SUBADDITION

David Choate

Abstract. Let $S = \{z = x + yj | x$ and y real, $-\pi < y \leq \pi\}$ and let $S^* = S \cup \{-\infty\}$. If $z = x_1 + y_1 j$, $w = x_2 + y_2 j \in S$, then define a *cylindrical addition*, $\oplus$, on S^* by $z \oplus w = (x_1 + x_2) + [(y_1 + y_2) \pmod{2\pi}]j$ and $z \oplus -\infty = -\infty$ for all $z \in S^*$. Define a subaddition, $\odot$, on S^* by $z \odot w = \log(e^z + e^w)$. Then $(C, +, \cdot) \cong (S^*, \oplus, \odot)$.

Subaddition has an application in signal processing.

A channel's fading can be modeled as the product of a slowly varying component and the transmitted signal. An amplitude-modulated signal can also be represented by a product of a carrier signal and envelope function.

The logarithmic function will transform a system modeled on a product to a conventional linear system that will yield to a classical attack. It is shown here that the logarithm, as a generalized superposition, will also transform a conventional linear system into another linear system, and therefore, nothing need be known about the original system before applying a logarithmic transformation.

1. Introduction. Let $S = \{z = x + yj | x$ and y real, $-\pi < y \leq \pi\}$ or equivalently, after an appropriate adjustment of the residue of y modulo 2π, $S = \{z = x + y \pmod{2\pi} j | x$ and y real $\}$, a horizontal strip. Let $S^* = S \cup \{-\infty\}$. Also, let $z = x_1 + y_1 j$ and $w = x_2 + y_2 j \in S^*$. Now, define a cylindrical addition on S^* as

$$z \oplus w = (x_1 + x_2) + [(y_1 + y_2) \mod (2\pi)]j$$

if both z and w are in S; otherwise $z \oplus w = -\infty$.

If $z = re^{j\theta}$, then define $\log(z) = \ln |r| + [\theta \pmod{2\pi}]j$ as usual.

Now let $z, w \in S^*$. Then define a new operation called *subaddition* on S^*, denoted by $\odot$, by

$$z \odot w = \log(e^z + e^w).$$

If we define $z \odot -\infty = -\infty = z \odot -\infty$ for every z in S^*, then $\odot$ is an operation on S^*, and clearly,

$$\log(z + w) = \log z \odot \log w.$$

2. The Field $(\mathbf{S}^*, \oplus, \odot)$. It is a simple exercise to show that $(S^*, \oplus, \odot)$ is a field, and, in fact, it will soon become unnecessary to do so. But for the purpose of illustration observe that the subadditive identity is $-\infty$ since

$$z \odot -\infty = \log(e^z + e^{-\infty}) = z.$$

Also, observe that if $z \in S$, then its subadditive inverse is $\pi j \oplus z$ since

$$\begin{aligned} z \odot (\pi j \oplus z) &= \log(e^z + e^{j\pi + z}) \\ &= \log[e^z(1 + e^{j\pi})] \\ &= \log(0) \\ &= -\infty. \end{aligned}$$

Certainly the subadditive inverse of $-\infty$ is $-\infty$. Therefore, every element in S^* has a subadditive inverse.

Furthermore, the distributive law of cylindrical addition over subaddition can be established with the following calculation.

For $u, v, w, \in S^*$,

$$\begin{aligned} u \oplus (v \odot w) &= \log(e^u) \oplus \log(e^v + e^w) \\ &= \log[e^u(e^v + e^w)] \\ &= \log(e^{u+v} + e^{u+w}) \\ &= \log(e^{u \oplus v} + e^{u \oplus w}) \\ &= (u \oplus v) \odot (u \oplus w). \end{aligned}$$

Observe that just as 0 has no multiplicative inverse in C, $-\infty$ has no cylindrical additive inverse in S^* and that the equation $-\infty \oplus z = -\infty$ is the $^*-$ equivalent to $(0)z = 0$ in C.

<u>Theorem 1</u>. $(C, \cdot, +) \cong (S^*, \oplus, \odot)$.

<u>Proof</u>. Define $\phi : C \to S^*$ by $\phi(z) = \log(z)$. Then,

$$\begin{aligned} \phi(z_1 z_2) &= \log(z_1 z_2) \\ &= \log(z_1) \oplus \log(z_2) \\ &= \phi(z_1) \oplus \phi(z_2). \end{aligned}$$

Furthermore,

$$\begin{aligned}\phi(z_1 + z_2) &= \log(z_1 + z_2)\\ &= \log(z_1) \odot \log(z_2)\\ &= \phi(z_1) \odot \phi(z_2).\end{aligned}$$

If $w \in S$, then its preimage under ϕ, $w \in S$, is e^w. Also the preimage of $-\infty$ is 0; so ϕ is onto.

If $\phi(z) = 0_{S^*}$, then $\log(z) = -\infty$, or $z = 0$; so ϕ is one-to-one.

3. The Complex Cylinder. There is a simple geometric interpretation of Theorem 1. Map the complex plane in Figure 1 onto the horizontal strip in Figure 2 by $f(z = re^{j\theta}) = \ln|r| + [\theta \pmod{2\pi}]j$. The three circles in the complex plane with radii $e^{-1}, 1$ and e are mapped into the three vertical lines in Figure 2. Since the upper and lower lines of the horizontal strip have been identified in the same congruence class modulo 2π, we have a cylinder shown in Figure 3.

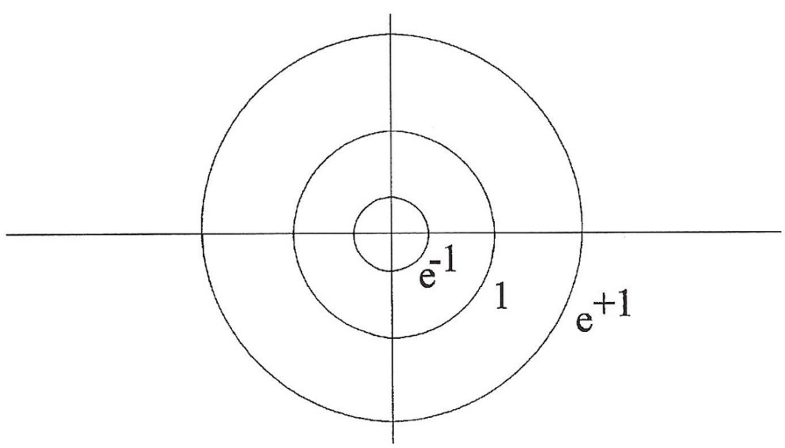

Figure 1.

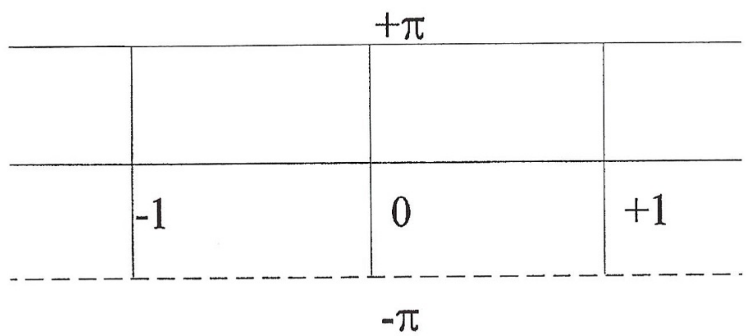

Figure 2.

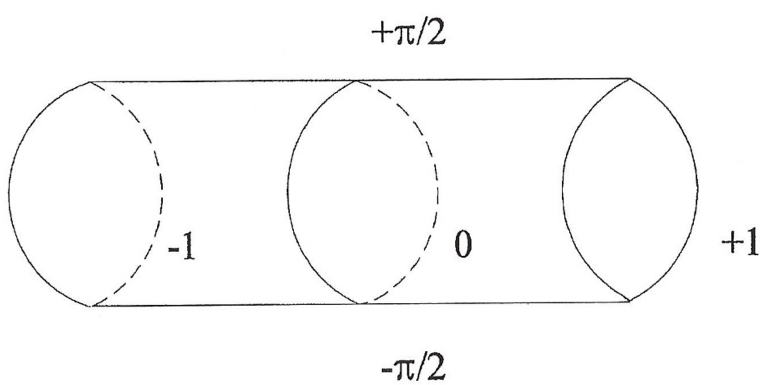

Figure 3.

To include $-\infty$ we must look down the right end of the cylinder. The circle with center $+1 = \log(e^{+1})$ appears the largest, the circle with center $-1 = \log(e^{-1})$ appears smallest and the end of the cylinder, $-\infty$, is a dot. This is the logarithmic image of Figure 1, the original complex plane.

4. Positive Infinity. Let $T^* = S \cup \{+\infty\}$ and define a new cylindrical addition as before except that $z \oplus +\infty = +\infty$ for any z in T^*. If we define a new subaddition $\otimes$ on T^* to be

$$z \otimes w = \log\{1/[(1/e^z) + (1/e^w)]\},$$

then it is easy to show, by a similar argument, that $(T^*, \oplus, \otimes) \cong (C, \cdot, +)$.

5. S*−Versions. To illustrate how easily theorems can be logarithmically transformed from $(C, \cdot, +)$ to $(S^*, \oplus, \odot)$ consider the *cylindrical quadratic equation*

$$(a \oplus 2x) \odot (b \oplus x) \odot (c) = -\infty$$

where $a, b, c, \in S^*$ and $a \neq -\infty$. (Of course, $2x = x \oplus x$.) Then we see at once that

$$x = \langle(\pi j \oplus b) \odot \{[(2b) \odot (\pi j \oplus \log 4 \oplus a \oplus c)]/2\}\rangle \oplus [\log(1/2) \oplus (-a)]$$

or

$$x = [\![(\pi j \oplus b) \odot \langle \pi j \oplus \{[(2b) \odot (\pi j \oplus \log 4 \oplus a \oplus c)]/2\}\rangle]\!] \oplus [\log(1/2) \oplus (-a)],$$

where cylindrical addition must be performed before subaddition.

6. A Superposition. All undefined and underdefined terms and symbols used in this section can be found in Chapter 5 of [1]. In fact, we are given a definition of a *superposition* H, a generalization of a system transformation, which must satisfy:
1. $H[x_1(n) \Box x_2(n)] = H(x_1(n) \circ x_2(n)]$
2. $H[c : x(n)] = c \uplus H(x(n)]$,

where $\Box$ is an input operation and $\circ$ is an output operation and where $:$ and $\uplus$ represent scalar multiplication.

Now, define $H : C \to S^*$ by $H(z) = \log(z)$. If we let

i. $\Box$ be $+$, ordinary addition in C,

ii. $\circ$ be $\odot$, or subaddition in S^*,
iii. : be scalar multiplication in C, and
iv. $\uplus$ be a scalar operation in S^* over C defined by

$$c \uplus H[x] = \log(c) \oplus H(x),$$

then we have a generalized superposition H (where H stands for *homomorphism.*)

But by [1] we can show that this homomorphic system can be written as a cascade of three systems provided that $\odot$ is commutative and associative (Theorem 1) and that we can prove the following theorem.

Theorem 2. The additive group S^* space under $\odot$ is a vector space over C with scalar multiplication $\uplus$.

Proof. Let $\alpha, \beta \in C$ and $v, w, \in S^*$. We now establish the four properties of a vector space.

(i.)
$$\begin{aligned} \alpha \uplus (v \odot w) &= \log(\alpha) \oplus (v \odot w) \\ &= [\log(\alpha) \oplus v] \odot [\log(\alpha) \oplus w] \\ &= (\alpha \uplus v) \odot (\alpha \uplus w). \end{aligned}$$

(ii.)
$$\begin{aligned} (\alpha \oplus \beta) \uplus v &= \log(\alpha + \beta) \oplus v \\ &= [\log(\alpha) \odot \log(\beta)] \oplus v \\ &= [\log(\alpha) \oplus v] \odot [\log(\beta) \oplus w] \\ &= (\alpha \uplus v) \odot (\beta \uplus w). \end{aligned}$$

(iii.)
$$\begin{aligned} \alpha \uplus (\beta \uplus v) &= \log(\alpha) \oplus [\log(\beta) \oplus v] \\ &= \log(\alpha\beta) \oplus v \\ &= (\alpha\beta) \uplus v. \end{aligned}$$

(iv.)
$$\begin{aligned} 1 \uplus v &= \log(1) \oplus v \\ &= v. \end{aligned}$$

Again, by [1] we know that since the system inputs constitute a vector space of complex numbers under addition and ordinary scalar multiplication and that the system outputs constitute a vector space under $\odot$, the subaddition, and $\uplus$, the scalar multiplication, then all systems of this class can be represented as a cascade of three systems where D_+, or $\log(\cdot)$ transforms a product or a sum into a conventional linear system L, and $(D\oplus)^{-1}$ is $\exp(\cdot)$.

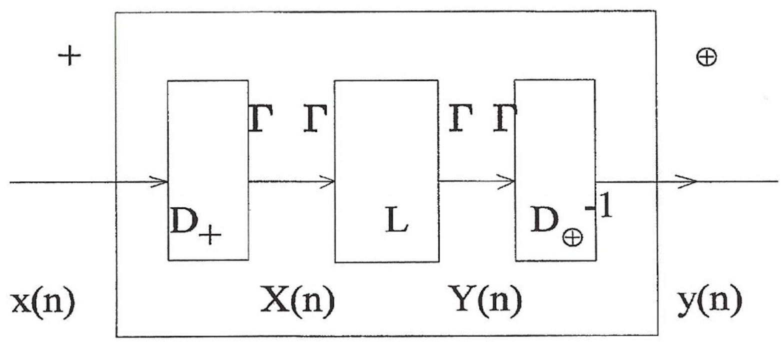

Figure 4.

Some systems can be modeled as products. For example, a channel's fading can be modeled as the product of a slowly varying component and the transmitted signal. An amplitude-modulated signal can also be represented by the product of a carrier signal and envelope function. In these systems homomorphic signal processing for multiplication can be used to determine frequencies. Superposition is a generalized principle of homomorphic signal processing.

The logarithmic function will transform a system modeled on a product to a conventional linear system that will yield to a classical attack. But a channel may or may not be fading. A signal may or may not be an amplitude-modulated one. It has been shown here that the logarithm, as a generalized superposition, will also transform a conventional linear system into another linear system, and therefore, nothing need be known about the system before applying a logarithmic transformation.

This research was sponsored by the Air Force Office of Scientific Research/AFSC, United States Air Force, under Contract F49620-93-C-0063. The Air Force is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notification hereon.

Reference

1. A. V. Oppenheim and R. W. Schafer, "Digital Signal Processing," Prentice-Hall, 1975.

David Choate
Department of Mathematics
Transylvania University
Lexington, KY 40508-1797
email: dchoate@music.transy.edu