Failed crypto: Matrices over non-standard arithmetic

Daniel R. L. Brown[*]

December 12, 2023

Abstract

A failed hypothesis is reported here. The hope was that large matrices over small non-standard arithmetic are likely to have infeasible division, and furthermore be secure for use in Rabi–Sherman associative cryptography.

1 Introduction

Rabi and Sherman [RS93] defined associative public-key cryptography in 1993. The main cost per user of a transaction is two applications of an associative binary operation (usually written as multiplication). The most direct attack is division, which finds effective private keys.

Matrix multiplication can be associative, if matrix entries are in a suitable realm. Standard realms such as fields and rings, and various quirky non-standard realms, including semirings, have associative matrix multiplication. More generally, it suffices for the realm to be marl (medial addition, associative multiplication, right and left distribution of multiplication over addition).

A first hypothesis for this report was that large matrices over a random small realm typically have infeasible division. One rationale was ignorance of a realm-generic matrix division algorithm. A second rationale was that marl realms might have algebraic quirks that are somehow obstacles to standard matrix division algorithms.

[*] BlackBerry, `danibrown@blackberry.com`

Experiment refuted the first hypothesis. Every random small realm so far examined seems to have matrix division quicker and simpler than matrix multiplication or standard matrix division. A revised hypothetical hope is that there might yet remain a rare small realm whose matrices have associative multiplication and infeasible division.

2 Matrix realms for associative crypto

A **realm** $(R, +, \times)$ is a set R with two binary operations defined on R, written as addition and multiplication.

A **matrix realm** $\mathrm{Mat}_t(R)$ is formed from a given realm R and a given binary tree t of $|t| = n$ leaves, by taking $n \times n$ square matrices over R and adapting the standard definition of matrix multiplication to use the tree t to determining the nesting of terms in the sums that are used to multiply individual rows and columns.

If matrix realm $\mathrm{Mat}_t(R)$ has associative multiplication, then its multiplication can be used in associative cryptography, which relies on the associative law $a(bc) = (ab)c$. For key agreement, a and c are private keys, ab and bc are public keys, and abc is the agreed secret key. For signatures, b is the private key, bc the public key, ab the signature, and $a(bc) = (ab)c$ verifies a signature. (Rectangular matrices can be used for compression.)

The resulting cryptography is secure only if matrix division is infeasible. So, for example, computing a binary operator $/$ such that $((ab)/b)b = ab$ for all matrices $a, b \in \mathrm{Mat}_t(R)$ should be infeasible. In particular, exhaustive search (of rows or of columns) must be infeasible, which requires that $|R|^{|t|} \geq 2^{128}$. This size requirement is not enough: better attacks are possible in many cases. A matrix realm should be carefully scrutinized before use in associative cryptography.

A supply of small realms with associative multiplication is first needed to apply this scrutiny.

3 Marl realms

Matrix realm $\mathrm{Mat}_t(R)$ has associative multiplication if R is **marl**, meaning that the four axioms:

$$\begin{aligned}(a+b)+(c+d) &= (a+c)+(b+d), && (1)\\ a(bc) &= (ab)c, && (2)\\ (a+b)c &= ac+bc, && (3)\\ a(b+c) &= ab+ac, && (4)\end{aligned}$$

hold for all $a, b, c, d \in R$. The four axioms are **medial addition** and **associative multiplication** and **right distribution** and **left distribution** (hence **marl**).

To be fair, it must also be said that some non-marl realms have associative matrix multiplication too.

4 Insecure examples

The early empirical findings can be illustrated by a few examples.

4.1 A randomized realm of size 8

The realm with set $\{0, 1, 2, 3, 4, 5, 6, 7\}$, and addition and multiplication:

+	0	1	2	3	4	5	6	7
0	3	0	2	1	6	5	7	4
1	5	1	6	0	2	3	4	7
2	1	5	4	3	7	0	6	2
3	0	3	7	5	4	1	2	6
4	3	0	2	1	6	5	7	4
5	1	5	4	3	7	0	6	2
6	0	3	7	5	4	1	2	6
7	5	1	6	0	2	3	4	7

×	0	1	2	3	4	5	6	7
0	2	7	3	4	5	6	0	1
1	7	7	1	7	1	7	1	1
2	3	1	4	5	6	0	2	7
3	4	7	5	6	0	2	3	1
4	5	1	6	0	2	3	4	7
5	6	7	0	2	3	4	5	1
6	0	1	2	3	4	5	6	7
7	1	1	7	1	7	1	7	7

(5)

is marl. Verifying marl axioms for this realm was first done mechanically, and then manually via reasoning from an isomorphism to a more natural structure. The $8^4 + 3(8^3) = 5632$ instances of the marl axioms for this realm would be too tedious manually verify. One instance of each marl axioms is easy enough to verify (writing 14 for 1 × 4):

$$\begin{gathered}(3+1)+(4+1)=3+0=0=4+1=(3+4)+(1+1),\\ 3(14)=31=7=74=(31)4,\\ (3+1)4=34=0=0+1=34+14,\\ 3(1+4)=32=5=7+0=31+34.\end{gathered}$$

Quirks of this realm include non-commutative and non-cancellative addition:

$$\begin{gathered}0=0+1\neq 1+0=5,\\ 2+1=5+1.\end{gathered}$$

Similar quirks tend to arise when choosing realms randomly.

Associative matrix multiplication happens because the realm is marl. An instance of associativity can be verified:

$$a=\begin{pmatrix}7&6&1&3&1\\7&2&4&1&5\\2&3&2&3&3\\6&4&2&4&0\\3&0&7&5&6\end{pmatrix},\quad b=\begin{pmatrix}2&6&3&3&7\\1&2&6&2&5\\7&1&0&3&2\\5&5&5&7&0\\1&6&4&3&2\end{pmatrix},\quad c=\begin{pmatrix}5&6&3&4&4\\1&6&2&4&1\\1&5&4&7&0\\1&6&1&1&1\\4&7&6&1&6\end{pmatrix},$$

$$d=ab=\begin{pmatrix}6&1&5&6&0\\7&0&0&6&0\\2&3&3&6&1\\6&0&5&6&0\\1&4&4&3&6\end{pmatrix},\qquad e=bc=\begin{pmatrix}4&4&6&0&4\\0&3&3&4&0\\4&7&7&1&7\\5&3&3&2&1\\4&4&6&5&7\end{pmatrix},$$

$$f=ae=a(bc)=\begin{pmatrix}0&1&1&4&5\\3&5&1&6&0\\0&0&3&4&0\\0&5&0&2&5\\2&2&6&3&2\end{pmatrix}=(ab)c=dc=g,$$

where a matrix entry such as $d_{4,3}$ is defined by computations:

$$\begin{aligned}
d_{4,3} = (ab)_{4,3} = \sum_{j=1}^{5} a_{4,j} b_{j,3} & \\
&= (((a_{4,1}b_{1,3} + a_{4,2}b_{2,3}) + a_{4,3}b_{3,3}) + a_{4,4}b_{4,3}) + a_{4,5}b_{5,3} \\
&= (((63 + 46) + 20) + 45) + 04 \\
&= (((3 + 4) + 3) + 3) + 5 \\
&= ((4 + 3) + 3) + 5 \\
&= (1 + 3) + 5 \\
&= 0 + 5 \\
&= 5.
\end{aligned}$$

Note that the tree used in the sum above is a left comb tree of five leaves, which we write as $5 = (((1 + 1) + 1) + 1) + 1$, where here the notations 1, 5, and + are tree arithmetic, which do not refer to the 8-element realm, but to binary trees and the addition of binary trees.

The 8-element realm (5) was selected using a partially randomized process. This realm reduces to a direct product of smaller realms, whose operations are easily described in terms of classical algebra. This reduction is easy to find, because the realm is small. Generally, known structures cannot be hidden in small realms. In this example, the reduction leads to a quick matrix division for the 8-element realm.

4.2 A realm of 9 endomorphisms

The 9-element realm with addition and multiplication:

+	0	1	2	3	4	5	6	7	8
0	0	2	1	6	8	7	3	5	4
1	2	1	0	8	7	6	5	4	3
2	1	0	2	7	6	8	4	3	5
3	6	8	7	3	5	4	0	2	1
4	8	7	6	5	4	3	2	1	0
5	7	6	8	4	3	5	1	0	2
6	3	5	4	0	2	1	6	8	7
7	5	4	3	2	1	0	8	7	6
8	4	3	5	1	0	2	7	6	8

×	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1	1
2	2	2	2	2	2	2	2	2	2
3	0	1	2	3	4	5	6	7	8
4	1	2	0	4	5	3	7	8	6
5	2	0	1	5	3	4	8	6	7
6	0	2	1	6	8	7	3	5	4
7	1	0	2	7	6	8	4	3	5
8	2	1	0	8	7	6	5	4	3

(6)

is marl. Again, it is easy to manually verify one instance of each of the four marl axioms. For example,

$$\begin{gathered}(3+1)+(4+1)=8+7=6=5+1=(3+4)+(1+1),\\ 3(14)=31=1=14=(31)4,\\ (3+1)4=84=7=4+1=34+14,\\ 3(1+4)=31=1=1+4=31+34.\end{gathered}$$

Some quirks of this realm are non-associative addition and non-commutative multiplication, for example:

$$\begin{gathered}3+(1+4)=3+7=2\neq 0=8+4=(3+1)+4,\\ 14=1\neq 2=41.\end{gathered}$$

Multiplication of 8×8 square matrices can be specified by choosing a binary tree with 8 leaves. For example, using tree arithmetic, define a tree

$$t=1+(2+2)+3=(1+((1+1)+(1+1)))+((1+1)+1). \tag{7}$$

An example of multiplication in $\mathrm{Mat}_t(R)$ is then

$$\begin{aligned}&\begin{pmatrix}1&7&3&1&4&3&2&0\\4&5&6&8&6&8&2&5\\7&8&6&7&0&1&6&6\\5&4&8&3&8&4&3&8\\7&0&1&6&1&0&4&3\\4&3&0&3&0&5&7&6\\1&0&0&4&6&0&0&5\\0&4&4&5&4&8&6&6\end{pmatrix}=ab\\ &\qquad=\begin{pmatrix}0&1&8&4&4&3&4&6\\2&7&6&7&6&7&6&7\\6&4&7&5&8&3&4&4\\3&2&2&3&8&7&7&5\\5&2&0&8&2&3&5&6\\5&1&8&0&3&5&3&4\\6&4&8&5&4&7&8&8\\1&8&6&0&1&8&2&7\end{pmatrix}\begin{pmatrix}8&6&2&5&0&3&0&7\\3&6&3&3&2&1&4&5\\5&7&0&0&5&6&5&5\\1&1&1&2&8&0&3&7\\4&2&4&7&3&5&5&3\\2&7&1&8&3&6&3&6\\6&1&7&0&4&5&1&6\\4&0&4&1&8&4&1&3\end{pmatrix}\end{aligned} \tag{8}$$

The entry $(ab)_{1,1}$ can be verified by multiplying entries the top row of a with the corresponding entries the left column of b, and then computing the t-sum, like this:

$$\begin{aligned}
(ab)_{1,1} &= \sum^{t}(a_{1,1}b_{1,1}, a_{1,2}b_{2,1}, \ldots, a_{1,8}b_{8,1}) \\
&= \sum^{t}(08, 13, 85, 41, 44, 32, 46, 64) \\
&= \sum^{t}(0, 1, 6, 2, 5, 2, 7, 8) \\
&= (0 + ((1 + 6) + (2 + 5))) + ((2 + 7) + 8) \\
&= (0 + (5 + 8)) + (3 + 8) \\
&= (0 + 2) + 1 \\
&= 1 + 1 \\
&= 1,
\end{aligned} \tag{9}$$

where the nesting of the sum $\sum^t$ matches the nesting of t in its tree arithmetic definition.

This marl realm was generated as the set of additive functions (endomorphisms) of an additive medial quasigroup:

$$\begin{array}{c|ccc}
+ & 0 & 1 & 2 \\
\hline
0 & 0 & 2 & 1 \\
1 & 2 & 1 & 0 \\
2 & 1 & 0 & 2
\end{array} \tag{10}$$

The Bruck–Murdoch–Toyoda (1938) theorem applies, so this 3-element medial quasigroup is isotopic to an abelian group, which in this case must be integers modulo 3.

The 9-element realm addition and multiplication can be explained from this medial quasigroup. Each 3-element row taken from the first three columns of the multiplication table represents an endomorphism on the medial quasigroup. The realm multiplication is function composition: with $(ef)(a) = e(f(a))$ for $a \in \{0, 1, 2\}$. The realm addition is function addition: with $(e + f)(a) = e(a) + f(a)$ for $a \in \{0, 1, 2\}$.

The 9-element realm here is also isomorphic to another realm, with elements $[a,b]$ for $a,b \in \{0,1,2\}$, and operations:

$$\begin{aligned} [a,b]+[c,d] &= [-a-b,\ -c-d], \\ [a,b][c,d] &= [ac,\ b+ad], \end{aligned}$$

where operations inside the square brackets are integer arithmetic modulo 3.

For the reasons above, and various other reasons, it seems that matrix division in this realm should be as quick as Gaussian elimination.

4.3 A size-11 realm with near-constant addition

The realm with addition and multiplication:

$+$	0	1	2	3	4	5	6	7	8	9	z
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	1
2	0	1	1	1	1	1	1	1	1	1	2
3	0	1	1	1	1	1	1	1	1	1	3
4	0	1	1	1	1	1	1	1	1	1	4
5	0	1	1	1	1	1	1	1	1	1	5
6	0	1	1	1	1	1	1	1	1	1	6
7	0	1	1	1	1	1	1	1	1	1	7
8	0	1	1	1	1	1	1	1	1	1	8
9	0	1	1	1	1	1	1	1	1	1	9
z	0	1	1	1	1	1	1	1	1	1	z

(11)

$\times$	0	1	2	3	4	5	6	7	8	9	z
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	1	1	1	1	1	1	1	1	z
2	0	1	1	2	1	1	2	4	4	5	z
3	0	1	1	3	1	1	3	7	7	9	z
4	0	1	2	1	4	5	4	1	2	1	z
5	0	1	2	2	4	5	5	4	5	5	z
6	0	1	2	3	4	5	6	7	8	9	z
7	0	1	3	1	7	9	7	1	3	1	z
8	0	1	3	2	7	9	8	4	6	5	z
9	0	1	3	3	7	9	9	7	9	9	z
z	z	z	z	z	z	z	z	z	z	z	z

(12)

is marl. In this realm, addition collapses drastically:

$$a + b = \begin{cases} a & \text{if } b = z, \\ 0 & \text{if } a = 0 \text{ or } b = 0, \\ 1 & \text{if } a \neq 0 \text{ and } b \neq 0, z. \end{cases}$$

In most cases, $a + b = 1$. Each row of the addition table is nearly constant, and so is each column, except the z-column, which is the identity column. Multiplication does not collapse as much as addition, but most rows and columns have many repeated entries. A multiplicative identity is 6, so its row and column are the identity function. Another multiplicatively canceling element is 8, and its row and columns are permutations.

Two large matrices usually have a product with most entries equal to 0, and almost all the rest of entries with value 1. Because matrix multiplication collapses, matrix division should be quick. Loosely speaking, to divide, just put zeros in the places that cause the zero rows in the product.

Thus matrix division should be much faster than matrix multiplication. This is typical for the most of the realms found by the search methods so far used. Indeed, matrix multiplication is often so non-cancellative that matrix division allows almost arbitrary entries to be assigned to the quotient matrix.

5 To do

The main question is, recall, the existence of a small realm with associative matrix multiplication and infeasible large matrix division (and more generally, security for instantiating associative cryptography). Ideally, the answer will either

- find such a secure small realm, or
- prove that all small realms are insecure.

An initial hypothesis that most small realms would be secure has been strongly rejected, according evidence on the smallest realms. A backup hope for cryptography is that some rare small realm is secure, despite current evidence to the contrary.

A clear answer might be obvious to experts. For example, Cunningham and Butković each describe simple algorithms for matrix division over minimax algebras (also known as tropical algebras). Monico found a new quick matrix division for a subclass of semirings (private communication).

Pending a clear answer, the interim plan for the next update of this report is to include:

- comparison to previous work,
- elementary lemmas about realms and magmas,
- a catalog of small realms and magmas,
- algorithms used to find realms with associative multiplication,
- algorithms for matrix division (including Monico's new algorithm).

Roughly 100 pages of elementary results compiled so far have failed to clearly answer the main question. Thousands of small realms have been examined in varying degrees of detail. The main pattern observed is a trend towards a collapse in matrix multiplication, which seems to imply matrix division quicker than multiplication. The exceptions to this trend that were subjected to closer examination were all realms with a structure that seemed to imply quick matrix algorithms, derivable from standard Gaussian elimination or simpler algorithms.

References

[RS93] Muhammad Rabi and Alan T. Sherman. Associative one-way functions: A new paradigm for secret-key agreement and digital signatures. Technical Report CS-TR-3183/UMIACS-TR-93-124, U. of Maryland, 1993.