
Article

Tri-state: from Shannon to Galois Fields in Communication Systems

Ed Gerck^{1,†} 

¹ Correspondence: egerck@gmail.com

[†] Current address: Planalto Research, 211 Hope St., #783, Mountain View, CA 94041, USA

Abstract: Communication, compression of information, transmission of information through noisy channels, interconnecting different information systems, cryptography, gate construction — these areas all depend on classical information theory. We show that, in classical terms, semantic aspects of communication are not at all irrelevant to the engineering problem, contrary to Shannon, and affect the message intended to be transmitted. This is revisited and captured by an analogy to trust, in that they are essential to the channel (for proper use), but cannot be transferred (under risk of flaws) through that same channel. Information is also described by, at least, a tri-state system — not by a binary logic. The trust analogy semantics can be coded as the Curry-Howard relationship, connecting computer code with structural logic, by way of different categories. Two-state and Boolean logic (aka Shannon semantics) was used classically before, with Shannon theory, but without trust analogy semantics – found to be a sine qua non condition. This is now familiar in classical gate construction with physical systems with, e.g., Verilog and SystemVerilog. The applications to computation and quantum theory are further explored, at least dismissing qubits and explaining its difficulties in representation. The most fundamental entity in today's theory of information is proposed to use at least three logical states, not bits, and in all applications, including: cyber-physical systems, devices, in computation, and in quantum theory.

Keywords: communication; information; tri-state, Galois field; quantum; qubit; qutrit; qudit; trust; interconnect; out-of-band

1. Introduction

In 1948, Claude Shannon published "A Mathematical Theory of Communication" [1], where the once fuzzy concept of "information" was proposed in a precise way to quantify the fundamental unit of classical information, the bit. This is a binary logic level system, following Boolean or classical logic, which carries two possible values, "0" and "1".

In its classical realization as a realizable physical system, using early bipolar junction transistors representing the bit, which, for example could be imagined to be just a relay, a transistor gate, or a mechanical switch, as pioneered by Shannon [1], one builds a system which is designed to have two distinguishable states only¹. The Law of the Excluded Middle (LEM) applies naturally to such a system, although it does not apply in a logic system with three or more logic levels².

Shannon did not consider semantics part of the design, writing: "Frequently the mes-

¹ There should be a sufficiently large energy barrier between them to create a "don't care" region — a region with no spontaneous transition, which would be evidently detrimental — occurring between the two logical states "0" and "1", allow for variations in the power supply, and noise pick-up in the lower level as well as the upper level.

² LEM says that "For every proposition 'p', either 'p' or 'not p' holds". To many this is a self-evident truth, but only works in a binary logical system, such as Boolean or classical logic [2].

sages have meaning; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are *irrelevant* to the engineering problem. The significant aspect is that the actual message is one selected from a set of possible messages." [1], ignoring the interconnects, essential part of a wider communication system, responsible for the necessary interconnections between different systems, heterogeneous and *a priori* different, with each other locked in N intersubjective relationships, mutually and intrinsically incompatible and undefinable, standing fixed under rules by different authorities, mechanisms, needs, or purposes — that is, by specialization.

But the semantics of a trust system³, which analogy [4] must be considered part of the wider communication system design, as interconnects, even though it must be out-of-band on its parts, and must exist under penalty of flaws, as discussed in Section 2.

These semantic aspects of communication are not at all irrelevant to the engineering problem, of the message intended to be transmitted, and are captured by an analogy to trust (as discussed in Section 2), in that they are essential to the channel (for proper use), but cannot be transferred (under risk of flaws) through that same channel [4].

The significant aspect is still that the actual message is one selected from a set of possible messages, but that it also is qualified to have the proper meaning. The system must be designed to operate for each possible selection — even though the selected message can be the same — given a meaning transmitted out-of-band, not just the one which will actually be chosen, since this is unknown at the time of design, and can be forced to deviate [4].

Trust can also be seen as that which can break one's system [4].

From this perspective, by believing in a *single* trusted introducer, a single source of information, a single trusted source, one has no correction channel available. One of the earliest references [4], however, to this situation as undesirable can be found some five hundred years ago in the Hindu governments of the Mogul period, who are known to have used at least three parallel reporting channels to survey their provinces with some degree of reliability, notwithstanding the additional efforts.

An additional motivation to revisit the Shannon Boolean analogy to communication systems in this work, comes from quantum mechanics. The classical system is important in considering the quantum analog, which then must not be a two-state system as today, while qubits are still used [5], even though interconnects are mentioned, and interconnects are in-band. It should also not be qutrits, or qudits, but a Galois field analogy with three or more logical states, as indicated here. The physical representations of quantum systems must be similar to the mathematical or computational aspects of quantum mechanics, as reviewed here, classically. Future quantum communication (and not just for raw computing power but significance) would then need some form of quantum equivalence of classical trust [4], for interconnects, and this is expected to be done through tri-state or more logical states — in correspondence with classical systems. And such is to be unique, as in complex analytic continuation [6], in the sense that knowing the value of it in some finite region, uniquely will determine the value at every other point. Information processing and communication has classically already replaced the Shannon two state Boolean logic with Verilog's three states (0, 1, Z) and

³ Trust works in a communication system, as that of which there is no doubt on what one knows in all the predicates of a sentence, as summarized by Frege [3] — namely in reference (name), sense (meaning), and entity (referent); e.g., that one knows (understands), that one knows (how to use), that one knows (where to find); see discussion in Section 2.

semantics of out-of-band interconnects, as further analysed in this work.

Lastly, another motivation for this work is found in CPSs (computer-physical systems), as modern robots. Trust is of modern consequence for robots and humans, and can no longer be ignored in a CPS, such as in self-driving vehicles, paramedical devices and heating strategy in buildings.

2. Trust analogy in communication

Trust is the problem. Understanding human trust is exactly what brought us to this great CS question in 1997 [7], which can also be marked as the start of CPSs: *how can one trust a set of bytes?* The answer, given here, provided a framework that has been tested and has been useful also in the fields of cybersecurity [7] and encryption with the AES (Advanced Encryption Standard), where it is particularly useful in translating computer data as they are represented in binary forms, using Galois extended fields $GF(2^m)$, as well-known.

The discussed framework allows one to use the concept of trust in a common heterogeneous environment, comprising humans and machines (CPSs), providing interconnects, where trust is understood exactly as what we humans call trust (e.g., as expected fulfillment of behavior) and bridges to machines in terms of qualified information based on factors independent of that information. One realizes that trust is essentially communicable, and that is why it can interconnect directly. But trust, as qualified reliance on information, needs multiple, independent channels to be communicated. If one has two entities (e.g., a client and a server) talking to one another, one has only one channel of communication. Clearly, one needs more than two entities. It seems unreasonable to require a hundred entities. Looking into millennia of human uses of trust, one realizes that one needs no more than four parties, in general, to induce trust (i.e., to communicate trust in a "clean slate" scenario): (1-2) the two parties in a dialogue, (3) at least one trusted introducer, and (4) at least one trusted witness.

For example, in German the word GIFT means poison, while the same word means gift in English. Those are fixed meanings in each culture. The meaning of the message cannot thus be ignored, nor can it be transmitted in-band, in the same channel, where it could possibly suffer risk under misuse, gaming, error or interference⁴. One must be absolutely certain about the meaning; no selection by the recipient should be possible, no possible gaming or fraud, and any selection can be correlated according to a precise system, which uses certain physical or conceptual entities, and no other.

Trusted introducers and trusted witnesses allow one to build two open-ended trust chains for every action, the witness chain providing the assurances ("how did we get here?") that led to the action (including the action itself) while the introducer chain ("where do we go from here?") provides the assurances both for a continuation of that action, for record-keeping, and for other actions that may need assurances stemming from it. One calls this principle the Trust Induction Principle: to induce trust, every action needs both a trusted introducer and a trusted witness, for a total of four parties.

Using Information Theory terminology, this paper defines this notion of trust as [7]:

"Trust is that which is essential to a communication channel but cannot be transferred from a source to a destination using that channel."

Here, a well-known theorem of topology [8] says that a generic one-to-one mapping

⁴ A similar situation happens between a bank's front-end office and back-office, where no surveillance of events has led to silent fraud, as well-known.

between spaces of different dimensionality must be discontinuous, in that a continuous path in one space must map into a broken path in the other. The consequences here are multiple, and this is being explored. Thus, the mathematical condition seems to imply the physical condition, and continuity, denied in one frame, is to be denied in all.

3. Tri-state versus two-state

Why does this matter? This work shows that, for the same function, computation can be accomplished better by using three logical states, which one can do experimentally using Verilog and tri-state, in communication systems — not two, not a mixture of 3 and 2, and not continuous. In an extension, we present theoretical reasons to obtain even better results with extended Galois fields $GF(3^n)$, using higher forms of three state logic, while maintaining a similar idea for the semantics, providing for out-of-band interconnects in a trust analogy.

A natural question is whether three-or-more valued logic systems can be embedded in a two-valued logical system. The answer is yes, according to this paper and Cobreros et. all. [9], but this paper does not stop there. As shown here in systems using Verilog versus early bipolar junction transistors [10], this would work at the expense of cost, speed, noise rejection and performance. Thus, it is known that scalability suffers with two-state.

The main motivations to use tri-state logic, as a ternary logic system, have been with Verilog [10], showing large qualitative improvements in computation and scalability, not realizability nor an immediate physical need.

As this Section will discuss, tri-state offers more discriminating channels than binary logic, allowing a much better resolution of indeterminate contributions, allowing them to be much better discriminated for and filtered. In this paradigm, everything helps — even noise. The noise is used to highlight the signal, which noise is considered to be too valuable to discard, bearing the result of previous processing (and cost).

Tri-state here is understood as:

1. 3-value logic, or ternary logic, in which there are three truth values indicating true, false, and some open-ended third value Z (indeterminate, e.g., as interconnects between different systems);
2. potentially including non-ergodic value variation;
3. including an open-ended number n of logical states, with n a natural number, using extended Galois fields $GF(3^n)$, as ramifications and branching out of the first Z level (e.g., ambivalent, trivalent, or obscure), without naming them;
4. both an ontic (i.e., relating to real existence, Natur) and an epistemic (i.e., informational, phenomenal, Wirklichkeit) interpretation.

Contrast with classical sentential or Boolean logic, that we consider has only one “true or false” ontic level, leading to two fixed epistemic levels.

To those who question that tri-state would be somehow “illogical” to consider, something in-between True and False, as in classical logic, in-between those two apparently tight adjacent logic levels — in unpublished notes, before 1910, Charles Sanders Peirce [11], however, soundly rejected the idea that all propositions must be either true or false. Peirce developed a semantics for what we are calling ternary logic, where the LEM is not valid, including some truth tables. A modern treatment can be seen in the results by Jones [12].

To implement three state logic and freedom from LEM, a possibility is a conventional

tri-state buffer or gate⁵, that exhibits three clear output states at a time [10]. But how to create a third state, if only two (on or off) seem possible? The answer is given in footnote 1, as the, at-first, ignored but necessary “don’t care” region.

The two-state logic levels are given below:

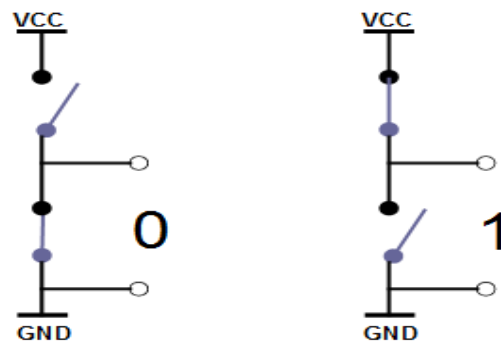


Figure 1. Example of two-state levels in a circuit, 0 and 1.

offering: (1) a low-level state “0” when the lower transistor in the totem-pole is on and the upper transistor is off; and (2) a high-level state “1” when the upper transistor in the totem-pole is on and the lower transistor is off.

The solution found for third logic level and implemented in Verilog [10], was to use an open circuit state “Z” or high-impedance state, that allows a direct wire connection of many outputs to a common line (i.e., a bus), exemplifying a programmable interconnect with the ability to move information between different systems that serve distinct tasks, which can be seen in the picture Fig.(2), showing the three cases of tri-state Verilog in positive logic:

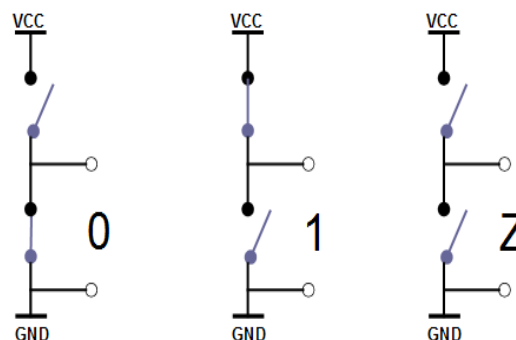


Figure 2. Example of three states logic: 0, 1, Z.

Using state Z to interconnect, information technologies, such as buffer or gate circuits, in challenge-response systems, can have a semantics [10,13] to connect to different systems, avoid race-conditions, handle faults, and maintain a coherent design. These aspects can be programmed dynamically at operation time, using tri-state implementations. The system uses a trust analogy, already introduced [4], which must operate out-of-band (for reasons cited in Section 2).

In classical systems with Verilog tri-state logic versus early bipolar junction transistors [10] one sees this design, which effectively [10,13] eliminates the Shannon two-state logic design [1] experimentally, reduces cost, and speed, improves noise rejection, and

⁵ Such as the 74LS241 octal buffer; a tri-state buffer can be thought of as an input controlled switch with an output that can be electronically turned “ON” or “OFF” by means of an external “Control” or “Enable” additional signal input.

enhances performance. This work provides the theoretical reasons for such improvements, relating them to higher logic levels and coherent semantics, which can be useful to CPS and quantum computing.

Information processing and communication are now majoritarily described by such ternary state systems and coherent bus semantics, driven by the Internet needs not just as raw computation but also in representation, in many classical systems such as FPGAs, ICs, CPUs, and others, and in multiple applications programmed using Verilog [10,13], with Verilog becoming an IEEE standard.

But this has also replaced in the field the Boolean algebra of a two-state system indicated by Shannon [1], mostly in gate construction with physical systems, with a trust analogy semantics (see Section 2) that allows a common bus to carry varying signals, in a coherent time. The primary reason, emerging from this Section, seems to be able to deal more effectively with noise.

4. Interconnections

Communication technology rests on a foundation built of interconnected information-processing systems, uniting very different systems that must nonetheless carry a common measure. This can be mathematically understood by the Curry-Howard relationship [14], a type of “worm hole” that bridges different logical systems, with different codes, one to the other, through common categories. The trust analogy (see Section 2), with its out-of-band transmission mode [4], is necessary for this function, which requires at least three logical states as in Fig.(2), not two as in Fig.(1), for communication.

The Internet has given us much more than a simple means of exchanging information worldwide with unprecedented ease, speed, availability and low cost, using two-state logic. A critical component of such systems is the “interconnect”, a device or process that allows transfer of information between disparate physical media, for example, semiconductor electronics, individual atoms, light pulses in optical fibers, satellite communications, or microwave fields. While interconnects have been well engineered for decades in the realm of classical information technology, they present special challenges, as they must allow the transfer of fragile states between different physical parts or degrees of freedom of the system. The diversity of platforms (TTL, tri-state, fluids, mechanical, electromagnetic, optical, etc.) that eventually forms a wider system poses additional challenges, reviewed in the last Section. In particular, the interconnection of “slow” and “fast” systems, or using online means of communication with varying delays and possible faults occurring at random or actively by an attacker.

The tri-state logic, and each implementation have benefits/drawbacks, however, has a more popular application in everyday devices than binary logic, or Shannon mode, where one can better see speed plus power savings, whereas with two-states we would have one model but sacrifice those benefits. As explained above, any three-valued logic system can be embedded in a two-valued logical system.

Yes, if they would be equal, or even equivalent at least, this would happen – and tri-state or two-state would be equivalent. But the states are in different dimensions, and a continuous path in the higher dimension (tri-state) would necessarily – must – map into a discontinuous path in the lower dimension (two-state). This happens due to a well-known theorem in topology [8].

This means that everything can be understood as causal with tri-state — even the unknown, the noise, in that indeterminacy. Three-valued logic (i.e., tri-state), besides contingency, reference failure, and vagueness, have been associated with at least three

other phenomena of interest in which the notion of *indeterminacy* plays a central role — namely conditionals, computability, and the semantic paradoxes [9]. Physically, atomic, molecular and ionic line formation itself, in matter, has been described, as well-known by Max Planck, in terms of three basic processes, namely as absorption, spontaneous emission, and stimulated emission — which can be mapped to three logical states by polymorphism. Additional processes are possible, considering collective effects, such as superradiance (Dicke) and superabsorption, motivating the consideration of more than three logical states ⁶.

The addition of a third truth value in ternary logic leads to a total of $3^3 = 27$ distinct operators on a single input value. The same operators with 2 inputs, result in a ternary logic with a *twenty thousand improvement*, offering more than 19K possibilities⁷, compared with only 16 distinct binary-logic operators reachable with 2 inputs. Thus, tri-state offers many more discriminating channels for a possible choice, than Boolean logic, allowing a better resolution of contributions.

Although, constructionally, one can conclude that a three-state system can always be embedded in a two-state system, following also Cobreros et. all. [9], efficiency and scalability suffers. This should be even more evident in computing, as more easily quantifiable.

Tri-state gates, in the Verilog choice [10,13], eliminate the need for open-collector gates in bus configurations, or multiplexers. The Curry–Howard isomorphism [14] then connects type theory with structural logic, creating a direct relationship between computer programs implemented by Verilog and mathematical proofs. A tri-state used for communication with Verilog [13] as a computing paradigm, is *evidence* for an ontic, modal logic with three states, as a good model for communication. It is also evidence that a Boolean logic system, such as following Shannon, is not sufficient for a communication system.

An important feature of most tri-state gates is that the output enable delay is longer than the output disable delay. If a control circuit enables one gate and disables another at the same time, the disabled gate enters the high-impedance state before the other gate is enabled. This eliminates the situation of both gates being active at the same time. There is a very small leakage current associated with the high-impedance condition in a tri-state gate. Nevertheless, this current is so small that as many as 100 tri-state outputs can be connected together to form a common-bus line.

Three states are needed also in election information systems, to represent the analogy of trust [4], not just with on/off bits of signal. See Section 2. Trust is not defined based on overly-defined variables, such as employer-employee relationships, beauty, power ⁸, age, authority, or pleasant stance. Here, trust is defined as in Section 2 and [4,7], with an Abstract Definition of Trust (ADT). Trust uses a parallel channel for communication, as routinely done in two-factor authentication (common today, but non existent before the ADT was first formulated, in 1998 [7]).

Not just Boolean logic states are, thus, needed for communication, as one needs e.g., meaning to rely on, e.g., that modern robots are represented as possible, without discontinuity, by humans, and vice versa. This is accomplished by sharing the same ADT, not the same information (information is measured by surprise, not by knowledge; false information exists [1]).

⁶ As allowed by $GF(3^n)$, offering 3, 9, 27, ... logical states.

⁷ i.e., $19683 = 3^{(3 \times 3)}$

⁸ Since the system's election purpose is often to define who will hold power, it must be impervious to its abuse.

Trust is what gives meaning to information [4], and allows information to be evaluated as true or false, or in-between (ambivalent, trivalent, obscure, and son on). For example, the same letters used for GIFT can mean “present” or “poison”, depending on one’s trust on the speaker’s language (English or German). Shannon arguments [1] do not even address this discrepancy which does not relate to information “in the wire”. See Section 2.

To wit:

1. The dimensionality of the real world, e.g., as information transfer, seems to be at least three (signal on/off and control), so discontinuity is harder to arise, which reduces the influence of errors;
2. the need to represent control (as trust) independently from the on/off signal can improve the signal, as well-known from classical systems, e.g., Carlson in [8].
3. The Einstein A and B coefficients of radiation model, in the Planck expression for black-body radiation, are related to the rates of spontaneous emission and absorption of light and the stimulated emission of light, all controlled by the intensity of light and resulting from coherent superposition as in Eq.(1), including in multi-photon pumping [15].
4. The formation of an atomic spectral line is thereby explained, including coherent contributions in providing and using energy [16].

5. Discussion

It would be desirable, therefore, to isolate those aspects of the current Information Theory that involve two-level logic, and are subject to modification by a more satisfactory theory, from aspects that involve only Galois field extended values offering three or more logic levels in $GF(3^n)$ and are thus relatively more trustworthy.

That seems to be the case of any Information Theory, not just that of Shannon; it seems that such theories cannot correctly describe the evolution of a physical system and CPS in terms of discrete variables of binary logic, but need richer logic states of dimensions three or higher, and coherent semantics providing the interconnects out-of-band, while the use of continuity is to continue to be deprecated.

Funding: This research received no external funding.

Acknowledgments: The author is indebted to André Gerck, Tiffany Gerck, and four anonymous reviewers. ResearchGate discussions were also used, for “live” feedback, important for interconnects, due to the physical isolation caused by COVID.

Conflicts of Interest: The authors declare no conflict of interest.

1. Shannon, C. E.. A mathematical theory of communication. Bell System Technical Journal, 27, 623–656, 1948.
2. R. Diaconescu. Axiom of choice and complementation. Proceedings of the American Mathematical Society, 51:176-178, 1975.
3. Frege, G.. “Sense and Reference”, howpublished = The Philosophical Review, vol. 57, no. 3, 1948, pp. 209–230, year=.
4. Gerck, E.. The Witness-Voting System. In Towards Trustworthy Elections, Springer Verlag, 27, p.1-36., 2010.
5. David Awschalom et al.. Development of Quantum Interconnects (QuICs) for Next-Generation Information Technologies. PRX Quantum 2, 017002, 2021.
6. Ahlfors, L. Complex Analysis. McGraw-Hill, Inc., 1979.
7. J. Feghhi, J. Feghhi and P. Williams. Trust Points, by Ed Gerck. In Digital Certificates: Applied Internet Security, Addison-Wesley, 1998.
8. Carlson, A. Buce. Communication Systems. McGraw Hill Kogakusha, Ltd., 1968.

-
9. Cobreros, P., Égré, P., Ripley, D., van Rooij, R.. Foreword: Three-valued logics and their applications. *Journal of Applied Non-Classical Logics*, 24:1-2, 1-11, <https://doi.org/10.1080/11663081.2014.909631>, 2014.
 10. M Morris, and Michael D , Ciletti. *Digital Design : with an Introduction to the Verilog HDL, VHDL, and SystemVerilog*, 2017.
 11. Anonymous reviewer. Private communication, 2021.
 12. Jones, D. W.. Standard Ternary Logic. <http://homepage.cs.uiowa.edu/~jones/ternary/logic.shtml>, 2016.
 13. Verilog. SystemVerilog is a standard hardware description and hardware verification language used to model, design, simulate, test and implement electronic systems. IEEE 1800, 2021.
 14. Girard, J.Y., Lafont, Y., and Taylor, P.. *Proofs and Types*. Cambridge University Press, 1989.
 15. Gerck, E., and Fill, E.. Blue-green atomic photodissociation lasers in group IIb: Zn, Cd, and Hg. *IEEE Journal of Quantum Electronics* 17(10):2140 - 2146, 1981.
 16. Gerck, E.. Quantum yields of I(2P_{1/2}) for CF₃I, C₂F₅I, i-C₃F₇I, n-C₃F₇I, n-C₆F₁₃I, and 1,2-C₂F₄I₂ at 308 and 248 nm. *The Journal of Chemical Physics* 79(1), 1983.