficiency.
- to move from 1-bit to 32-bit processors in the design of algorithms

A *block LFSR* (or σ *-LFSR*) is a word-oriented LFSR

(word oriented = vectorial)

Definition of of block LFSRs

$\mathbb{F}_q$ finite field ($q = 2$ if you wish); $\mathbf{M}_m(\mathbb{F}_q)$: matrices $m \times m$

$$C = (C_0, \ldots, C_{n-1}) \in \mathbf{M}_m(\mathbb{F}_q)^n$$

$$\mathbf{X}_0 = (X_0, X_1, \ldots, X_{n-1}) \in (\mathbb{F}_q^m)^n$$

(X_i) = sequence of $\mathbb{F}_q^m$ determined by the *block recurring sequence*

$$X_{n+i} = C_{n-1}.X_{i+n-1} + \cdots + C_1.X_{i+1} + C_0.X_i, \quad i = 0, 1, \ldots$$

This system is a *block LFSR* (think to a m-bit processor)
$\mathbf{X}_0$ = initial state of the LSFR;
$\mathbf{X}_k = (x_k, x_{k+1}, \ldots, x_{k+n-1})$ = kth state

Associate to such a block LFSR the

Block companion matrix:

$$\mathsf{C} = \begin{bmatrix} 0 & 0 & \dots & 0 & C_0 \\ \mathbf{I}_m & 0 & \dots & 0 & C_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & C_{n-2} \\ 0 & 0 & \dots & \mathbf{I}_m & C_{n-1} \end{bmatrix} \in \mathbf{M}_{mn}(\mathbb{F}_q)$$

Then $\mathbf{X}_{k+1} = \mathbf{X}_k.\mathsf{C}$ and C is the *state transition matrix* :

$$\mathbf{X}_k = \mathbf{X}_0.\mathsf{C}^k \quad (k \geq 0)$$

Notation: here any $\mathsf{A} \in \mathbf{M}_{mn}(\mathbb{F}_q)$ is divided in *blocks* $A_{ij} \in \mathbf{M}_m(\mathbb{F}_q)$:

$$\mathsf{A} = \begin{bmatrix} A_{11} & \dots & A_{1n} \\ \dots & \dots & \dots \\ A_{n1} & \dots & A_{nn} \end{bmatrix} \in \mathbf{M}_n(\mathbf{M}_m(\mathbb{F}_q))$$

Block LFSRs

Associate to a general block LSFR with companion matrix

$$\mathsf{C} = \begin{bmatrix} 0 & 0 & \dots & 0 & C_0 \\ \mathbf{I}_m & 0 & \dots & 0 & C_1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & C_{n-2} \\ 0 & 0 & \dots & \mathbf{I}_m & C_{n-1} \end{bmatrix} \in \mathbf{M}_{mn}(\mathbb{F}_q)$$

the *polynomial matrix*

$$P_C(\lambda) = \mathbf{I}_m \lambda^n - C_{n-1}\lambda^{n-1} - \cdots - C_0 \in \mathbf{M}_m(\mathbb{F}_q[\lambda])$$

Then the *characteristic polynomial* of C is

$$\chi_{\mathsf{C}}(\lambda) = \det P_C(\lambda).$$

Order and period

Order of an invertible matrix $\mathsf{C} \in \mathrm{GL}_n(\mathbb{F}_q)$:

$$\operatorname{ord} \mathsf{C} = \text{the smallest integer } N \geq 1 \text{ such that } \mathsf{C}^N = \mathbf{I}_n$$

The sequence of states $(\mathbf{X}_k)$ is *periodic* :

$$\mathsf{C}^N = \mathbf{I}_n \quad \Longrightarrow \quad \mathbf{X}_{N+i} = \mathbf{X}_N \quad \text{if} \quad i \geq 0$$

The period of the LFSR equals the order of C

Singer cycles

One wants the period to be as long as possible

$$A \in \mathrm{GL}_n(\mathbb{F}_q) \quad \Longrightarrow \quad \mathrm{ord}\, A \leq q^n - 1$$

Equivalent conditions:

1. $\mathrm{ord}\, A = q^n - 1$
2. $\chi_A(\lambda)$ is a primitive polynomial

Such an A is called a *Singer cycle*

[primitive pol. = minimal pol. of a generator of $\mathbb{F}_{q^n}^\times$]

Primitive block LFSRs

A block LSFR is *primitive* if its period is equal to $q^{mn} - 1$ for any choice of a nonzero initial state.

$$\iff \quad \operatorname{ord} \mathsf{C} = q^{mn} - 1 \quad \text{(Singer cycle)}$$

Theorem (Ghorpade & al.)

Equivalent conditions:

1. $\chi_{\mathsf{C}}(\lambda)$ is a primitive polynomial of degree mn
2. The block LSFR is primitive

ZENG Guang & al.
J. Electronics & Information Technology, 2009:

"Using a primitive block LFSR with $n = 4$ *over* $\mathbb{F}_{32}$ *in ABC software (avatar of Turing, SSC2, Sober, Snow) increases its period from* $2^{32}(2^{127} - 1)$ *to* $2^{32}(2^{128} - 1)$.

More important, this increases the Hamming weight of the characteristic polynomial of an equivalent LFSR over $\mathbb{F}_2$ *(of degree* 128*) from* 3 *to* 65.

Consequently, its resistance to fast correlation attack is consolidated, while the guaranteed efficiency in software is almost the same.

Speed can reach 25 *Gbits/sec on a* 3 *GHz CPU."*

The problem of construction

One wants to construct block primitive LFSRs
Let $\chi \in \mathbb{F}_q[\lambda]$ primitive, $\deg \chi = mn$, and define the *conjugacy class*

$$\mathscr{C} = \{A \in \mathrm{GL}_{mn}(\mathbb{F}_q) \mid \chi_A = \chi\}$$

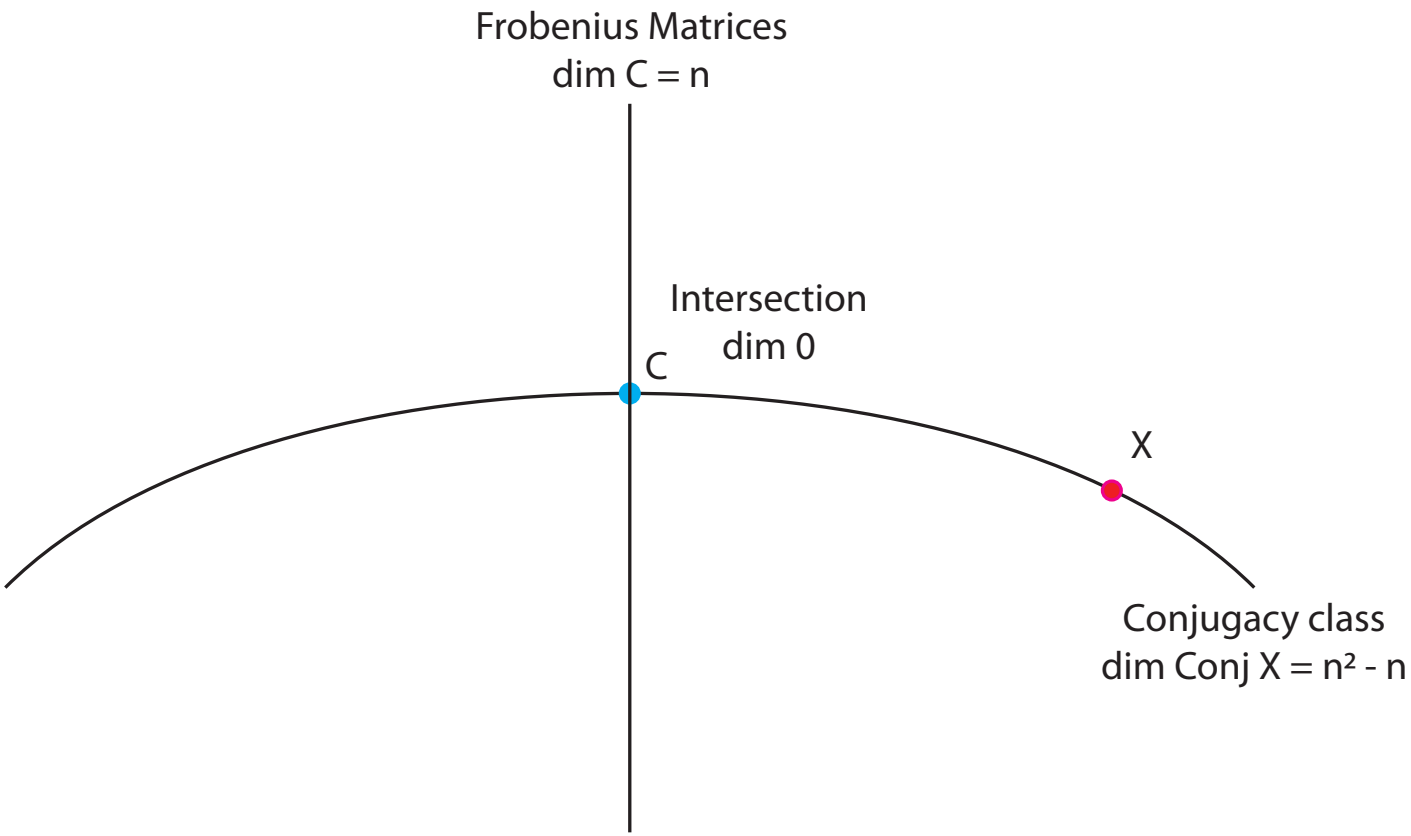
Problem

Find the block companion matrices in $\mathscr{C}$, that is, find

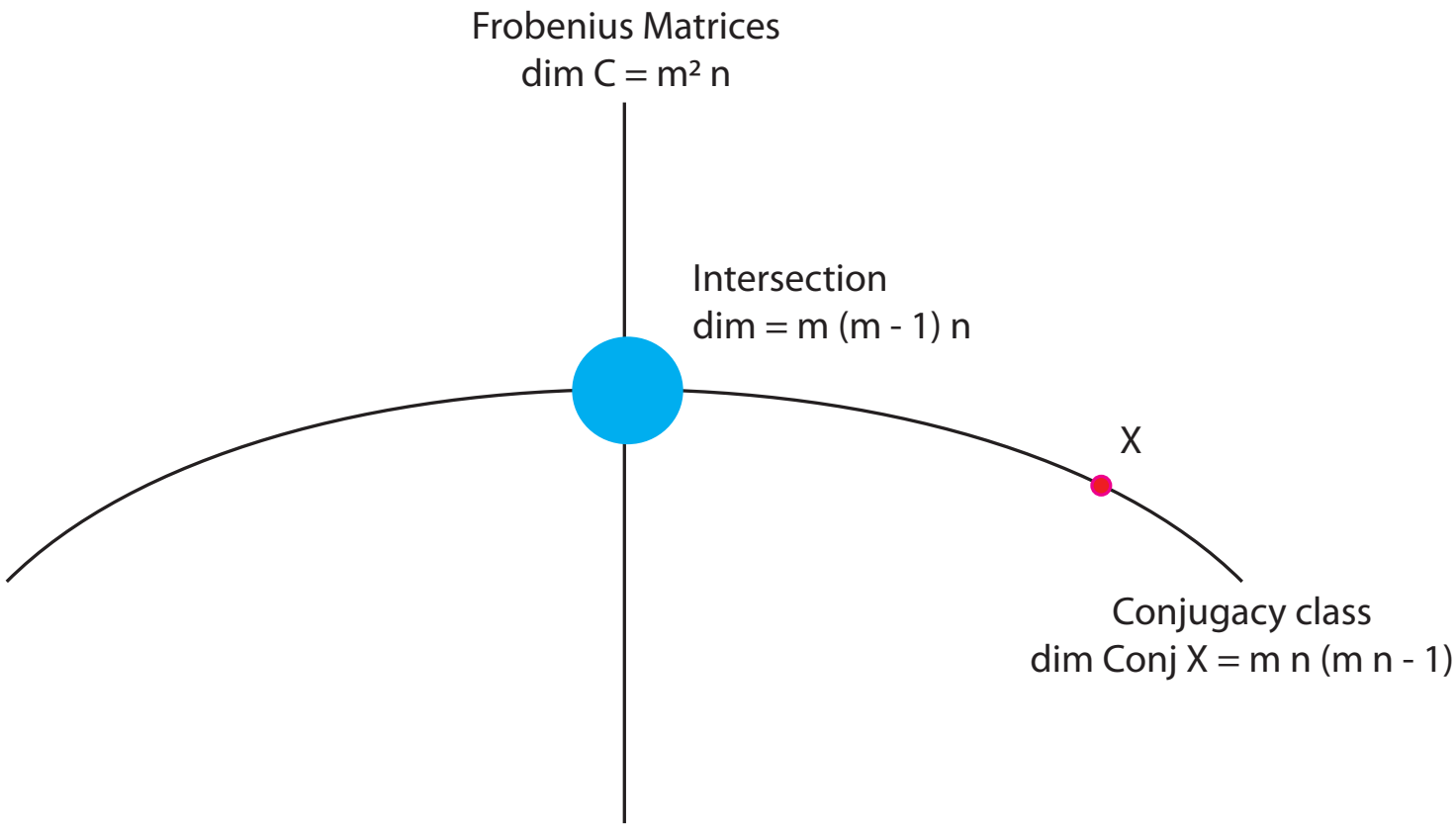
$$\mathbf{X} = \mathscr{C} \cap \mathbf{Cmp}$$

Cmp = vector space of block companion matrices in $\mathrm{GL}_{mn}(\mathbb{F}_q)$

Scalar companion matrix in a conjugacy class



Block companion matrices in a conjugacy class



Enumeration of Block LSFRs

Enumeration Theorem (Chen and Tseng, 2012)

$$|\mathbf{X}| = q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i)$$

Notation

Let α be a root of χ.

$$\mathbb{F}_q(\alpha) = \mathbb{F}_{q^{mn}}, \quad \sigma x = x^q, \quad \sigma^n = \tau, \quad \tau^m = \mathrm{id}.$$

$$T = \begin{bmatrix} \alpha & 0 & \dots & 0 \\ 0 & \tau\alpha & & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \tau^{m-1}\alpha \end{bmatrix} \in \mathrm{GL}_m(\mathbb{F}_{q^{mn}}),$$

S : set of matrices

$$S = \begin{bmatrix} 1 & u_2 & \dots & u_m \\ 1 & \tau u_2 & \dots & \tau u_m \\ \dots & \dots & \dots & \dots \\ 1 & \tau^{m-1} u_2 & \dots & \tau^{m-1} u_m \end{bmatrix} \in \mathrm{GL}_m(\mathbb{F}_{q^{mn}}).$$

Block Vandermonde matrices

If $S \in \mathbf{S}$, define the *block Vandermonde matrix*

$$V_S = \begin{bmatrix} S & T.S & \dots & T^{n-1}.S \\ \sigma S & \sigma(TS) & \dots & \sigma(T^{n-1}.S) \\ \dots & \dots & \dots & \dots \\ \sigma^{n-1}S & \sigma^{n-1}(T.S) & \dots & \sigma^{n-1}(T^{n-1}.S) \end{bmatrix}$$

A difficulty:

- In the *scalar case*, the determinant of V_S is known (Vandermonde determinant !)
- In the *block case* ($m > 1$), *no known way* to decide if V_S is invertible

Structure of $\mathbf{X}$

Theorem

Let

$$\mathbf{S}^{\times} = \{S \in \mathbf{S} \mid \det \mathsf{V}_S \neq 0\}.$$

The map

$$\begin{array}{ccc} \mathbf{S}^{\times} & \longrightarrow & \mathbf{X} = \mathscr{C} \cap \mathbf{Cmp} \\ S & \mapsto & \mathsf{V}_S{}^{-1}.\mathsf{T}.\mathsf{V}_S \end{array}$$

is a bijection.

This provides an algorithm for the construction of all companion matrices with a given characteristic polynomial

Illustration: the case $m = 2$

Take $m = 2$ (2 bits !), $n = 3$, and assume that

$$\chi(\lambda) = \lambda^6 + \lambda^3 + 1$$

is irreducible in $\mathbb{F}_p$, e.g. $p = 2, 5, 11, \&c$. Then

$$T = \begin{bmatrix} \zeta & 0 \\ 0 & \zeta^8 \end{bmatrix} \quad \text{where} \quad \chi(\zeta) = 0,$$

$$S = \begin{bmatrix} 1 & u \\ 1 & \bar{u} \end{bmatrix}, \quad u = \sum_{i=0}^{5} u_i \zeta^i$$

$$\mathsf{V}_S = \begin{bmatrix} 1 & u & \zeta & u\zeta & \zeta^2 & u\zeta^2 \\ 1 & u^8 & \zeta^8 & u^8\zeta^8 & \zeta^7 & u^8\zeta^7 \\ 1 & u^2 & \zeta^2 & u^2\zeta^2 & \zeta^4 & u^2\zeta^4 \\ 1 & u^{16} & \zeta^7 & u^{16}\zeta^7 & \zeta^5 & u^{16}\zeta^5 \\ 1 & u^4 & \zeta^4 & u^4\zeta^4 & \zeta^8 & u^4\zeta^8 \\ 1 & u^{32} & \zeta^5 & u^{32}\zeta^5 & \zeta & u^{32}\zeta \end{bmatrix}$$

Up to a constant,

$$\det \mathrm{V}_S = u_3^3 - 2u_2u_3u_4 + u_1u_4^2 - u_4^3 \\ + u_2^2u_5 - u_1u_3u_5 + 3u_3u_4u_5 - 2u_2u_5^2 + u_5^3$$

According to the Enumeration Theorem, this hypersurface of $\mathbb{A}^6$ has exactly q^5 points over $\mathbb{F}_q$, and

$$|\mathbf{S}| = q^6, \quad |\mathbf{S}^\times| = q^5(q-1).$$

Binaries

If $q = 2$, then

$$|\mathbf{S}| = 64, \quad |\mathbf{S}^\times| = 32.$$

In the following slide we enumerate the two last columns of the 32 binary block companion matrices

$$C = \begin{bmatrix} 0 & 0 & 0 & 0 & * & * \\ 0 & 0 & 0 & 0 & * & * \\ 1 & 0 & 0 & 0 & * & * \\ 0 & 1 & 0 & 0 & * & * \\ 0 & 0 & 1 & 0 & * & * \\ 0 & 0 & 0 & 1 & * & * \end{bmatrix} \in \mathbf{M}_6(\mathbb{F}_2)$$

such that

$$\chi_C(\lambda) = \lambda^6 + \lambda^3 + 1.$$

(we are content with $\mathbb{F}_2$: around 10^{14} solutions on $\mathbb{F}_{256}$) $\longrightarrow$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 1 & 1 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 0 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 0 \\ 1 & 1 \\ 1 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 0 \end{bmatrix} \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$\times$$