Quasigroups and Related Systems **27** (2019), 317 − 324

Means compatible with semigroup laws

Ranganathan Padmanabhan and Alok Shukla

Abstract. A binary mean operation $m(x, y)$ is said to be compatible with a semigroup law $*$, if $*$ satisfies the Gauss' functional equation $m(x, y) * m(x, y) = x * y$ for all x, y. Thus the arithmetic mean is compatible with the group addition in the set of real numbers, while the geometric mean is compatible with the group multiplication in the set of all positive real numbers. Using one of the Jacobi theta functions, Tanimoto [6], [7] has constructed a novel binary operation $*$ compatible with the arithmetico-geometric mean $\operatorname{agm}(x, y)$ of Gauss. Tanimoto shows that it is only a loop operation, but not associative. A natural question is to ask if there exists a group law $*$ compatible with arithmetic-geometric mean. In this paper we prove that there is no semigroup law compatible with agm and hence, in particular, no group law either. Among other things, this explains why Tanimoto's operation $*$ using theta functions must be non-associative.

1. Introduction

Gauss discovered the arithmetico-geometric mean (agm) at the age of 15. Starting with two positive real numbers x and y, Gauss considered the sequences $\{x_n\}$ and $\{y_n\}$ of arithmetic and geometric means

$$x_0 = x, \quad y_0 = y, \quad x_n = \frac{x_{n-1} + y_{n-1}}{2}, \quad y_n = \sqrt{x_{n-1}y_{n-1}}, \quad \text{for } n \geqslant 1.$$

Then Gauss defined $\operatorname{agm}(x, y)$ to be the common limit of the sequences $\{x_n\}$ and $\{y_n\}$, i.e.,

$$\operatorname{agm}(x, y) = \lim_{n\to\infty} x_n = \lim_{n\to\infty} y_n. \tag{1}$$

For an engaging historical account on agm and its applications in mathematics readers are referred to [1],[2].

In this paper, we ask if there exist a group law $*$, which is compatible with agm. Before proceeding further we give some definitions relevant to this work.

Definition 1.1 (See for example, [5])**.** Let S be a set equipped with a binary operation m. It is said that m is a *mean*, if it satisfies the following

(M_1) $\quad m(x, x) = x,$

2010 Mathematics Subject Classification: Primary: 20N05; Secondary: 26E60
Keywords: arithmetic mean, geometric mean, harmonic mean, arithmetic-geometric mean, compatible group law, loops, medial law.

(M_2) $m(x,y) = m(y,x)$,

(M_3) $m(x,y) = m(z,y) \implies x = z$.

Definition 1.2 (Compatibility of binary operations)**.** Let S be a set equipped with a binary mean operation m and another binary operation $*$. The binary mean operation m, and the binary operation $*$, are said to be *compatible* with each other, if $m(x,y) * m(x,y) = x * y$ for all $x, y \in S$.

Here we find conditions on the mean m which force any compatible operation $*$ to be a group operation.

Let $\mathrm{AM}(x,y) = \dfrac{x+y}{2}$ be the arithmetic mean of $x, y \in \mathbb{R}$ with $+$ being the usual addition in $\mathbb{R}$. Then clearly $\mathrm{AM}(x,y) + \mathrm{AM}(x,y) = x + y$, therefore, the classical arithmetic mean $\mathrm{AM}(x,y)$ is compatible with the group law of $+$ in $\mathbb{R}$, in the sense of Definition 1.2. Similarly, the geometric mean GM is also compatible with the group law of multiplication in positive reals. Similarly, it can be verified that the harmonic mean $h(x,y) = \dfrac{2xy}{x+y}$ is compatible with the semigroup law $x * y = \dfrac{xy}{x+y}$. It is then natural to consider if there exists any such group operation over $\mathbb{R}^+$, which is compatible with the arithmetic-geometric mean (agm) of Gauss. In other words, we want to address the question, if there exists a group operation $*$, such that $\mathrm{agm}(x,y) * \mathrm{agm}(x,y) = x * y$. Using one of the Jacobi theta functions, Shinji Tanimoto has successfully constructed a non-associative loop operation $\star$ (c.f. [6], [7], Sec. below) that is compatible with agm. However, no group law $*$ compatible with agm is known to exist. Indeed, we prove that no such group law $*$ can exist, which is compatible with agm.

1.1. A non-associative loop operation compatible with agm

Now we recall the binary operation $\star$ introduced by S. Tanimoto in [6], [7].

Definition 1.3 (Tanimoto, [6], [7])**.** For any two positive numbers x and y, choose the unique q $(-1 < q < 1)$ such that $1/\mathrm{agm}(x,y) = \theta^2(q)$. Here, θ is one of the Jacobi theta functions:

$$\theta(q) = \sum_{n=-\infty}^{+\infty} q^{n^2} = 1 + 2\sum_{n=1}^{\infty} q^{n^2}.$$

Then define

$$x \star y = \theta^2(-q)/\theta^2(q). \tag{2}$$

We also recall the following theorems from [7], which describe the properties of the $\star$ operation. We note that here variables x, y are positive real numbers.

Theorem 1.4 (Tanimoto, [7]). *The operation $\star$ defined above satisfies the following properties.*
(A) $1 \star x = x$ for all x. *Hence* 1 *is the unit element of the operation.*
(B) $x \star x = y \star y$ *implies* $x = y$.
(C) $x \star y = \mathrm{agm}(x, y) \star \mathrm{agm}(x, y)$. *Thus the mean with respect to the operation is the* agm.

Theorem 1.5 (Tanimoto, [7]). *The operation $\star$ satisfies the following algebraic properties.*
(D) $a \star x = a \star y$ *implies* $x = y$ *(a cancellation law).*
(E) $(ax) \star (ay) = a \star (a(x \star y))$ *for any* a, x, y *(a distributive law).*
(F) *If* $z = x \star y$, *then* $y = x(x^{-1} \star (x^{-1}z))$. *In particular, the inverse of x with respect to the operation is* $x(x^{-1} \star x^{-1})$.

Finally, we note that Tanimoto claims that the $\star$ operation is not associative (although, he does not give any example).

2. Main results

Now we are ready to prove our claim that there does not exist any group law $*$, that is compatible with agm in the sense of the Definition 1.2. In this direction, first we prove the following theorem.

Theorem 2.1. *Let $m(x, y)$ and $*$ be two binary operations defined over a non-empty set containing a distinguished element e such that*

(M_1) $m(x, x) = x$,

(M_2) $m(x, y) = m(y, x)$,

(M_3) $m(x, y) = m(z, y) \implies x = z$,

(M_4) $m(x, y) * m(x, y) = x * y$. *(Gauss' Functional Equation),*

(M_5) $e * x = x$,

(M_6) $x * x = y * y \implies x = y$.

Then m is medial, i.e., $m(m(x, y), m(z, u)) = m(m(x, z), m(y, u))$ *if and only if the $*$ operation is associative.*

Before proving Theorem 2.1, we state and prove the following lemmas.

Lemma 2.2. *Under the hypothesis* (M_1)-(M_6) *of Theorem* 2.1, *we have the following results.*

(i) $m(x, y) = m(e, x * y)$,

(ii) $x * y = y * x$.

Proof. The lemma follows from the following calculations.

(i). We have

$$\begin{aligned} m(x,y)*m(x,y) &= x*y \qquad (\text{from } (M_4)) \\ &= e*(x*y) \qquad (\text{from } (M_5)) \\ &= m(e,x*y)*m(e,x*y) \qquad (\text{from } (M_4)). \end{aligned}$$

Now the result follows from (M_6).

(ii). $x*y = m(x,y)*m(x,y) = m(y,x)*m(y,x) = y*x$. □

Lemma 2.3. *Assume the hypothesis* $(M_1)-(M_6)$ *of Theorem* 2.1*. Also assume either* $*$ *is associative, or* m *is medial. Then*

$$m(x,e)*m(e,y) = m(x,y). \tag{3}$$

Proof. First we assume that $*$ is associative. Then the desired conclusion follows from the following calculation and (M_6).

$$\begin{aligned} &(m(x,e)*m(e,y))*(m(x,e)*m(e,y)) \\ &= m(x,e)*m(e,y)*m(x,e)*m(e,y) \qquad (\text{from the associativity of } *) \\ &= m(x,e)*m(x,e)*m(e,y)*m(e,y) \qquad (\text{from Lemma 2.2 } (ii)) \\ &= (m(x,e)*m(x,e))*(m(e,y)*m(e,y)) \qquad (\text{from the associativity of } *) \\ &= (x*e)*(e*y) \qquad (\text{from } (M_4)) \\ &= x*y \qquad (\text{from Lemma 2.2 } ((ii) \text{ and } (M_5)) \\ &= m(x,y)*m(x,y) \qquad (\text{from } (M_4)) \end{aligned}$$

Next we assume that m is medial, i.e.,

$$m(m(x,y),m(z,u)) = m(m(x,z),m(y,u)).$$

Then we have

$$\begin{aligned} &m(m(x,y),m(z,u))*m(m(x,y),m(z,u)) \\ &= m(m(x,z),m(y,u))*m(m(x,z),m(y,u)) \\ \Longrightarrow\ & m(x,y)*m(z,u) = m(x,z)*m(y,u) \qquad (\text{from } (M_4)) \qquad (4) \\ \Longrightarrow\ & m(x,y)*m(e,e) = m(x,e)*m(y,e) \qquad (\text{put } z=u=e) \\ \Longrightarrow\ & m(x,y)*e = m(x,e)*m(e,y) \qquad (\text{from } (M_1) \text{ and } (M_2)) \\ \Longrightarrow\ & m(x,y) = m(x,e)*m(e,y) \qquad (\text{from } (M_5) \text{ and Lemma 2.2 } (ii)) \end{aligned}$$

□

Proof of Theorem 2.1. Assume that $*$ is associative. Then

$$\begin{aligned}
&m(m(x,y),m(z,u)) * m(m(x,y),m(z,u)) \\
&= m(x,y) * m(z,u) \qquad \text{(from } (M_4)) \\
&= (m(x,e) * m(e,y)) * (m(z,e) * m(e,u)) \qquad \text{(from Lemma 2.3)} \\
&= m(x,e) * m(e,y) * m(z,e) * m(e,u) \qquad \text{(from the associativity of } *) \\
&= m(x,e) * m(z,e) * m(e,y) * m(e,u) \qquad \text{(from Lemma 2.2 } (ii)) \\
&= m(x,e) * m(e,z) * m(y,e) * m(e,u) \qquad \text{(from } (M_2)) \\
&= (m(x,e) * m(e,z)) * (m(y,e) * m(e,u)) \qquad \text{(from the associativity of } *) \\
&= m(x,z) * m(y,u) \qquad \text{(from Lemma 2.3)} \\
&= m(m(x,z),m(y,u)) * m(m(x,z),m(y,u)) \qquad \text{(from } (M_4)).
\end{aligned}$$

This proves one direction of the theorem, as (M_6) now implies that m is medial, i.e., $m(m(x,y),m(z,u)) = m(m(x,z),m(y,u))$.

Next to prove the other direction assume that

$$m(m(x,y),m(z,u)) = m(m(x,z),m(y,u)).$$

Then from (4) we have

$$m(x,y) * m(z,u) = m(x,u) * m(z,y).$$

For $x = e$, the above relation becomes

$$m(e,y) * m(z,u) = m(e,u) * m(z,y). \tag{5}$$

Now,

$$\begin{aligned}
m(e,y) * m(z,u) &= m(e,y) * m(e,z*u) \qquad \text{(from Lemma 2.2 } (i)) \\
&= m(y,e) * m(e,z*u) \qquad \text{(from } (M_2)) \\
&= m(y,z*u) \qquad \text{(from Lemma 2.3)} \\
&= m(e,y*(z*u)). \qquad \text{(from Lemma 2.2 } (i))
\end{aligned} \tag{6}$$

Similarly,

$$m(e,u) * m(z,y) = m(e,u*(z*y)). \tag{7}$$

From (5), (6), and (7), we get

$$m(e,y*(z*u)) = m(e,u*(z*y)).$$

$$\begin{aligned}
&m(e,y*(z*u)) = m(e,u*(z*y)) \\
&\implies y*(z*u) = u*(z*y) \qquad \text{(from } (M_3)) \\
&\implies y*(z*u) = u*(y*z) \qquad \text{(from Lemma 2.2 } (ii)) \\
&\implies y*(z*u) = (y*z)*u. \qquad \text{(from Lemma 2.2 } (ii))
\end{aligned}$$

This completes the proof. □

Corollary 2.4 (of Theorem 2.1). *There does not exist any group law $*$, that is compatible with* agm.

Proof. From the definition of agm, it is obvious that $\mathrm{agm}(x,x) = x$ and $\mathrm{agm}(x,y) = \mathrm{agm}(y,x)$. Further, if $\mathrm{agm}(x,y) = \mathrm{agm}(x,z)$, then

$$\mathrm{agm}(x,y) \star \mathrm{agm}(x,y) = \mathrm{agm}(x,z) \star \mathrm{agm}(x,z) \implies x \star y = x \star z \implies y = z,$$

from Theorem 1.4 (C) and Theorem 1.5 (D). Therefore, agm is a mean operation in the sense of Definition 1.1. It can be verified from a direct numerical computation that agm is not medial, for example $\mathrm{agm}(\mathrm{agm}(1,2), \mathrm{agm}(3,4)) \neq \mathrm{agm}(\mathrm{agm}(1,3), \mathrm{agm}(2,4))$. But then, it means agm can not be compatible with any $*$ operation which is associative and satisfies $(M_4) - (M_6)$, otherwise Theorem 2.1 will imply that agm is medial. Therefore, there can not exist any group law $*$, that is compatible with agm. □

Suppose for a mean m, if $m(m(x,y), m(x,z)) = m(x, m(y,z))$, then the mean m is said to be self-distributive. By an abuse of language, let us call a loop operation $*$ to be "self-distributive" if $(x*x)*(y*z) = (x*y)*(x*z)$. Theorem 2.5 given below justifies this. The connection between mediality and self-distributivity can be found in [4] and references therein.

It is easy to see that in the above proofs, the full force of associativity (or, for that matter the medial law) is not used. Indeed, 'associativity' and 'medial' in Theorem 2.1, can be replaced by '$*$-self-distributive' and 'm-self-distributive', respectively and the proof of the theorem still remains valid.

Theorem 2.5. *For a mean m and a binary operation $*$ satisfying (M_1)-(M_6) of Theorem* 2.1, *m is self-distributive, i.e., $m(m(x,y), m(x,z)) = m(x, m(y,z))$ if and only if the $*$ operation is self-distributive.*

One can easily verify (for example by using Mathematica) that

$$\mathrm{agm}(\mathrm{agm}(1,2), \mathrm{agm}(1,3)) \neq \mathrm{agm}(1, \mathrm{agm}(2,3)).$$

Hence, Gauss' Functional Equation for agm can not be solved even among self-distributive loops.

Although, we have remarked earlier that the proof of Theorem 2.5 follows on the same line as Theorem 2.1, we are enclosing an automated proof of this theorem by using Prover9 [3], in the Appendix, for readers interested in automated reasoning.

Acknowledgments. We sincerely thank the referee for all the suggestions and corrections which enhanced the presentation of the paper.

A computation using Mathematica shows $2.359575 = \mathrm{agm}(\mathrm{agm}(1,2), \mathrm{agm}(3,4)) \neq \mathrm{agm}(\mathrm{agm}(1,3), \mathrm{agm}(2,4)) = 2.359305$. Theorem 2.1, then implies that $\star$ is not associative, verifying Tanimoto's unsupported claim.

3. Appendix

$*$-self-distributivity identity implies m-self-distributivity.

```
1 m(x,m(y,z)) = m(m(x,y),m(x,z)) # label(goal).  [].
3 m(x,y) = m(y,x).  [].
5 m(x,y) * m(x,y) = x * y.  [].
6 x * x != y * y | x = y.  [].
7 x * e = x.  [].
8 (x * y) * (x * z) = (x * x) * (y * z).  [].
9 m(m(c1,c2),m(c1,c3)) != m(c1,m(c2,c3)).  [1].
10 m(c1,m(c2,c3)) != m(m(c1,c2),m(c1,c3)).  [9].
15 m(x,y) * m(y,x) = y * x.  [3,5].
16 x * y = y * x.  [3,5,15].
17 x * y != z * z | m(x,y) = z.  [5,6].
23 c1 * m(c2,c3) != m(c1,c2) * m(c1,c3).  [6,10,5,5].
32 c1 * m(c3,c2) != m(c1,c2) * m(c1,c3).  [3,23].
48 e * x = x.  [16,7].
50 (x * y) * (z * x) = (x * x) * (y * z).  [16,8].
79 c1 * m(c3,c2) != m(c2,c1) * m(c1,c3).  [3,32].
130 m(e,x * x) = x.  [17,48].
132 m(x * x,y * y) = x * y.  [17,8].
160 m(e,x * y) = m(x,y).  [5,130].
221 c1 * m(c3,c2) != m(c1,c3) * m(c2,c1).  [16,79].
293 m(x * y,z * z) = m(x,y) * z.  [5,132].
294 m(x * x,y * z) = x * m(y,z).  [5,132].
662 m(x * y,z * x) = x * m(y,z).  [50,160,160,294].
1706 m(x * y,z * u) = m(x,y) * m(z,u).  [5,293].
1748 m(x,y) * m(z,x) = x * m(y,z).  [662,1706].
1749 $F.  [1748,221].
```

m-self-distributivity implies $*$-self-distributivity identity.

```
1 (x * y) * (x * z) = (x * x) * (y * z) # label(non_clause) # label(goal).  [].
2 m(x,x) = x.  [].
3 m(x,y) = m(y,x).  [].
4 m(x,y) != m(z,y) | x = z.  [].
5 m(x,y) * m(x,y) = x * y.  [].
6 x * x != y * y | x = y.  [].
7 x * e = x.  [].
8 m(x,m(y,z)) = m(m(x,y),m(x,z)).  [].
9 m(m(x,y),m(x,z)) = m(x,m(y,z)).  [8].
10 (c1 * c2) * (c1 * c3) != (c1 * c1) * (c2 * c3).  [1].
13 m(x,y) != m(z,x) | y = z.  [3,4].
15 m(x,y) * m(y,x) = y * x.  [3,5].
16 x * y = y * x.  [3,5,15].
17 x * y != z * z | m(x,y) = z.  [5,6].
22 m(x,y) * m(x,z) = x * m(y,z).  [9,5,9,5].
24 e * x = x.  [16,7].
```

```
26 m(x,y) != m(x,z) | y = z.  [3,13].
29 m(e,x * x) = x.  [17,24].
33 x * x != y | m(e,y) = x.  [24,17].
41 m(e,x) != y | y * y = x.  [29,26].
55 x != y | y * y = x * x.  [29,41].
56 m(e,x * y) = m(x,y).  [33,22,2].
58 m(x * x,y) = x * m(e,y).  [29,22,24].
68 m(x,e) != m(y,z) | y * z = x.  [56,13].
74 m(x,y) * m(e,z) = m(x * y,z).  [56,22,24].
79 m(x,y * y) = y * m(e,x).  [58,3].
80 m(x * x,y) = x * m(y,e).  [3,58].
99 m(x * x,y * z) = x * m(y,z).  [56,58].
134 m(x,y * y) = y * m(x,e).  [3,79].
153 m(x,x * y) = x * m(y,e).  [80,22,22,2,3].
220 m(x * x,y) = m(x,x * y).  [153,80].
225 m(x,y * y) = m(y,y * x).  [153,134].
240 m(x,x * (y * z)) = x * m(y,z).  [99,220].
338 x * (y * y) = y * (y * x).  [55,225,22,2,22,2].
427 (x * x) * y = x * (x * y).  [338,16].
448 (c1 * c2) * (c1 * c3) != c1 * (c1 * (c2 * c3)).  [10,427].
504 m(c1 * c2,c1 * c3) != c1 * m(c2,c3).  [68,448,3,56,240].
550 m(x,y) * m(z,u) = m(x * y,z * u).  [56,74].
568 m(x * y,x * z) = x * m(y,z).  [22,550].
569 $F.  [568,504].
```

References

[1] **G. Almkvist, B. Berndt**, *Gauss, Landen, Ramanujan, the Arithmetic-Geometric Mean, Ellipses, π, and the Ladies Diary*, Amer. Math. Monthly, **95** (1988), 585 – 608.

[2] **D.A. Cox**, *The Arithmetic-Geometric Mean of Gauss*, In: Pi, A source book, Springer, 1997, 481 – 536.

[3] **W.W. McCune**, *Prover9 and Mace4*, http://www.cs.unm.edu/ mccune/prover9/, version 1.6.0.

[4] **N.S. Mendelsohn, R. Padmanabhan**, *A polynomial map preserving the finite basis property, J. Algebra*, **49** (1977), 154 – 161.

[5] **K. Strambach**, *Distributive quasigroups*, In: Foundations of geometry: selected proceedings of a conference, (1976), 251.

[6] **S. Tanimoto**, *A novel operation associated with Gauss' arithmetic-geometric means*, (Japanese). Sugaku **49**)1997), 300 – 301.

[7] **S. Tanimoto**, *A novel operation associated with Gauss' arithmetic-geometric means*, arXiv:0708.3521, 2007.

Received February 27, 2019

R. Padmanabhan
Department of Mathematics, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada
e-mail: padman@cc.umanitoba.ca

A. Shukla
Department of Mathematics, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada
e-mail: Alok.Shukla@umanitoba.ca