MARCELO SALHAB BROGLIATO

ESSAYS IN COMPUTATIONAL MANAGEMENT SCIENCE

ESSAYS IN COMPUTATIONAL MANAGEMENT SCIENCE

MARCELO SALHAB BROGLIATO

Escola Brasileira de Administração Pública e de Empresas
Fundação Getulio Vargas

January 2018

Marcelo Salhab Brogliato: *Essays in Computational Management Science,* © January 2018

SUPERVISORS:
Alexandre Linhares LOCATION:

Rio de Janeiro

ABSTRACT

Short summary of the contents in English...

RESUMO

Aqui entre o resumo...

Showing gratitude is one of the simplest yet most powerful things humans can do for each other.

— Randy Pausch, The Last Lecture

ACKNOWLEDGMENTS

Finally, thanks to everyone who helped me in any way, for each word, for caring, for your support in difficult moments and for all jokes and talks that made my days worthwhile. Surely this work was done thanks to all of you. After all, nobody does it alone!

CONTENTS

LIST OF TABLES

Part I

INTRODUCTION

1 INTRODUCTION

If anything good can ever be said about the second world war, it might be this: the war effort sparked a massive number of scientific fields.

Though most fields existed prior to the war, after the war they were funded by the public as strategic pieces of the major nations arsenal against future conflagrations. One of the fields in question was that of Management Science (also called Operations Research in military circles, as researchers filled the ranks of planners of war operations). Management Science had started as an industrial field, in movements stemming from Taylor and the origin of the production line by Henry Ford. That was the first moment in industry in which operations were systematically subject to some of the tools of science: measurement, experimentation, hypothesis-testing, statistics, mathematical optimization, etc.

This humble beginnings date from almost 100 years ago. Today the field has advanced to a great number of nations, and the amount of applications has grown explosively. Of particular interest to us is the advent of the computer, and of engineering efforts that brought exponential growth in computational power to the hands of individuals. Whilst, during the war, computations were mostly done by hand, the electronic computer took over afterwards; up to an extent that it is not outlandish to say that this original field can be referred to, today, as computational management science.

Applied mathematics and computer science serve simultaneously as a theoretical foundation and the major tool available to the field. Though this is a doctoral thesis concerning business, in this document one should expect to find the language and nomenclature of mathematical modeling and computer science as our primary and most natural language.

This thesis will present a number of different topics for exploration. Though the range of the topics is large, as it usually is in management science, it is my hope to convince readers of the value of this doctoral thesis brought by three specific, self-contained, scientific papers. The first of which studies the possibility of distributed financial ledgers.

1.1 DISTRIBUTED FINANCIAL LEDGERS

United Nations World Food Programme, 'Blockchain Against Hunger: Harnessing Technology In Support Of Syrian Refugees', 30

May 2017, https://www.wfp.org/news/news-release/blockchain-against-hunger-harnessing-technology-support-syrian-refugees, accessed in January 17, 2018.

United Nations World Food Programme, 2016, The Year in Review, Report.

Woyke, E., 2017, 'How blockchain can bring financial services to the poor', MIT Technology Review, April 18.

The World Bank estimates that there are two billion people without access to financial services. As banks are unable to sustain operations in numerous poverty-stricken areas, services such as money transfers, access to credit, digital/distant payments, inflation protection, etc., remain beyond reach for 'the unbanked'. This seems to be one of the factors that perpetuate poverty. The Bill and Melinda Gates Foundation chose as focus of its "Level-One project": to provide basic financial services through cell phones. Another initiative, the United Nations World Food Programme has began, in 2017, an experiment in Jordan, in which the organization provides funds for thousands of people towards its goal of food relief. An interesting aspect of this program has been the format of the funds distributed: they have been all on the ethereum blockchain.

The possibility of having a completely digital financial system without the overheads of traditional banking systems has appeared with the release of Bitcoin and similar blockchain technologies. This field questions numerous traditional assumptions in computer science, record-keeping, banking & finance, and economic inclusion. The seminal work of Nakamoto [51] described the architecture of Bitcoin, a peer-to-peer electronic cash system, also known as cryptocurrency. Bitcoin's currency ledger is public and stored in a blockchain across thousands of computers. Even so, no one is able to spend either somebody else's funds nor to double spend their own funds. In order to be confirmed, each transaction must be both digitally signed by the owner of the money and the funds verified in the blockchain by Bitcoin's miners. The question of whether Bitcoin (or related works) can scale to billions of people is, however, far from settled.

One of the interesting parts of Bitcoin are the incentives. On one hand, users have incentive to use Bitcoin because the fees are small, the money transfer is quick and global, and the currency issuance rate is well known. On the other hand, the miners have incentive to be part of Bitcoin's network because new coins are found every ten minutes. These incentives keep the community together and have maintened Bitcoin alive.

The impact of Bitcoin in society – and hence in the companies and the government – has been growing every day. People are increasingly using Bitcoin to exchange money and transfer money overseas. Companies are looking into Bitcoin as an alternative to

reduce banking fees. The poor may be included in the finance system through Bitcoin. People may hedge their assets against their governments' money issuance and inflation — as in the case of Venezuela.

Bitcoin is the first and most famous cryptocurrency, used worldwide, with a highly volatile market cap, as of this writing, of $ 192 bi. Even so, it faces serious scalability challenges; such as serious quality of service and network congestion when the number of transactions per second is high, and an increase in the transaction fees and uncertain delays in transactions' confirmations.

Note that these problems have been a deliberate decision from the current developers of the "bitcoin-core", which believe that is it risky to increase the the blocksize (in which all transactions are stored). It is not known whether a blocksize, say, of 1GB, would be feasible to sustain the decentralization of the network.

Iota is a second cryptocurrency that, instead of using a blockchain, proposes the use of a "tangle' architecture': a different way to register the currency ledger across thousands of computers. Although it has not been confirmed in practice yet, its architecture seems to be significantly more scalable than Bitcoin's blockchain. As we will see, the problem here is exactly the opposite of Bitcoin's. Iota needs a minimum of transactions per seconds in order to work properly.

Our analysis suggests an architecture for a distributed currency which is inspired in both Bitcoin's blockchain and Iota's tangle in order to solve the scalability problems. While Bitcoin's network saturates when it hits a certain number of transactions per second, Iota's does not work properly with less than a certain number of transactions per second. Our proposed architecture seems to work in both scenarios: low and high number of transactions per second.

In this first study we will investigate some issues regarding this possibility, namely: (i) cryptographic security and game-theoretical attacks; (ii) scalability; (iii) self-governance of the system; (iv) appropriate incentive system to all participants.

A second topic that may have an outsized influence on business and that we will be taking a closer look is a model of artificial intelligence.

1.2 ARTIFICIAL INTELLIGENCE

Technology has been one of the underlying engines behind economic growth. It has been changing the whole society – people, companies, and governments. Cities and houses had to be rethought when cars became popular. Trains allowed distant places to exchange high volume of goods. Airplanes and boats opened countries to overseas business. And, finally, the internet has had a

profound impact in nearly everyone's life, as it changed everything – from the way we communicate, behave, do business, do shopping, share ideas, and so forth.

One area of technology that has been redefining business is computer science. Together with the internet, computer science has been one of the most important tools to scale a business model – and create many others which were impossible before. More and more expensive human labor has been replaced by algorithms. Managers are able to make better decisions because they receive real time information. The supply chain has incredibly evolved thanks to advances in logistics supported by routing algorithms, storage algorithms, and many others optimization algorithms.

Artificial intelligence has been disrupting many businesses. Uber is able to handle hundred of thousands of requests. Amazon optimizes the location of each product based on demand. Netflix increases the quality of their services offering movies specific to the taste of each customer. Spotify learns which kind of music users like the most and suggests playlists. Banks prevent fraud classifying which patterns are strange to their customers.

It is gradually becoming impossible to imagine a world without artificial intelligence.

Behind many artificial intelligence systems, there is pattern recognition: The capacity to match information from new data with information which has already been seen and is stored in memory. It may be used in classification, face recognition, character recognition, and so forth.

The second paper lies at the intersection of cognitive psychology, computer science, neuroscience, and artificial intelligence. Sparse Distributed Memory, or SDM for short, is a theoretical mathematical construct that seems to reflect a number of neuroscientific and psychologically plausible characteristics of a human memory. SDM has already been used to different pattern recognition problems, like noise reduction, handwriting recognition, robot automation, and so forth.

We implement a RB-Complete[1] SDM framework that not only shows small discrepancies from previous theoretical expectations, but also may be of use to other researchers interested in testing their own hypotheses and theories of SDM. The computer code has been used in a previous Ph.D. Thesis; the code has shown some small discrepancies from theoretical expectations; the code has been ran on a number of different architectures and information-processing devices (e.g., CPUs, GPUs). We also reproduce previous experiments and present new possibilities for SDM.

1 'Ridiculously Buzzword Complete: the model is (i) Open-Source, (ii) Cross-Platform; (iii) highly parallel; (iv) able to execute on CPUs and/or GPUs; (v) it can be run on the 'cloud'; etc.

1.3 DIFFUSION OF INNOVATION

In 2014, a group of Princeton's researchers predicted that Facebook's users would abandon the platform by 2017 [18]. The forecast was done applying a disease spreading model which has correctly predicted the abandonment of "MySpace". Facebook replied applying exactly the same methodology as Princeton's researchers. In their own words: "Using the same robust methodology featured in [Princeton's] paper, we attempted to find out more about this 'Princeton University' – and you won't believe what we found!". Then, they conclude: "This trend suggests that Princeton will have only half its current enrollment by 2018, and by 2021 it will have no students at all, agreeing with the previous graph of scholarly scholarliness. Based on our robust scientific analysis, future generations will only be able to imagine this now-rubble institution that once walked this earth".

Whilst this brouhaha reminds one of the dangers of extrapolation, our third paper will revisit the prospects of our esteemed colleagues in Facebook. Lying at the intersection of Marketing, Diffusion of Technological Innovation, and modeling, the Bass model of diffusion of innovation will be extended, in order to account for users who, after adopting the innovation for a while, decide to reject it later on (possibly bringing down the number of active users—something impossible in Bass' original model). Four alternative mathematical models are presented and discussed with the Facebook's users dataset.

1.4 THE FINE PRINT...

Before embarking on the technical topics, small qualifications must be asked from my readers. First, as stated above, though these problems have immense and urgent importance to the fields of study in business, the language in which we will approach them and discuss them most naturally will be that of mathematics and computer science. There will not be surveys, interviews, questionnaires, or such methods typically used in the social sciences: This is basically a work of modeling.

A second and final qualification: It is my hope that readers of this thesis will accept the format of self-contained studies, as just as valid as a monograph on a particular topic. With these qualifications, we are ready to venture into the world of computational management science.

Part II

AN ALTERNATIVE STRUCTURE TO A BLOCKCHAIN: CONFIRMATIONS WITHOUT BLOCKS

2 INTRODUCTION

The main problem when one is trying to create a digital money is how to prevent double spending. As the money is digital, and copies can be made *ad nauseam*, what can prevent counterfeiting? That is, what would prevent users from sending copies of the same money to two (or more) people? That is exactly the problem solved by Bitcoin and its underlying blockchain technology. The current solution behind fiat money is having a single issuer, a central bank, and trusting the financial institutions.

Bitcoin (BTC) is the first digital currency, also known as digital money, internet money, and cryptocurrency. It is the first currency based on cryptography techniques, distributed and decentralized, and with no central bank. Bitcoin is distributed since its ledger is public and is stored in thousands of computers. It is decentralized because there is no authority (or government) who decides its future — any decision must be accepted by its community. The security of Bitcoin relies on digital signature technology and network agreement. While digital signature ensures ownership, i.e., the funds may only be spend by their owners, and nobody else; the network agreement both prevents double spending and ensures that all processed transactions have sufficient funds. In short, every transaction must spend only unspent funds, must have enough funds available, and must be signed by its owners, authorizing its execution. When all these requirements are met, the funds are transfered.

According to Barber et al. [6], despite the 30-year literature on e-cash, most of the proposed schemes requires a central authority which controls the currency issuance and prevents double spending. The no central point of trust and predictable money supply together with a clever solution to the double spending problem is what separates Bitcoin from the previous e-cash philosophies.

Bitcoin provides interesting incentives to all players, namely the users and the miners. On one hand, users may have incentives to use Bitcoin because of the following: (i) the fees are small and does not depend on the amount being transfered — but only in the size (in bytes) of the transaction — (ii) the transfers will be confirmed in a well-known period; (iii) it is not possible to revert an already confirmed transfer, not even with a judicial order; and (iv) and the currency issuance rate is well-known and preset in Bitcoin's rules, which makes the Bitcoin supply predictable and trustworthy, different from fiat currencies which depends on decisions of their

central banks — i.e., it would be virtually impossible to face a hyper inflation in Bitcoin due to currency issuance. On the other hand, miners have incentive to mine Bitcoin because new Bitcoins are found every ten minutes and they may also receive the fees of unconfirmed transactions. These incentives have kept the Bitcoin network up and running since 2009 with barely no interruptions (99.99% uptime).

Since 2009, Bitcoin has been growing and becoming more and more used all around the world. It started as an experiment based in a seminal work by Nakamoto [51] and expanded to the most important and successful cryptocurrency with a highly volatile $192 billion market capitalization, as of this writing [23]. There are hundreds of companies investing in different uses of the technology, from exchanges to debit cards, and billions of dollars being invested in the new markets based on Bitcoin's technology.

Despite Bitcoin's huge success, there are still many challenges to be overcome. We will focus on a specific subset of those challenges, namely the scaling, decentralization, and spam challenges. One important challenge that we will skip is to reduce the size of the ledger (or blockchain), which today is around 125GB and is growing at a rate of 4.5GB per month [11].

The network must scale to support hundreds of transactions per second, while its capacity is around only eight transactions per second. Thus, the more Bitcoin becomes popular, the more saturated the network is. Network saturation has many side effects and may affect the players incentive to keep the network running. The transaction fees have to be increased to compete for faster confirmation. The pool of unconfirmed transactions grows indefinitely, which may cause some transactions to be discarded due to low memory space available, as the previously predictable confirmation time of transactions becomes unpredictable.

Bitcoin seems to have the most decentralized network between the cryptocurrencies, even so there are few miners and mining pools which together control over 50% of the network's computing (hash)power. Thus, they have an oversized influence when it comes to changes in the Bitcoin protocol's behaviour, and it is also seen as a problem to be solved. The more decentralized, the more trustworthy Bitcoin is.

Generating new transactions in Bitcoin has a tiny cost, because one only has to generate the transaction itself, digitally sign it, and propagate in the Bitcoin network. On one hand, it means that any device is capable of generating new transactions, but, on the other hand, it makes Bitcoin susceptible to spam attacks. One may generate hundreds of thousands of new valid transactions, overloading the unconfirmed transactions pool and saturating the network.

The number of ideas and publications focusing in improving Bitcoin's design and overcoming those challenges is increasing every day. Many of these proposals are organized into BIPs (Bitcoin Improvement Proposals) which are discussed and implemented by the community; while others come in the form of whitepapers and alternative software forks (which would include the need of a protocol upgrade). Other proposals are published in blogs and forums, describing new cryptocurrencies. Bitcoin's community hardly ever publishes their ideas in academic journals, preferring instead, of BIPs, white papers, and web discussions.

After the launch of Bitcoin, more than 1,000 other cryptocurrencies has been created (REF). In general, they are Bitcoin-like, which means they use similar technologies, including the blockchain. Some cryptocurrencies differs a lot from Bitcoin, like the ones which use the DAG model [29, 62, 44, 71, 45, 74]. We are specially interested in one of them: Iota.

Iota uses a DAG model, called tangle, which has a different design than Bitcoin's blockchain. It has neither mining nor confirmation blocks and transaction fees. Each transaction has its own proof-of-work, and is used to confirm other transactions forming a directed acyclic graph. In Iota, as transactions confirm transactions, the network benefits from a high volume of new transactions. Hence, theoretically, it scales to any large number of transactions per second. The scaling problem of tangle is exactly the opposite of Bitcoin's. It must have at least a given number of transaction per seconds, otherwise the transactions are not confirmed and the cryptocurrency does not work.

The present work intends to analyze a new architecture which lies between Bitcoin and Iota and may be a viable solution to both Bitcoin's scaling, centralization, and spam problems. We also present a mathematical analysis of Bitcoin's mining, forking, and safety.

3

BITCOIN & BLOCKCHAIN

In Nakamoto's (2009) seminal paper, there is no distinction between bitcoin and blockchain. They are just one thing which solves an important theoretical problem: how to create a distributed and decentralized digital form of hard money in the internet, in which all users can agree as to whom is entitled to which funds.

But, in practice, it is interesting to separate these concepts. Bitcoin uses the blockchain technology to create a distributed ledger, while the blockchain is a technology which allows information to be stored in an immutable and distributed way.

The blockchain technology works through the creation of new blocks. Each new block confirms that all the previous blocks are valid and have not been tampered with. The mechanism that assures the immutability is proof-of-work, which makes it computationally infeasible to tamper with previous transaction records without having to recalculate all the previous proof-of-works faster than all of the remaining machines of the network.

The proof-of-work is a mathematical problem with the following characteristics: (i) it is hard to find a solution; (ii) this hardness level may be adjusted; and (iii) it is fast to check whether the proposed solution is correct.

Bitcoin's blockchain uses the mathematical problem of finding a random number which, after being applied to the hash function SHA-256 twice, results in a number smaller than a given threshold A. As SHA-256 is a pseudo-random function, its output is uniformly distributed between 0 and $2^{256} - 1$ [35]. Thus, if the given number is $A = 2^{255}$, one has probability 50% of finding a solution (just the most significant bit of the hash needs to be zero). But if the given number is $A = 2^{240}$, one has probability 0.0015% of finding a solution (as the 16 most significant bits of the hash must equal zero). Hence, finding a solution is a hard problem which difficulty depends on the given number A. The lesser the given threshold A, the higher the difficulty. On the other side, checking whether a solution is correct is fast, one just has to apply the SHA-256 twice and compare.

By design, Bitcoin's blockchain proof-of-work difficulty is dynamically adjusted every 2016 blocks to keep an average pace of 10 minutes between block creation. Thus, the goal is to adjust the difficulty every 14 days. If it takes less than 14 days to find 2016 blocks, that means the network's hash power has increased, thus the difficulty is increased. If it takes more than 14 days to find 2016

blocks, it means the network's hash power has decreased, thus the difficulty is decreased.

When miners are finding a solution to a new block, they are mining or working in the new block. A block is found when a solution to the proof-of-work is found. Two miners may find blocks in a small interval of time. In this case, both will propagate their blocks and the network will randomly choose one of them as the next block. This phenomenon is called a fork. Thus, when the next block is found, one of those blocks will be confirmed and the other will be ignored and referred to as an orphan block. The network agrees that work should be done in the block at the longest chain in the blockchain. When a new block is found, it indirectly confirms all the previous blocks in the chain and their transactions.

Newly propagated blocks are validated by the Bitcoin's network. If the solution of the proof-of-work is incorrect or if any transaction included in the block has any issue, then the block is discarded. In order to work properly, the whole network must agree in what is allowed and what is not. Should one think that something should be allowed and accept it in their blocks, the remaining of the network will discard their newly propagated blocks. That is why Bitcoin's network is distributed and decentralized. Everything depends on the agreement of the network, or, precisely, the agreement of the owners of at least 50% of the hash power. Even if the remaining 49% disagrees, the 50% or more who agree will generate, on average, more blocks than the remaining of the network and their rules will prevail on the longest chain. If a disagreement between miners' rules happens, that is referred as either a hard-fork or a soft-fork (in general, a hard-fork relaxes the constraints, while the latter hardens them).

For instance, no group with more than 50% of the network's hash power agreed into increasing the maximum block size to increase the number of transactions confirmed by a block, and thus increasing the network's capacity. Thus, the capacity remains the same and the community has been discussing the issue in search of a consensus.

Bitcoin uses the blockchain technology to create a distributed ledger. It allows every new block to generate new bitcoins and also to collect the fees from the confirmed transactions within the block. Bitcoin's transactions have two main parts: (i) inputs, and (ii) outputs. Each transaction sends bitcoins from one or more input addresses to one or more output addresses. In order to prove that one is the owner of the input bitcoins, one must digitally sign the transaction proving such ownership.

The digital signature scheme used by Bitcoin is based on a pair of private and public keys. The private key is used to sign the transaction, while the public key is used to check whether the signature is valid. Thus, the owner of some Bitcoin funds is, in fact,

the owner of a pair of private and public keys. The private key must never be publicly published, as whoever has access to the private key is able to spend its funds. In other words, in order to protect their funds, the owners must protect the private key. If one loses their private key, unfortunately, access to their funds will be lost forever. The public key may be used to a proof-of-ownership, i.e., one may publish the public key with some message digitally signed by the private key, proving that he/she is the owner of the funds.

Bitcoins (BTCs) owned by someone are, in fact, unspent outputs in one or more transactions. For instance, one may have 6 BTCs spread between three transactions' unspent output: the first with 1 BTC, the second with 2 BTCs, and the third with 3 BTCs.

In a transaction, the inputs are pointers to other transactions' outputs (which they are spending). A transaction output may only be spent once and thus may not be partially spent. For instance, when one has 3 BTCs in one transaction output and would like to send 1 BTC to a friend, they have to create a transaction with one input spending the 3 BTCs and two outputs, one for the friend with 1 BTC and one's change with 2 BTCs.

Each transaction's output has a script that is executed by the miners to check whether one has or has not permission to spend that output. In other words, whether one has the ownership of that output. In order to execute these scripts, the miners also need some data. This data is given by the transaction which is spending the output.

The output's scripts usually checks whether the public key is valid and whether the digital signature was signed by the private key associated to that public key. Although there are only 3 commonly used scripts, one may create a custom script using the Bitcoin's script language [1].

The input contains the data which prove that the sender is the owner of the referred outputs, i.e., the input which must be accepted by the output scripts being spent. Usually, each input has the public key of the sender and a digital signature.

Those users accustomed to block explorers may have been misled by the transaction information that these websites provide. For example, suppose a miner receives a transaction with "one input from address A1". This "one input" actually consists of a pointer to a previous unspent output (i.e., there is no "input" address, as is displayed, but only a pointer). This pointer reference allows lookup to be executed in $O(1)$ time.

After lookup, the miner knows how many BTC tokens are available at that unspent output. But, in order to certify ownership of that output, the miner receives instructions in the form of a script

1 Your courageous author once tried to make a transaction with custom script to try to double spend a deposit to an exchange, only to learn through this intrepid adventure that Bitcoin allows only 3 script patterns and the others are treated as invalid.

with the rules that lead to the desired unspent output address (and this one is displayed as the input address by those websites). Because this process requires a digital signature, only the holder of the corresponding private key is able to sign such a transaction.

Next we will do a mathematical analysis of Bitcoin in order to deeply understand its minings properties, how a fork would affect the network, and its security against attackers.

4

ANALYSIS OF BITCOIN

4.1 HASH FUNCTION

Hash functions has been widely studied in computer science. In short, a hash function $h : \{0,1\}^\infty \to \{0,1\}^n$ has the following properties:

1. $x = y \Rightarrow h(x) = h(y)$
2. $h(x) \sim \mathcal{U}(0, 2^n - 1)$, where $\mathcal{U}$ is the uniform distribution, i.e., $\forall a \in [0, 2^n - 1], \mathbf{P}(h(x) = a) = \frac{1}{2^n}$

In other words, when two inputs are the same, they have the same output. But, when the inputs are different, their outputs are uniformly distributed. Clearly, the hash functions are surjective but not injective. They are not injective because the image of h has only 2^n elements and the domain has infinite elements. When $x \neq y$ and $h(x) = h(y)$, we say that x and y are a collision. A hash function is considered to be safe when it is unknown how to find a collision of a given hash.

Bitcoin uses two hash functions: HASH-160 and HASH-256. The first has $n = 160$ and consists of the composition of *SHA-256* and *RIPEMD-160*. The latter has $n = 256$ and applies *SHA-256* twice.

For further information, see Gilbert and Handschuh [35], Dobbertin et al. [30].

4.2 MINING ONE BLOCK

Let $\mathbb{B}$ be the set of Bitcoin blocks and $h : \mathbb{B} \to \{0,1\}^{256}$ be the Bitcoin *HASH-256* function. The mining process consists of finding $x \in \mathbb{B}$ such as $h(x) < A$, where A is a given threshold. The smaller the A, the harder to find a new block. In fact, $\mathbf{P}(h(x) < A) = \frac{A}{2^{256}}$.

Hence, in order to find a new block, one must try different inputs $(x_1, x_2, \ldots, x_k)$ until they find a solution, i.e., all attempts will fail ($h(x_i) \geqslant A$ for $i < k$) but the last ($h(x_k) < A$). The probability of finding a solution exactly in the k^{th} attempt follows a geometric distribution. Let X be the number of attempts until a success, then $\mathbf{P}(X = k) = (1-p)^{k-1}p$, where $p = \frac{A}{2^{256}}$. Also, we have $\mathbf{P}(X \leqslant k) = 1 - (1-p)^k$. The average number of attempts is $\mathbf{E}(X) = 1/p$ and the variance is $\mathbf{V}(X) = \frac{1-p}{p^2}$.

In the Bitcoin's protocol, the given number A is adjusted so that the network would find a new a block every 10 minutes, on average. Suppose that the Bitcoin's network is able to calculate H hashes per

second — H is the total hash rate of the network. The time required to find a solution would be $T = X/H$, and $\mathbf{E}(T) = \mathbf{E}(X)/H$ would be the average number of seconds to find a new block. So, the rule of finding a new block every 10 minutes ($\eta = 600$ seconds) — on average — leads to the following equation: $\mathbf{E}(T) = \eta = 600$. So, $\mathbf{E}(T) = \mathbf{E}(X)/H = \frac{1}{pH} = \eta = 600 \Rightarrow p = \frac{1}{\eta H}$. Finally, $\mathbf{E}(X) = \eta H$, $\mathbf{E}(T) = \eta$, $\mathbf{V}(X) = (\eta H)^2 - \eta H$, and $\mathbf{V}(T) = \eta^2 - \eta/H$.

The cumulative distribution function (CDF) of T is $\mathbf{P}(T \leqslant t) = \mathbf{P}(X/H \leqslant t) = \mathbf{P}(X \leqslant tH) = 1 - (1-p)^{tH} = 1 - \left(1 - \frac{1}{\eta H}\right)^{tH}$. But, as the Bitcoin's network hash rate is really large, we may approximate the CDF of T by $\lim_{H\to\infty} \mathbf{P}(T \leqslant t) = 1 - e^{-\frac{t}{\eta}}$, which is equal to the CDF of the exponential distribution with parameter $\lambda = \frac{1}{\eta}$.

Theorem 1. *When $H \to +\infty$, the time between blocks follows an exponential distribution with parameter $\lambda = \frac{1}{\eta}$, i.e., $\lim_{H\to+\infty} \mathbf{P}(T \leqslant t) = 1 - e^{-\frac{t}{\eta}}$.*

Proof.

$$\begin{aligned}\mathbf{P}(T \leqslant t) &= 1 - (1-p)^{tH} \\ &= 1 - \left(1 - \frac{1}{\eta H}\right)^{tH}\end{aligned}$$

Replacing $u = \eta H$,

$$\begin{aligned}\lim_{H\to+\infty} \mathbf{P}(T \leqslant t) &= \lim_{u\to+\infty} 1 - \left(1 - \frac{1}{u}\right)^{\frac{tu}{\eta}} \\ &= \lim_{u\to+\infty} 1 - \left[\left(1 - \frac{1}{u}\right)^{u}\right]^{\frac{t}{\eta}} \\ &= 1 - (1/e)^{\frac{t}{\eta}} \\ &= 1 - e^{-\frac{t}{\eta}}\end{aligned}$$

□

Now, we would like to understand from which value of H it is reasonable to assume that T follows an exponential distribution.

Theorem 2. $x > M \Rightarrow |(1 + 1/x)^x - e| < e/M$.

Proof. Let's use the classical inequality $\frac{x}{1+x} < \log(1+x) < x$ for $x > -1$. So, $\frac{1/x}{1+1/x} < \log(1+x) < 1/x$. Simplifying, $\frac{1/x}{1+1/x} = 1/(1+x)$. Thus, $1/(1+x) < \log(1+1/x) < 1/x \Rightarrow x/(1+x) < x\log(1+1/x) < 1$.

As $\log(1 + \frac{1}{M}) > 0$ and $1 < 1 + \log(1 + \frac{1}{M})$.

$x > M \Rightarrow 1/x < 1/M \Rightarrow 1 + 1/x < 1 + 1/M \Rightarrow 1/(1 + 1/x) > 1/(1 + 1/M) \Rightarrow x/(1+x) > M/(1+M)$.

Again, $\log(1+x) < x \Rightarrow \log(1 - 1/M) < -1/M \Rightarrow 1 + \log(1 - 1/M) < (M-1)/M < M/(1+M)$, since $(x-1)/x < x/(x+1)$.

Hence, $1+\log(1-1/M) < M/(1+M) < x/(1+x) < x\log(1+1/x)$, and $x\log(1+1/x) < 1 < 1+\log(1+\frac{1}{M})$.

Finally,

$$
\begin{aligned}
1+\log(1-1/M) &< x\log(1+1/x) < 1+\log(1+\frac{1}{M}) \\
e^{1+\log(1-1/M)} &< e^{x\log(1+1/x)} < e^{1+\log(1+\frac{1}{M})} \\
e\cdot e^{\log(1-1/M)} &< e^{\log((1+1/x)^x)} < e\cdot e^{\log(1+\frac{1}{M})} \\
e(1-1/M) &< (1+1/x)^x < e(1+\frac{1}{M}) \\
e-e/M &< (1+1/x)^x < e+e/M \\
-e/M &< (1+1/x)^x - e < e/M
\end{aligned}
$$

Therefore, $|(1+1/x)^x - e| < e/M$. □

We may consider H big enough to say that T follows an exponential distribution when $e/H < \epsilon$, where ϵ is the maximum approximation error. When $\epsilon = 10^{-6} \Rightarrow H > e\cdot 10^6$. So, when $H > 2.6$Mh/s, our approximation is good enough.

The symmetrical confidence interval with level α would be $[t_0, t_1]$, where $\mathbf{P}(t_0 < T < t_1) = 1-\alpha$, $\mathbf{P}(T < t_0) = \alpha/2$, and $\mathbf{P}(T > t_1) = \alpha/2$. These conditions give the following equations: $1-e^{-t_0/\eta} = \alpha/2$, and $e^{-t_1/\eta} = \alpha/2$. Solving these equations, we have $t_0 = -\eta\ln(1-\alpha/2)$, and $t_1 = -\eta\ln(\alpha/2)$.

For instance, if $\alpha = 10\%$, then $t_0 = 30.77$ and $t_1 = 1797.44$ (or $[0.51, 30.76]$ in minutes). Thus, 90% of the time the intervals between blocks are between 30 seconds and 30 minutes.

The fact that the time between blocks follows an exponential distribution with $\lambda = 1/\eta = pH$ may be used to estimate the total network's hash rate (or a miner's hash rate). For further information, see [58].

4.3 MINING SEVERAL BLOCKS

Let $T_1, T_2, T_3, \ldots, T_n$ be the time to find the first block (T_1), then the time to find the second block (T_2), and so on. Let's analyze the distribution of $Y_n = \sum_{i=1}^{n} T_i$. As Y_n is the sum of random variables which follow an exponential distribution with same $\lambda = \frac{1}{\eta}$, then $Y_n \sim \text{Erlang}(n, \frac{1}{\eta})$. Thus, the CDF of Y would be $\mathbf{P}(Y_n < t) = 1 - \sum_{k=0}^{n-1} \frac{1}{k!} e^{-\lambda t}(\lambda t)^k$.

Many exchanges require at least six confirmations in order to accept a deposit in Bitcoin. So, for $n = 6$, $\mathbf{P}(Y_6 < 1\,\text{hour}) = \mathbf{P}(Y_6 < 3600) = 0.5543$. The symmetrical confidence interval with $\alpha = 10\%$ is $[27, 105]$ in minutes. Thus, 90%

of the times, it will take between 27 minutes and 1 hour and 45 minutes to have your deposit accepted — assuming that your transaction will be confirmed in the very next block. The pdf of Y_6 is shown in Figure 1. The 10% symmetrical confidence interval is shown in the white area.

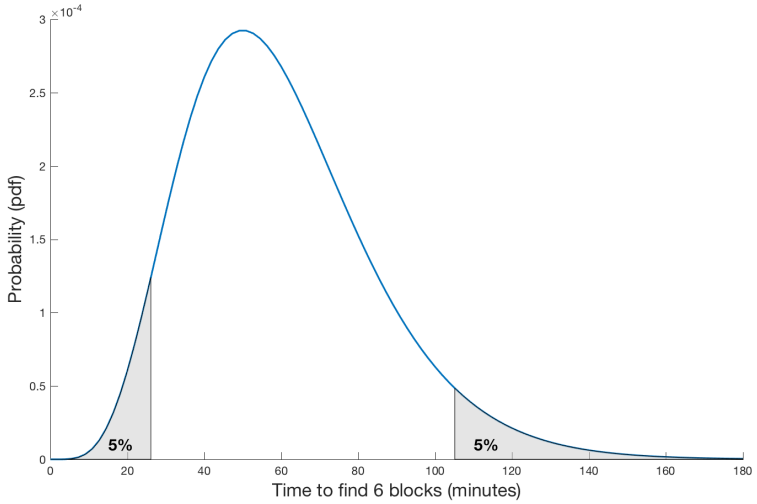


Figure 1: Probability density function of Y_6, i.e., probability of finding 6 blocks after time t. The shaded areas shows the lower 5% and upper 5% of the pdf.

4.4 MINING FOR A MINER

Let's analyze the probability of finding a new block for a miner who has α percent of the network's total hash rate. Let $T_\alpha = \frac{X}{\alpha H}$ be the time required for the miner to find a new block. As $T_\alpha = \left(\frac{1}{\alpha}\right) T$, when $H \to +\infty$, T_α also follows an exponential with parameter $\lambda_\alpha = \frac{\alpha}{\eta}$. Hence, we confirm the intuition that the miner with α percent of the network's total hash power will find α percent of the blocks.

Theorem 3. *When the miner with α percent of the network's total hash rate is part of the mining network,* $\mathbf{P}$*(next block is from* $T_\alpha) = \alpha$.

Proof.

$$\begin{aligned}
\mathbf{P}(\text{next block is from } T_\alpha) &= P\left(T_\alpha = \min\{T_\alpha, T_{1-\alpha}\}\right) \\
&= \frac{\lambda_\alpha}{\lambda_\alpha + \lambda_{1-\alpha}} \\
&= \frac{\alpha/\eta}{\alpha/\eta + (1-\alpha)/\eta} \\
&= \frac{\alpha}{\alpha + 1 - \alpha} \\
&= \alpha.
\end{aligned}$$

□

Theorem 4. *When one miner with α percent of the network's total hash rate multiplies their hash rate by m, the probability of this miner find the next block is multiplied by $\frac{m}{m\alpha+1-\alpha}$.*

Proof. When miners increase their hash rate, they also increase the network's total hash rate. Let H be the network's hash rate before the increase. Thus, the network's total hash rate after the increase is $H + (m-1)\alpha H = (1-\alpha+m\alpha)H$. So,

$$\begin{aligned}
\mathbf{P}(\text{next block is from } T_{m\alpha}) &= P\left(T_{m\alpha} = \min\{T_{m\alpha}, T_{1-\alpha}\}\right) \\
&= \frac{\lambda_{m\alpha}}{\lambda_{m\alpha} + \lambda_{1-\alpha}} \\
&= \frac{m\alpha/\eta}{m\alpha/\eta + (1-\alpha)/\eta} \\
&= \frac{m\alpha}{m\alpha + 1 - \alpha} \\
&= \alpha\left(\frac{m}{m\alpha + 1 - \alpha}\right).
\end{aligned}$$

□

Corollary. *If one miner has a really tiny percent of the network's total hash rate, then multiplying their hash rate by m approximately multiplies their probability of finding the next block by m.*

Proof.

$$\lim_{\alpha\to 0} \mathbf{P}(\text{next block is from } T_{m\alpha}) = \lim_{\alpha\to 0} \frac{m}{m\alpha + 1 - \alpha} = m.$$

□

That way, it is not exactly correct to say that when one doubles their hash rate, their probability will double as well. It is only true for small miners.

4.5 ORPHAN BLOCKS

An orphan block would be created if a new block is found during the propagation time of a new block. Let α be the percentage of the total hash rate of the node which is outdated, and Δt the propagation time in seconds. Thus, $\mathbf{P}(\text{new orphan}) = \mathbf{P}(T < \Delta t) = 1 - e^{-\frac{\alpha\Delta t}{\eta}}$. For instance, if a node has 10% of the total hash rate and it takes 30 seconds to receive the update, then $\mathbf{P}(\text{new orphan}) = 1 - e^{-\frac{0.1\cdot 30}{600}} = 0.004987$.

4.6 ANALYSIS OF NETWORK'S HASH RATE CHANGE

The difficulty, given by the number A, is adjusted every 2016 blocks. As, $\mathbf{P}(13 \text{ days} < Y_{2016} < 15 \text{ days}) = \mathbf{P}(13 \cdot 24 \cdot 3600 < Y_{2016} < 14 \cdot 24 \cdot 3600) = 0.9986$, it is expected that the total time to find 2016 blocks will be between 13 and 15 days, assuming that the network's hash rate remains constant. If it takes less than the expected time, it means that the network's total hash rate has increased. While if it takes more than the expected time, it means that the network's total hash rate has decreased. So, let's analyze what happens when the network's hash rate changes significantly.

Let $H \cdot u(t)$ be the network's total hash rate over time. So, the number of hashes calculated in t seconds is $H\int_0^t u(t)dt$. Hence, $\mathbf{P}(T \leqslant t) = \mathbf{P}(X \leqslant H\int_0^t u(t)dt)$. When $H \to +\infty$, $\mathbf{P}(T \leqslant t) = 1 - e^{-\frac{1}{\eta}\int_0^t u(t)dt}$, and the pdf of T is $\frac{u(t)}{\eta} \cdot e^{-\frac{1}{\eta}\int_0^t u(t)dt}$.

Let's say that the network's total hash rate has suddenly multiplied by α. So, $u(t) = \alpha$, $\int_0^t u(t)dt = \alpha t$, and T also follows an exponential distribution, but with $\lambda = \frac{\alpha}{\eta}$. Thus, $Y_n^\alpha = \sum_{i=1}^n T_i^\alpha \sim \text{Erlang}(n, \frac{\alpha}{\eta})$. Thus, $\mathbf{E}[Y_n^\alpha] = \frac{\mathbf{E}[Y_n]}{\alpha}$, i.e., the average total time required to find n blocks will be divided by α, while $\mathbf{V}[Y_n^\alpha] = \frac{\mathbf{V}[Y_n]}{\alpha^2}$ and the variance will be divided by α^2. Hence, on one hand, when the network's hash rate increases ($\alpha > 1$), the 2016 blocks will be found earlier. On the other hand, when the network's hash rate decreases ($\alpha < 1$), the 2016 blocks will be found later.

For example, if the network's total hash rate suddenly doubles ($\alpha = 2$), then $\mathbf{P}(6.5 \text{ days} < Y_{2016} < 7.5 \text{ days}) = 0.9986$, and the time required to find 2016 blocks halved. On the other side, if the network's total hash rate suddenly halves ($\alpha = 0.5$), then $\mathbf{P}(27 \text{ days} < Y_{2016} < 29 \text{ days}) = 0.9469$, and the time required to find 2016 blocks doubled. It is an important conclusion, since it shows that even if half of the network stops mining, it will only double the time to the next difficulty adjustment, i.e., the time between blocks will be 20 minutes for, at most, the next 29 days, at which point the adjustment will occur and everything will be back to the normal 10 minutes between blocks.

4.6.1 *Hash rate smoothly changing*

Let $u(t) = \frac{1+abx}{1+bx}$. It is an useful function because $u(0) = 1$ and $\lim_{t\to\infty} u(t) = a$. The bigger the b, the faster $u(t) \to a$. For example, if $a = 2$, it means H would be smoothly doubling. If $a = 0.5$, it means H would be smoothly halving.

It is easy to integrate $u(t)$ because $\frac{1+abx}{1+bx} = \frac{1-a}{1+bx} + a \Rightarrow \int_0^t u(x)dx = at + \frac{1-a}{b}\log(1+bt)$. So,

$$F_T(t) = 1 - (1+bt)^{\frac{\lambda(a-1)}{b}} e^{-\lambda a t}.$$

$$f_T(t) = \lambda \left(\frac{1+abt}{1+bt} \right) (1+bt)^{\frac{\lambda(a-1)}{b}} e^{-\lambda a t}.$$

Assuming that $n = \frac{\lambda(a-1)}{b}$ is integer, we have:

$$F_T(t) = 1 - (1+bt)^n e^{-\lambda a t}$$

Thus,

$$\begin{aligned}
\mathcal{L}\{F_T(t)\} &= \mathcal{L}\{1 - (1+bt)^n e^{-\lambda a t}\} \\
&= \mathcal{L}\{1\} - \mathcal{L}\{(1+bt)^n e^{-\lambda a t}\} \qquad (\mathcal{L} \text{ is a linear operator}) \\
&= \frac{1}{s} - \mathcal{L}\{(1+bt)^n e^{-\lambda a t}\} \\
&= \frac{1}{s} - \sum_{k=0}^{n} \binom{n}{k} b^k \mathcal{L}\{t^k e^{-\lambda a t}\} \\
&= \frac{1}{s} - \sum_{k=0}^{n} \binom{n}{k} b^k \frac{k!}{(s+\lambda a)^{k+1}}
\end{aligned}$$

Hence, as $\mathcal{L}\{f_T(t)\} = s\mathcal{L}\{F_T(t)\}$,

$$\mathcal{L}\{f_T(t)\} = 1 - \sum_{k=0}^{n} \binom{n}{k} \frac{s b^k k!}{(s+\lambda a)^{k+1}}$$

Then,

$$\begin{aligned}
\frac{d}{ds}\mathcal{L}\{f_T(t)\} &= -\sum_{k=0}^{n} \binom{n}{k} b^k k! \frac{d}{ds} \frac{s}{(s+\lambda a)^{k+1}} \\
&= -\sum_{k=0}^{n} \binom{n}{k} b^k k! \left[\frac{1}{(s+a\lambda)^{k+1}} - \frac{s(k+1)}{(s+a\lambda)^{k+1}} \right] \\
\frac{d}{ds}\mathcal{L}\{f_T(t)\}|_{s=0} &= -\sum_{k=0}^{n} \binom{n}{k} b^k k! \frac{1}{(\lambda a)^{k+1}} \\
&= -\frac{1}{a\lambda} \sum_{k=0}^{n} \binom{n}{k} k! \left(\frac{b}{\lambda a} \right)^k \\
&= -\frac{1}{a\lambda} \sum_{k=0}^{n} \frac{n!}{(n-k)!} \left(\frac{b}{\lambda a} \right)^k \\
&= -\frac{1}{a\lambda} \left[n! \sum_{k=0}^{n} \frac{1}{(n-k)!} \left(\frac{b}{\lambda a} \right)^k \right] \\
&= -\frac{1}{a\lambda} \left[n! \sum_{k=0}^{n} \frac{1}{k!} \left(\frac{b}{\lambda a} \right)^{n-k} \right] \qquad (k \to n-k) \\
&= -\frac{1}{a\lambda} \left[n! \left(\frac{b}{\lambda a} \right)^n \sum_{k=0}^{n} \frac{1}{k!} \left(\frac{b}{\lambda a} \right)^{-k} \right] \\
&= -\frac{1}{a\lambda} \left[n! \left(\frac{b}{\lambda a} \right)^n \sum_{k=0}^{n} \frac{1}{k!} \left(\frac{\lambda a}{b} \right)^k \right]
\end{aligned}$$

Finally, as $\mathbf{E}[T] = -\mathcal{L}\{f_T(t)\}|_{s=0}$,

$$\mathbf{E}[T] = \frac{1}{\lambda a}\left[n!\left(\frac{b}{\lambda a}\right)^n \sum_{k=0}^{n} \frac{1}{k!}\left(\frac{\lambda a}{b}\right)^k\right], \text{ where } n = \frac{\lambda(a-1)}{b}$$

Let's check this equation for already known scenarios. When $a = 1$, then $n = 0$ and $\mathbf{E}[T] = 1/\lambda$. When $b \to +\infty$, it reduces to the case in which the hash rate is multiplied by a, which we have already studied. In fact, $n \to 0$, $u(t) \to a$, and $\mathbf{E}[T] = \frac{1}{\lambda a}$.

Theorem 5.

$$a > 1 \textit{ and } x > M \Rightarrow \left|\frac{1+abx}{1+bx} - a\right| < \frac{a-1}{1+bM}$$

Proof. $x > M \Rightarrow \frac{1}{1+bx} < \frac{1}{1+bM}$. As $1 - a < 0$, $\frac{1-a}{1+bx} > \frac{1-a}{1+bM}$. Thus, $\frac{1-a}{1+bM} < \frac{1-a}{1+bx} + a - a = \frac{1+abx}{1+bx} - a < 0 < \frac{a-1}{1+bM}$. Hence, $-\frac{a-1}{1+bM} < \frac{1+abx}{1+bx} - a < \frac{a-1}{1+bM}$. □

For instance, if we would like to know the impact of smoothly double the hash rate in the next week, then the parameters would be $\lambda = 1/600$, $a = 2$, $M = 1$ week $= 3600 \cdot 24 \cdot 7 = 604,800$, b can be calculated using $\epsilon = \frac{a-1}{1+bM} < 0.01 \Leftarrow b > 0.000163690 \Leftarrow n < 10.1818$. So, for $n = 10$, then $b = 0.000166666$ and $\epsilon = 0.009823 < 0.01$, as expected. Finally, $\mathbf{E}[T] = 557.65$. In other words, during the next week, the average time between blocks will be 9 minutes and 17 seconds, instead of the normal 10 minutes. If the hash rate had suddenly doubled, the average time between blocks would be 5 minutes.

4.6.2 *Piecewise linear model of hash rate change*

Let's analyze what would happen if the network's hash rate is growing linearly with angular coefficient a^2, i.e., $u(a, b, t) = a^2 t + b$. Thus, $\mathbf{P}(T \leqslant t) = 1 - e^{-\frac{bt + a^2t^2/2}{\eta}}$.

It is well known that $\mathbf{E}(T) = \int_0^\infty 1 - \mathbf{P}(T \leqslant t)dt$. Thus, replacing $y = \frac{a^2t+b}{a\sqrt{2\eta}}$, and using the fact that $\int_0^\infty e^{-x^2}dx = \frac{\sqrt{\pi}}{2}\operatorname{erf}(x)$, we have:

$$\begin{aligned}
\mathbf{E}(T)|_{t_1}^{t_2} &= \int_{t_1}^{t_2} \exp\left(-\frac{bt + a^2t^2/2}{\eta}\right) dt \\
&= \frac{\sqrt{2\eta}}{a}\exp\left(\frac{b^2}{2a^2\eta}\right)\int_{y_1}^{y_2}\exp(-y^2)dy \\
&= \frac{\sqrt{2\eta}}{a}\exp\left(\frac{b^2}{2a^2\eta}\right)\frac{\sqrt{\pi}}{2}[\operatorname{erf}(y_1) - \operatorname{erf}(y_2)] \\
&= \frac{\sqrt{2\pi\eta}}{2a}\exp\left(\frac{b^2}{2a^2\eta}\right)[\operatorname{erf}(y_2) - \operatorname{erf}(y_1)] \qquad (1)
\end{aligned}$$

Where $y_1 = \frac{a^2 t_1 + b}{a\sqrt{2\eta}}$ and $y_2 = \frac{a^2 t_2 + b}{a\sqrt{2\eta}}$.

Thus, $\mathbf{E}(T) = \mathbf{E}(T)|_0^\infty$. When $t_1 = 0 \Rightarrow y_1 = \frac{b^2}{2\sqrt{2\eta}}$ and $t_2 \to \infty \Rightarrow y_2 \to \infty \Rightarrow \text{erf}(y_2) = 1$, then:

$$\mathbf{E}(T) = \frac{\sqrt{2\pi\eta}}{2a} \exp\left(\frac{b^2}{2a^2\eta}\right)\left[1 - \text{erf}\left(\frac{1}{a\sqrt{2\eta}}\right)\right]$$

The function $\mathbf{E}(T)|_{t_1}^{t_2}$ may be used to a piecewise linear analysis of any hash rate change. Let's analyze the hash doubling in one week. Then, $u(1\text{week}) = u(604800) = 2$, thus $a^2 = \frac{1}{604800} \Rightarrow a = \frac{1}{120\sqrt{42}}$. Let's sample the interval $[0, 1\text{week}]$ every hour, i.e., $(t_0, t_1, t_2, \ldots, t_168)$, where $t_i = i \cdot 1\text{hour} = i \cdot 3600$.

For each point t_i, let $g_i(t) = [H(t - t_i) - H(t - 604800)]u(t) + 2H(t - 604800)$, then $\mathbf{E}(T) = \mathbf{E}(T)|_{t_i}^{t_{i+1}} + 1 - e^{\frac{t}{\eta}}$. The result is presented in Figure .

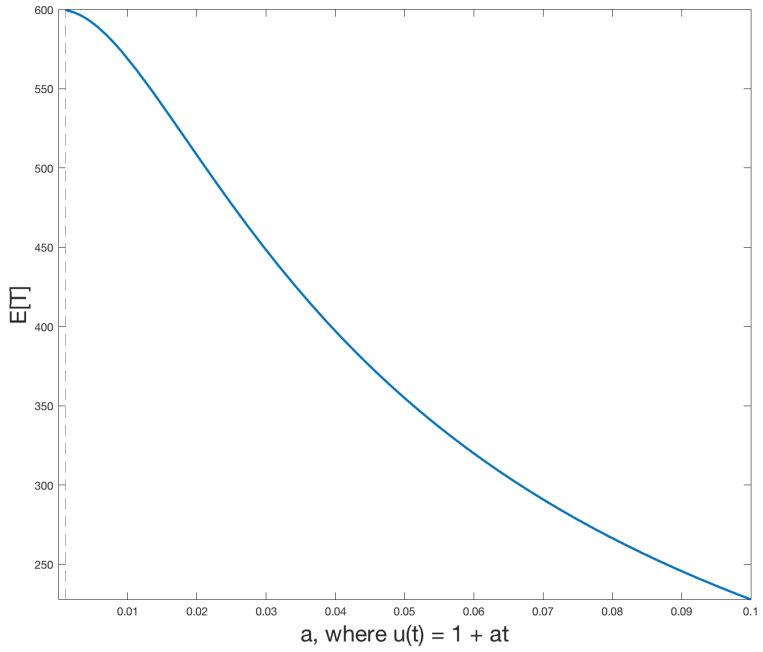


Figure 2: $\mathbf{E}[T]$ when H increases linearly with $u(t) = 1 + at$.

4.7 ATTACK IN THE BITCOIN NETWORK

There are many possible ways to attack the Bitcoin (REF). In this section, we are interested in a particular attack: the double spending attack.

In the double spending attack, the attacker's send some funds to the victim, let's say a merchant. They wait for k confirmations of the transaction, and the victim delivers the good or the service to the

attacker. Then, the attacker mine enough blocks with a conflicting transaction, double spending the funds which was sent to the victim. If the attacker is successful, the original transaction will be *erased* and the victim will be left with no funds at all. In order to be successful, the attacker must propagate more blocks than the network in the same period, propagating a chain longer than the main chain. Hence, we would like to understand what the odds are that the attacker will be successful. This attack was originally discussed by Nakamoto [51].

In order to maximize their odds, the attacker must start to mine the new blocks as soon as they send the funds to the victim. In this moment, it starts to mine in the head of the blockchain, just like the rest of the network. So, in the beginning, the attacker and the network are in exactly the same point.

Let βH be the hash rate of the attackers, and γH be the network's hash rate without the attackers. Thus, when $H \to +\infty$, we already know that $T_{\text{attackers}}$ and T_{network} follow exponential distributions with parameters $\lambda_{\text{attacker}} = \frac{\beta}{\eta}$ and $\lambda_{\text{network}} = \frac{\gamma}{\eta}$, respectively.

As [51] has done, we will also model the attack using the Gambler's Ruin. In this game, a gambler wins \$1 at each round, with probability p, and loses \$1, with probability $1 - p$. The rounds are independent. The gambler starts with \$$k$ plays continuously until he either accumulates a target amount of \$$m$, or loses all his money. Let $\rho = \frac{1-p}{p}$, then the probability of losing his fortune is:

$$\mathbf{P}(\text{losing his fortune}) = \begin{cases} \frac{\rho^k - \rho^m}{1-\rho^m}, \text{ if } \rho \neq 1, \\ \frac{m-k}{m}, \text{ if } \rho = 1. \end{cases}$$

When $m \to +\infty$,

$$\mathbf{P}(\text{losing his fortune}) = \begin{cases} \rho^k, \text{ if } \rho < 1, \\ 1, \text{ if } \rho \geqslant 1. \end{cases}$$

The gambler winning \$1 is the same as the network finding a new block, the gambler losing \$1 is the same as the attacker finding a new block. The initial \$$k$ is the same as the number of blocks the attacker is behind the network. Thus, the gambler loses his fortune is the same as the attacker successfully finds k or more blocks than the network, i.e., losing his fortune means that the attack was successful.

In our case, $p = \frac{\lambda_{\text{network}}}{\lambda_{\text{network}} + \lambda_{\text{attacker}}} = \frac{\gamma}{\beta+\gamma}$, thus $\rho = \frac{\beta}{\gamma}$. Hence, $\rho < 1 \Leftrightarrow \beta < \gamma$.

Suppose that the attacker is mining with the network. Suddently, he stops mining with the network and starts attacking, i.e., starts to mine in another chain. In this scenario, since the attacker's hash rate is not mining with the network anymore, $\gamma = 1 - \beta$. Thus, $\beta < \gamma \Rightarrow \beta < 0.5 \Leftrightarrow \rho < 1$. Here comes the conclusion that, if the attacker has 50% or more of the network's hash rate, then his attack will be certainly successful. We got exactly the same equations and conclusions as [51].

But this scenario seems not to be the optimal attack, because the attacker has waited k confirmations before starting the attack. A better approach would be to start attacking just after propagating the transaction. In this case, our previous model is not good, because even if the attacker have found more blocks than the network, he cannot propagate those blocks before the network has found k confirmations. So, we have to model the probabilities before the network has found the k block. Then, if the attacker has more blocks than the network, he has successfully attacked. Otherwise, we return to the previous model, in which the attacker must still find more blocks.

Theorem 6. *Assuming that the attacker starts the attack just after publishing the transaction, the probability of the attacker has already found exactly s blocks while it waits the network to find k blocks is* $\mathbf{P}(S = s) = \binom{k+s-1}{s}(1-p)^s p^k$.

Proof. The attacker must find exactly s blocks while the network must find exactly k blocks. It is as they would be walking the grid from the point $(0,0)$ to (s,k), where it is only allowed to go up or right, like in Figure 3. When the attacker finds a block, it would be a movement to the right. When the network finds a block, it would be an upward movement. No matter the order which the blocks are found, all the paths occur with probability $(1-p)^s p^k$.

The walking ends when $(\cdot, k)$ is reached, i.e., when the network finds k blocks, regardless of how many blocks the attacker has found – i.e., it is not allowed to walk above the line $(\cdot, k)$. Thus, the number of paths between $(0,0)$ and (s,k) moving only upward or to the right, without going into the line $(\cdot, k)$ is exactly the number of paths between $(0,0)$ and $(s, k-1)$, which is equal to the number of permutations of the sequence $(u, u, \ldots, u, r, r, \ldots, r)$ in which there are s movements to the right (r) and $k-1$ upward movements (u). This number of permutations is $\frac{(k-1+s)!}{s!(k-1)!} = \binom{(k-1)+(s)}{s}$ because there are s repetitions of the element r and $k-1$ repetitions of the element u.

Finally, the probability is $\binom{k+s-1}{s}(1-p)^s p^k$.

□

Assuming that the attacker starts mining just after publishing the victim's transaction, the probability of the attacker will have found more than k blocks while it waits the network to find k blocks is $\mathbf{P}(S \geqslant k) = \sum_{s=k}^{\infty} \binom{k+s-1}{s}(1-p)^s p^k$.

Theorem 7.

$$\mathbf{P}(S \geqslant k) = 1 - \sum_{s=0}^{k-1} \binom{k+s-1}{s}(1-p)^s p^k.$$

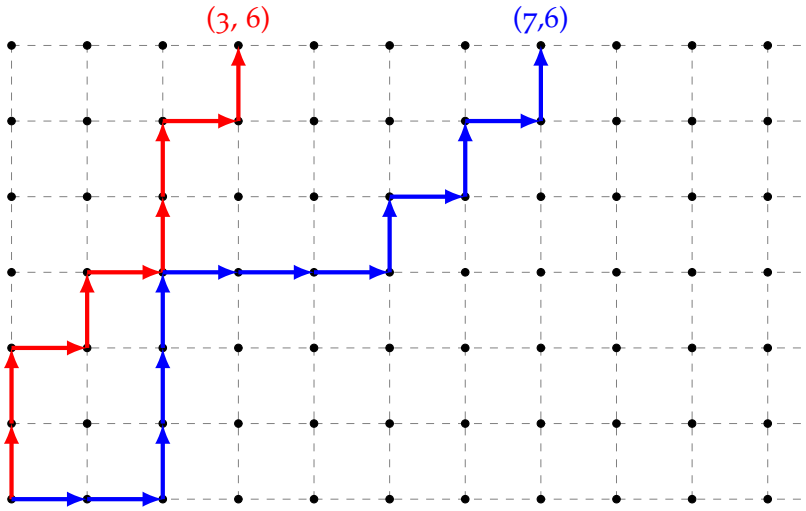


Figure 3: Both the attacker and the network are mining. Each step up is a new block found by the network with probability p. Each step right is a new block found by the attacker with probability $1-p$. It ends when the network finds k blocks — in this example, $k = 6$. The red path has probability $p^6(1-p)^3$, while the blue path has probability $p^6(1-p)^7$. Notice that the blue path is a successfull attack, because the attacker has found more blocks than the network. In the red path, the attacker still have to catch up 3 blocks to have a successful attack, which happens with probability ρ^3, if $p < 0.5$.

Proof. Let's use the following identity:

$$\frac{1}{(1-z)^{a+1}} = \sum_{i=0}^{\infty} \binom{i+a}{i} z^i, \text{ for } |z| < 1$$

Thus, replacing $z = 1-p$, $i = s$, and $a = k-1$, we have:

$$\frac{1}{p^k} = \sum_{s=0}^{\infty} \binom{s+k-1}{s} (1-p)^s$$

$$1 = \sum_{s=0}^{\infty} \binom{s+k-1}{s} (1-p)^s p^k.$$

Now, just split $\sum_{s=0}^{\infty} = \sum_{s=0}^{k-1} + \sum_{s=k}^{\infty}$ and it is done. □

Using this last theorem, we moved from an infinity sum to a finity sum.

Theorem 8. *Let* $p = \frac{\gamma}{\beta+\gamma}$.

$$\mathbf{P}(\textit{successful attack}) = \begin{cases} 1 - \sum_{s=0}^{k-1} \binom{k+s-1}{s} \left((1-p)^s p^k - (1-p)^k p^s\right), & p \geqslant 0.5 \\ 1, & p < 0.5. \end{cases}$$

Proof.

$$\mathbf{P}(\text{successful attack}) = \mathbf{P}(S \geqslant k) + \sum_{i=0}^{k-1} \mathbf{P}(s = i)\rho^{k-i}$$

□

For $k = 6$, $p = 0.9$, $\mathbf{P}(\text{successful attack}) = 0.0005914121600000266$.
For $k = 6$, $p = 0.7$, $\mathbf{P}(\text{successful attack}) = 0.15644958192000014$.

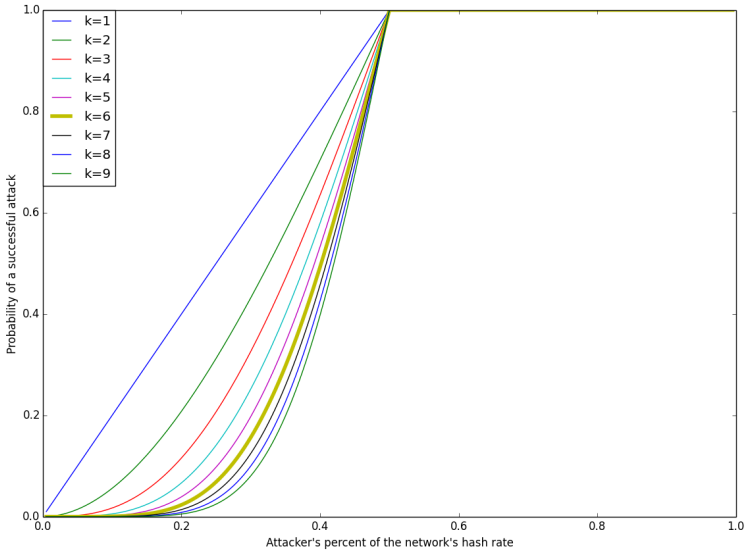


Figure 4: Probability of a successful attack according to the network's hash rate of the attacker (β).

4.8 CONFIRMATION TIME AND NETWORK CAPACITY

Let's say that when a new transaction is propagated it is enqueued in the unconfirmed transaction queue. Then, when a new block is found, some of these transactions in the queue are confirmed. We are interested in some measures of the queue, like the expected time to confirm a transaction and the queue's length.

Let's assume that all transactions have exactly the same size S and pay exactly the same fee. If the Bitcoin block's maximum size is M, there would be room for $s = \lfloor M/S \rfloor$ transactions in each block. Using the results from Bailey [5], we have found that $\pi_n = \frac{z_s - 1}{z_s^{n+1}}$ is the probability of having n unconfirmed transactions in the pool subjected to $s > m$, where $m = \frac{\lambda_{TX}}{\lambda_{blocks}}$ and z_s is the single root of the polynomial $z^s(1 + m(1 - z)) - 1$ with $|z_s| > 1$. The average size of the unconfirmed transaction pool is $\mathbf{E}(\pi) = \frac{1}{z_s - 1}$. Thus, $s > m \Rightarrow \lambda_{TX} < s\lambda_{blocks}$. The probabilities form a simple geometric

series, and so they are exponentially decreasing. We may interpret it as a stable system, i.e., the unconfirmed transactions pool size is finite. In the Bitcoin's network, $\lambda_{\text{blocks}} = 1/\eta$ and the average number of transactions per block is $s = 2,250$, so, this solution is valid when $\lambda_{TX} < 2,250/600 = 3.75$. Hence, 3.75 is the maximum number of new transactions per second that the Bitcoin's network may handle. When $\lambda_{TX} > 3.75$, the unconfirmed transaction pool starts to grow indefinitely.

The average waiting time of a transaction to be confirmed, when $m < s$, is $\mathbf{E}(w) = \frac{1}{\lambda_{TX}(z_s - 1)}$.

When $m \ll s$, $z_s \to 1 + 1/m$. So, the average number of unconfirmed transactions is $\mathbf{E}(\pi) \to m$ and the average waiting time $\mathbf{E}(w) \to \frac{1}{\lambda_{\text{blocks}}} = \eta = 600$ seconds. In the Bitcoin's network, $s \gg m \Rightarrow \lambda_{TX} \ll 3.75$.

When $\lambda_{TX} \to s$, $z_s \to 1$. So, $\mathbf{E}(\pi) \to +\infty$.

Finally, we conclude that the Bitcoin's network capacity is $\lambda_{\text{blocks}} s = s/\eta = s/600$ transactions per second, where s is the average number of transactions per block.

4.9 FORK ANALYSIS

When a disagreement between miners' rules happens, that is referred as either a hard-fork or a soft-fork. It is said to be a soft-fork when the rules are backward compatible, and a hard-fork when the rules are not backward compatible. In general, a hard-fork relaxes the constraints, while the latter hardens them.

Suppose that the miners' are split in two groups, G_1 and G_2, with different rules. Let's say H_1 and H_2 are their hash rate, respectively. We have two different scenarios to analyze: (i) when neither of them accepts other's blocks; and (ii) when G_2 accepts G_1's blocks, but not the other way around.

Scenario (i) is easy to analyze, because the network would just split and, after a while, both difficulties will be adjusted. Then, they will be just like two different Bitcoin networks.

Scenario (ii) is more trick. As G_2 accepts G_1 blocks, their hashrate will matter. If $H_1 > H_2$, then G_2 will frequently skip their blockchain, because G_1's blockchain will be longer most of the time. If $H_1 < H_2$, then G_2 may have its own blockchain after a while — a true fork. But what would happen if H_1 keeps increasing and eventually gets larger than H_2? It if happens for sufficient time, the whole G_2's blockchain may be discarded in order to move to G_1's blockchain when G_1's gets longer.

Theorem 9. *When $H_1 > H_2$, the*

5

DAG MODEL

DAG model proposes a whole different approach to confirmations. It proposes that there is no need for a block to confirm transactions, as transactions can confirm themselves. Here, each transaction has its own proof-of-work, named weight, and they must confirm two other, previous, transactions. Hence, each transaction has an accumulated weight, which is the accumulated proof-of-work that has confirmed it so far. In this sense, instead of a chain of blocks, the transactions and their confirmations form a directed and acyclic graph, as in Fig. 5.

Like the Blockchain, the DAG model is another technology to store immutable data and may be the underlying technology to different applications, such as cryptocurrencies, digital contracts (Ethereum-like), digital notaries, and so forth. The main question which this work proposes to answer is: Is it reliable to use DAG model? In which conditions?

The transactions may be either confirmed or unconfirmed. The confirmed transactions have been already confirmed by at least one more transaction. It does not mean they are already irreversible and protected against a double spend attack — it just means at least one transaction has done some work to confirm it. The unconfirmed transactions are called tips and they are eager to be confirmed. Usually a new transaction selects two tips to confirm, but this rule may not be followed.

Transactions may have any format, including Bitcoin-like transactions—with inputs, outputs, and scripts. But it also may be completely different, just like in the cryptocurrency Iota [62]. This work will not discuss details of the transactions' format, because we understand that it does not affect exactly the network scalability and security.

The accumulated weight of a transaction A is the sum of all weights of the transactions which confirm A, including A itself, i.e., $w_A + \sum_{A \rightsquigarrow P} w_P$. For example, in Fig. 5, the accumulated weight of transaction 3 is the sum of the weights of the transactions 5, 6, 7, and 8. The accumulated weight may be interpreted as how hard it is to rollback a transaction. It is analogous to the number of confirmations of a block in Bitcoin.

The score of a transaction A is the sum of all weights of the transactions which are being confirmed by A, including A itself, i.e., $w_A + \sum_{P \rightsquigarrow A} w_P$. For example, in Fig. 5, the score of transaction 3 is the sum of the weights of the transactions 1 and 2. It is a measure of

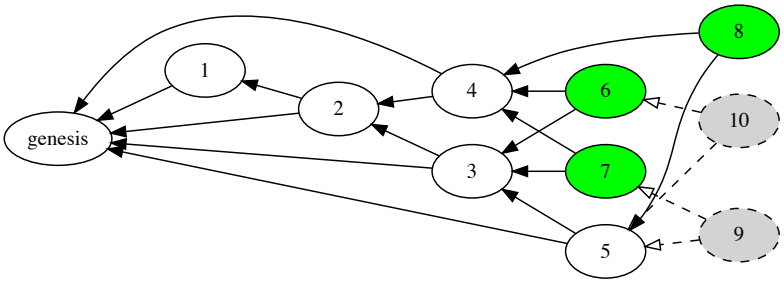


Figure 5: White nodes represent transactions that have been confirmed at least once. Green circles represent unconfirmed transactions (tips). Gray and dashed nodes are the transactions currently solving the proof-of-work in order to be propagated.

how much proof-of-work has been done before confirming this transaction. It may indicate whether the confirmed transactions have received enough attention (and hashpower) or whether it may have received tangential attention.

The height of a transaction A is the length of the longest path from transaction A to the genesis transaction. For example, in Fig. 5, the height of transaction 5 is four ($5 \rightarrow 3 \rightarrow 2 \rightarrow 1 \rightarrow$ genesis). It may be interpreted as the "'age" of the transaction. The lower the height, the older the transaction.

The depth of a transaction A is the length of the longest path in the inverted graph from transaction A to any unconfirmed transaction (tip). For example, in Fig. 5, the depth of transaction 2 is three ($2 \rightarrow 3 \rightarrow 5 \rightarrow 8$). It is the opposite of the height. It may be interpreted as the youth of the transaction. The lower the depth, the younger the transaction. When a new transaction is confirming two transactions with high depth, it is referred as lazy transaction.

An important factor of DAG model is how the new transactions choose which transactions they will confirm. There are several possible approaches, such as randomly selecting two of the unconfirmed transactions (tips). In Fig 5, the reader may have noticed that transaction 8 will confirm transaction 4, which has already been confirmed by transaction 7. It may be on purpose, or maybe transaction 4 was unconfirmed when it was chosen, but it got confirmed during the calculation of the proof-of-work or the network propagation of the transaction. The selection algorithm seems to be important to protect the network against double spend attacks.

The higher the volume of new transactions, the more unconfirmed transactions will appear. In Fig. 6, the reader can notice that the number of new transactions was increased for a while, and then

decreased back to the original value. The DAG has behaved well when exposed to a high load scenario, since it reduced the number of tips to only three. It is like a moving swarm which gets wider when the number of new transactions increases and gets thinner when the number of new transactions decreases.

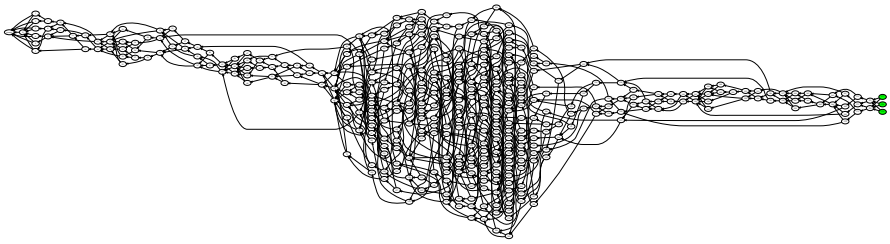


Figure 6: Suddenly the number of transactions per second increases and the width of the swarm grows. After a while, the number of transactions per second decreases and the width of the swarm shrinks.

Conflicting transactions may happen when two or more transactions try to spend the "same money" — or, in the Bitcoin's transaction format, try to spend the same output. In this case, the network must choose which of the transactions will be accepted and the other one will be invalidated, even when both have already been confirmed. In fact, when one transaction is invalidated, the whole sub-DAG which confirms it is also invalidated. In this case, it may happen to reverse some transactions.

Intuitively, when there is a conflict, the network should accept the transaction which has greater accumulated weight, invalidating the others (see Fig. 7). But it may be not enough to prevent a nuclear submarine attack.

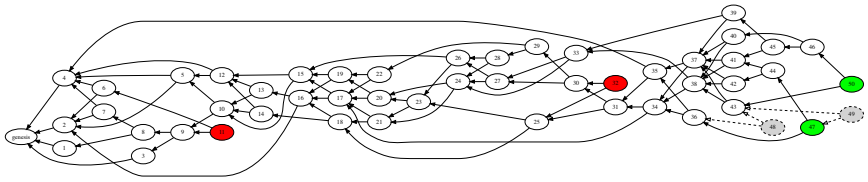


Figure 7: The red nodes are transactions which had some conflict with previous transaction and were invalidated by the network. Notice that none of them have been confirmed.

5.1 NUCLEAR SUBMARINE ATTACK

The nuclear submarine attack, also known as the parasite chain attack, is when the attacker generates a separate DAG (or a side DAG), with many transactions and a lot of proof-of-work. This side DAG is off the network, i.e., its transactions have not been propagated. Then, at a convenient moment, the attacker suddenly

propagates these transactions. The whole network needs to decide how to handle these transactions.

If the transactions have no conflict with any transaction of the main DAG, i.e., there is no transaction spending the "same money", then it seems easy to handle the transactions. But, as it is an attack, probably there will be some conflicts, and it is not easy to choose which transaction should be invalidated. As the attacker has been generating a separate DAG, the conflicting transaction may have an accumulated weight similar or greater than the transaction in the main DAG. Thus, using only the accumulated weight may not be enough to prevent this attack.

For example, the attacker may generate a transaction which transfers all their funds to another address. Then, they start to generate many new transactions which confirms themselves and even confirms some of the transactions in the main DAG. But none of these transactions are propagated to the network. Then, the attacker buys something in the real world, pays with cryptocurrency, and wait until the payment gets the accumulated weight demanded by the merchant. Finally, the attacker suddenly propagates all the transactions to the network in a small window of time. This may cause the network to accept the attacker's original transaction instead of the one used to pay the merchant. Hence, the merchant transaction is invalidated, and the double spend attack has succeeded.

5.2 PROPOSAL: QUESTIONS TO BE EXPLORED

Given these preliminaries, these are some questions with which we will be concerned.

In this paper, we will analyze the network scaling and security. How a DAG network scales, simulating different loads and measuring the bandwidth, computational effort, and storage space necessary to handle all the transactions in time. What is the minimum transaction's aggregated weight which it may be considered unlikely to be reversed?

We are interested in how the rate of new transactions affects how long it takes to a new transaction to be confirmed for the first time. We had already run some simulations under normal load (Fig. 8) and high load (Fig. 9).

Besides the time to the first confirmation, it is also important to measure how long it takes to a new transaction reach a specific accumulated weight. It is useful for exchanges and merchants to set their minimum requirements. Bitcoin's exchanges and merchants usually requires a minimum of 6 confirmations blocks.

As the DAG network is distributed, its users may use different parameters — they cannot violate the network's rules, but they may

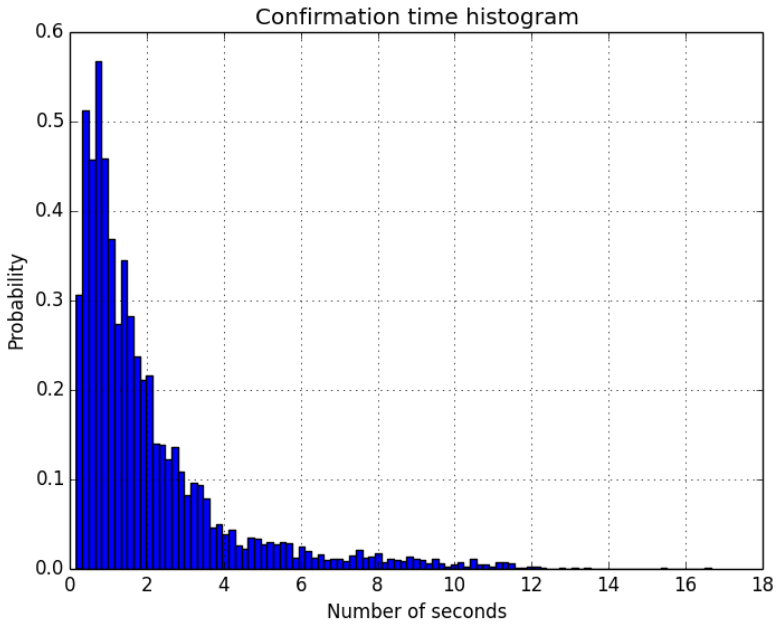


Figure 8: Histogram of how long has been a transaction waiting until its first confirmation. It was a simulation of 15 minutes with new transactions rate changing between 1 and 15 tx/s.

use different tip selection algorithms, for instance. We would like to explore how different users' parameters may affect the network, how much is necessary to cause either a hard-fork or a soft-fork.

[62] suggests that constraining transactions' weight in a range would both prevent spam, because it would be necessary a minimum work to propagate a new transaction, and attacks, because an attacker would not be allowed to propagate a transaction with very high weight. We agree with the spam argument, and would like how a minimum weight would affect mobile devices's new transactions. We partially agree with the upper bound, because an attacker would be able to generate many transaction with lower weight. We will analyze if constraining transactions' weight would be effective against nuclear submarine attacks.

We have another suggestion to prevent nuclear submarine attacks: set a maximum depth for the transactions confirmed by a new transaction. So, new transactions would have to confirming newer transactions instead of old transactions, and a nuclear submarine attack would be controlled because the attacker would be not be able to create a large separate DAG. But the maximum depth rule would possibly also affect transaction created by low (hash)power devices, because it would take a longer time to solve the proof-of-work and, if the confirmations are going fast, the transaction would possibly be invalidated. This raises another important question: what would be an optimal maximum depth allowed?

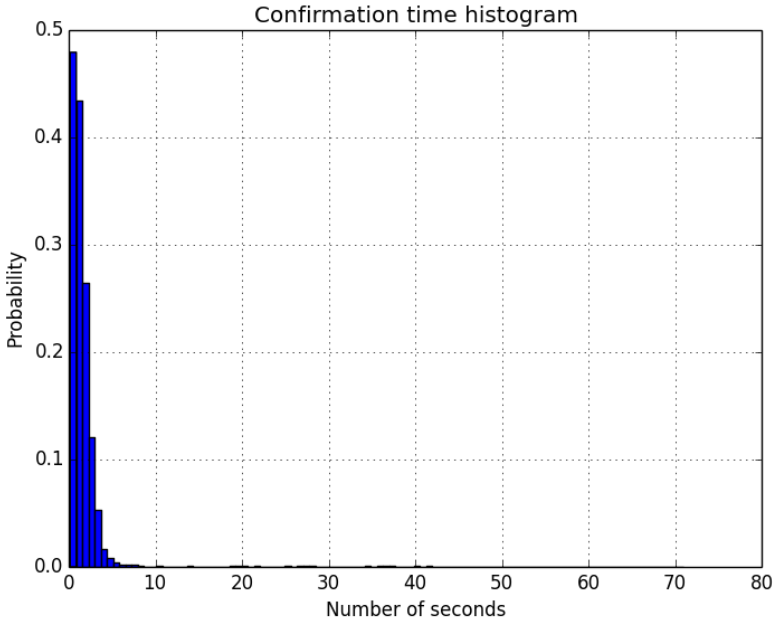


Figure 9: Histogram of how long has been a transaction waiting until its first confirmation. It was a simulation of 5 minutes with new transactions rate of 50 tx/s, i.e., very high load.

If we would like to include fee transactions, how would it be distributed between confirmations? As transactions may have multiple direct confirmations, it is not obvious who would receive the transaction fee. An intuitive suggestion would be to give the fee to the first confirmation with a minimum weight, but it might have some propagation problems, because it takes a while to propagate a transaction in the network and there would be conflict.

In order to solve the fee distribution problem, we will simulate how the network would behave if we include blocks. These blocks would be like Bitcoin's, with an adjustable proof-of-work according to the network's hashpower. They would receive the fees from all confirmed transactions which had not been confirmed by any block before, and they would be able to generate new coins. These blocks would also help solving other problems.

6 METHODOLOGY

The methodology we have been using is computer simulation. Through the simulation of many scenarios of DAG model with different parameters, we will understand how the network behaves in complex scenarios, mainly when the load is suddenly increased, and when the network is under attack. We will first test our hypothesis through simulation and than prove them mathematically.

The simulator has been developed using an event-based design which is capable of running hours of simulation in just a few minutes. It creates agents who decide to make a transaction, then they select which transactions will be confirmed, then they spend some time working in the proof-of-work, and, finally, they propagate the transaction to the network. The other agents receive the transaction and may accept or deny it. The agents may use different parameters among themselves.

When a new transaction is added to the DAG, it uses a depth-first search [24] (i) to update the aggregated weight of the directly and indirectly confirmed transactions, (ii) to calculate its own score, and (iii) to generate a topological sort [24]. The topological sort is used to calculate the longest path from all other transactions to the new transaction, and this longest path is used to update the depth of the whole DAG. If the new transaction confirms only transactions which has already been confirmed, the depth update is skipped thanks to Theorem 10.

The necessary time to generate the proof-of-work is estimated by the function $k \cdot 2^{weight}$, where k is a constant related to the computing power of the agent and weight is randomly chosen.

The time between two new transactions is sampled from the exponential distribution with parameter λ. The value of λ is changed over time, causing changes in the load of the network. We consider 1 tx/s to be a low load, and 15 tx/s to be a high load. Even though we have already tested up to 100 tx/s.

The simulator will output different reports: (i) snapshots of the DAG at interesting moments, such as Fig. 5, 6, and 7; (ii) histogram of confirmation time, such as Fig. 8 and 9; and many others.

7

ANALYSIS OF DAG MODEL

In order to a further understanding of the DAG Model, we will analyze the mathematical model behind it.

The DAG Model's mining starts just like Bitcoin's, i.e., $\mathbf{P}(h(x) < A) = \frac{A}{2^{256}}$. Then, it follows that solving a transaction proof-of-work follows a geometric distribution. Let X be the number of attempts until a success, then $\mathbf{P}(X = k) = (1-p)^{k-1}p$, where $p = \frac{A}{2^{256}}$. Also, $\mathbf{P}(X \leqslant k) = 1-(1-p)^k$. The average number of attempts is $\mathbf{E}(X) = 1/p$.

Let w be the transaction's weight, i.e., $\mathbf{E}(X) = w \Rightarrow w = 1/p$. Let $T = X/H$ be the time required to solve the transaction's proof-of-work, where H is the hash rate of the transaction's owner. Then, $\mathbf{P}(T < t) = \mathbf{P}(X < tH) = 1-(1-p)^{tH} = 1-\left(1-\frac{1}{w}\right)^{tH} = 1-e^{tH\log\left(1-\frac{1}{w}\right)}$, i.e., T follows an exponential distribution with $\lambda = -H\log\left(1-\frac{1}{w}\right)$.

The number of transactions solving the proof-of-work may be modeled by a Birth and Death process, since if we have k transactions solving the proof-of-work only two things may happen: either a new transaction will be created or one the transactions will finish solving the proof-of-work. Let the time between new transactions follows an exponential distribution with μ parameter, then the probability of a new transaction emerges before any transaction finishes its proof-of-work is $q_k = \mathbf{P}(T_{\text{new tx}} = \min\{T_{\text{new tx}}, T_1, T_2, \ldots, T_k\}) = \frac{\mu}{\mu+\sum_{i=1}^{k}\lambda_i}$. Hence, the probability of any transaction finishes its proof-of-work before a new transaction emerges is $p_k = 1-q_k = \frac{\sum_{i=1}^{k}\lambda_i}{\mu+\sum_{i=1}^{k}\lambda_i}$.

Every time a new transaction emerges, it chooses two tips to confirm before solving the proof-of-work. When it finishes solving the proof-of-work, it is propagated and becomes a tip. So, two new transactions may choose the same tips to confirm. If there are t tips, a new transaction will randomly choose 2 out of these t tips, even if they have already been chosen by other new transactions — in fact, they do not know which have been chosen because these new transactions have not being propagated yet.

The following theorems will be mathematically proved. They have already been used in the implementation of the simulator.

Theorem 10. *When a new transaction confirms an already confirmed transaction, the depth of all transactions remains the same, i.e., the depth of the transactions are only changed when a new transaction confirm an unconfirmed transaction.*

Theorem 11. *The height of a transaction is equal to the maximum height of its parents plus one.*

Theorem 12. *If new transactions choose randomly the unconfirmed transactions to be confirmed, then no unconfirmed transaction will be left behind, i.e., all transactions will be confirmed in due time.*

8 CONCLUSION

Bitcoin's underlying technology blockchain has been called by many as a major invention comparable to the invention of the internet. But it is unlikely that Bitcoin and blockchain have achieved the final or most optimal design for a secure and scalable electronic transaction system. In this work, we will investigate whether DAG model is suitable to be a real alternative to blockchain.

Preliminary results obtained from our simulator have shown that, using a random tip selection strategy, the network seems to support up to 50 transactions per second, with no tip abandoned (Fig. 6) or taking too long to have at least one confirmation (Fig. 9). Today, Bitcoin network can barely handle 8 transactions per second without increasing the unconfirmed transaction list to hundreds of thousands — several transactions take days to be confirmed.

We have not yet tested the security of the network against double spend attacks. It will be one of the next steps and we expect to block a nuclear submarine attack including a rule for invalidate new conflicting transactions which confirm transactions with depth greater than a given threshold. We are unsure whether this rule would invalidate legitimate transactions on a high load scenario.

We also plan to improve the analysis of the confirmation time. So far, we have the histograms of how long it takes to a transaction to be confirmed for the first time (Fig. 8 and 9). We will also generate the histograms of how long it takes to a transaction to have an accumulated weight of at least a given number. It is an important histogram because it helps merchants and users to decide how long they should wait to consider the transaction almost irreversible.

We will also work on the mathematical modeling of DAG networks, and the equations will help us to understand the limits of these networks.

Part III

SPARSE DISTRIBUTED MEMORY: A CROSS-PLATFORM, MASSIVELY PARALLEL, OPEN SOURCE REFERENCE IMPLEMENTATION

9 INTRODUCTION

Sparse Distributed Memory (SDM) [41] is a mathematical model of long-term memory that has a number of neuroscientific and psychologically plausible dynamics. Such model may be applied in all sort of applications because it would replicate human capacity to remember past experiences from clues of the present. For instance, when one is walking on a dark alley and is afraid of something, one cannot explain where ones fear come from. They just feel it. We may interpret this situation as clues of the present — a dark alley — recalling past experiences from memory and thus generating the scared feeling. Our memory is able to make a parallel between previous experiences and the clues. Although one has never been in the exactly same situation, ones brain makes an analogy and recognizes the danger. This flexibility into mapping one situation in another is an important human feature which is hard to replicate into computers.

It has been applied in many different fields, like pattern recognition [55, 64], noise reduction [50], handwriting recognition [32], robot automation [63, 49], and so forth. [46] has showed that SDM respects the limits of short-term memory discussed by **?**] and **?**]. Despite all those applications, there is not a reference implementation which would allow one to replicate the results published in a paper, to check the source code for details, and to improve it. Thus, even though intriguing results have been achieved using SDM, it requires great effort of researchers to improve someone's work.

It is our belief that such a tool could bring orders of magnitude more researchers and attention if they were able to use the model, at zero cost, with an easy to use high-level language such as python in an intuitive platform such as juypyter notebook. Neuroscientists interested in long-term memory storage should not have to worry about high-bandwidth vector parallel computation. This new tool provides a ready to use system in which experiments can be executed almost as soon as they are designed and it may accelerate researches [68].

Our motivation was our own effort in order to run our models. As there is no reference implementation, we had to implement our own and run several simulations to ensure that our implementation was correct and bug free. Thus, we had to deviate from our main goal — which was to test our models — and to focus in the implementation

itself. Furthermore, new members in our research group had to go through different source codes developed by former members.

Extensions of SDM has been used in many applications. For example, Snaider and Franklin [70] extended SDM to efficiently store sequences of vectors and trees. Rao and Fuentes [63] used a modified SDM in an autonomous robot. Meng et al. [50] modified SDM to clean patterns from noisy inputs. Fan and Wang [32] extended SDM with genetic algorithms. Chada [19] extended SDM creating the Rotational Sparse Distributed Memory (RSDM), which is used to modeling network motifs, dynamic flexibility, and hierarchical organization, all results from neuroscience literature.

The main contribution of this work is a reference implementation which yields (i) orders of magnitude gains in performance, (ii) has several backends and operations, (iii) has been validated against the mathematical model, (iv) is cross-platform, and (v) is easily extended to fulfill other research models. Our reference implementation may, hopefully, accelerate research into the model's dynamics and make it easier for readers to replicate any previous results and easily understand the source-code of the model. Moreover, it is compatible with jupyter notebook and researchers may share their notebooks possibly accelerating the advances in their fields [68].

Other contributions have also been introduced, which include (i) a noise filtering approach, (ii) a supervised classification algorithm, (iii) and a reinforcement learning algorithm, all of them using only the original SDM proposed by Kanerva, i.e., with no additional mechanisms, algorithms, data structures, etc. Although some of our applications have already been explored in previous work [50, 32, 64], all of them have done some adapting of SDM to their problems, and none of them have used just the ideas introduced by Kanerva. We have presented different approaches with no adaptations at all.

Finally, we have found an anomaly in one of Kanerva's prediction, which we believe is related to SDM capacity. We have also tested a generic reading operation proposed by professor Paulo Murilo (personal communication).

10 NOTATION

n	Number of dimensions, i.e., $n = 1,000$.
N	Size of the binary space — $\lvert\{0,1\}^n\rvert = 2^n$.
N'	Number of hard-locations samples from $\{0,1\}^n$. Its typical value is 1,000,000, as suggested by Kanerva [41].
H	Same as N'.
r	Access radius, i.e., when $n = 1,000$ and $N' = 1,000,000$, its typical value is 451. This value is calculated to activate, on average, one thousand of N'.
η	A bitstring, usually a datum.
η_x	A clue x bits away from η, i.e., $\text{dist}(\eta, \eta_x) = x$.
ξ	A bitstring, usually an address.
$\text{dist}(x, y)$	Hamming distance between x and y
$d(x, y)$	Same as $\text{dist}(x, y)$

11

SPARSE DISTRIBUTED MEMORY

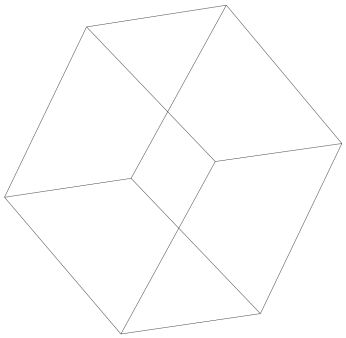
Sparse Distributed Memory (SDM) is a mathematical model for cognitive memory published by Kanerva [41]. It introduces many interesting mathematical properties of n-dimensional binary space that, in a memory model, are psychologically plausible. Most notable among these are the tip-of-the-tongue phenomenon, conformity to Miller's magic number [46] and robustness against loss of neurons.

The data and address space belong to binary space and are represented by a sequence of bits, called bitstrings. The distance between two bitstrings is calculated using the Hamming distance. It is defined for two bitstrings of equal length as the number of positions at which the bits are different. For example, 00110_b and 01100_b are bitstrings of length 5 and their Hamming distance is 2. One has to be careful when thinking intuitively about distance in SDM because the Hamming distance does not have the same properties of, say, the Euclidean distance in 3 dimensions, i.e., both follow triangle inequality ($d(A,B) \leqslant d(A,C) + d(B,C)$), which Euclidean distance in 3 dimensions may be interpreted as "if A is close to B, and B is close to C, then A is also close to C" — $d(A,B) \leqslant r \text{ and } d(B,C) \leqslant r \Rightarrow d(A,C) \leqslant 2r$ —, but in SDM, although the inequality is also valid, two bitstrings would be close when, for instance, $r = 430$, so $2r = 860$ would cover all other bitstrings. Hence, it makes no sense to say that A is also close to C. This difference in intuition may trick even experienced researchers when analyzing some situations.

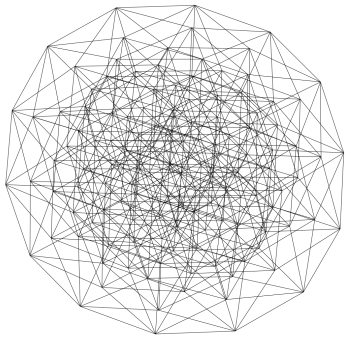
The space studied by Kanerva is also called the *hypercube graph*, or Q_n, as in Figure 10. For a fixed $n \in \mathbb{Z}$, the graph $G = (V, E)$, in which $v \in V$ iff there is a bijective function $b : V \to \{0,1\}^n$ and $(v_i, v_j) \in E$ iff $H(b(v_i), b(v_j)) = 1$, where H is the Hamming distance. That is, n-sized bitstrings correspond to nodes and edges exist between nodes `iff` they flip a single bit. Though Kanerva has derived many combinatorial properties of the space, additional results have been found in the graph-theoretical literature. A good survey is provided by Harary et al. [37].

Unlike traditional memory used by computers, SDM performs read and write operations in a multitude of addresses, also called neurons. That is, the data is not written, or it is not read in a single address spot, but in many addresses. These are called activated addresses, or activated neurons.

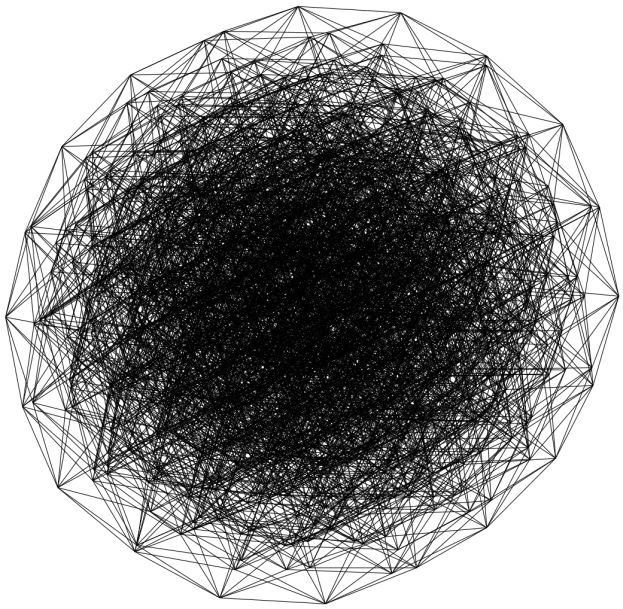
The activation of addresses takes place according to their distances from the datum. Suppose one is writing datum η at address ξ, then



(a) Q_3



(b) Q_7



(c) Q_{10}

Figure 10: Here we have Q_n, for $n \in \{3, 7, 10\}$. Each node corresponds to a bitstring in $\{0,1\}^n$, and two nodes are linked iff the bitstrings differ by a single dimension. A number of observations can be made here. First, the number of nodes grows as 2^n as n grows; which makes the space intractable as $n >> 20$. Another interesting observation, better seen in the figures below, is that most of the space lies 'at the center', at a distance of around 500 from any given vantage point.

all addresses inside a circle with center ξ and radius r are activated. So, η will be stored in all these activated addresses, which are around address ξ, such as in Figure 11. An address ξ' is inside the circle if its hamming distance to the center ξ is less than or equal to the radius r, i.e. $distance(\xi, \xi') \leqslant r$.

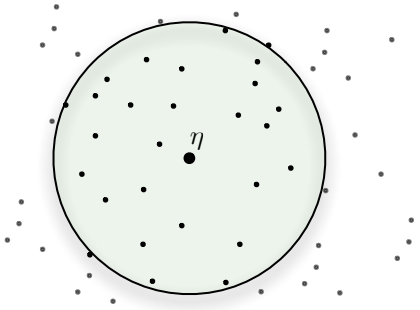


Figure 11: Activated addresses inside access radius r around center address.

Every time write or read in SDM memory activates a number of addresses with close distance. The data is written in these activated addresses or read from them. These issues will be addressed in due detail further on, but a major difference from a traditional computer memory is that the data are always stored and retrieved in a multitude of addresses. This way SDM memory has robustness against loss of addresses (e.g., death of a neuron).

In traditional memory, each datum is stored in an address and every look up of a specific datum requires a search through the memory. In spite of computer scientists having developed beautiful algorithms to perform fast searches, almost all of them do a precise search. That is, if you have an imprecise clue of what you need, these algorithms will simply fail.

In SDM, the data space is the same as the address space, which amounts to a vectorial, binary space, that is, a $\{0,1\}^n$ space. This way, the addresses where the data will be written are the same as the data themselves. For example, the datum $\eta = 00101_b \in \{0,1\}^5$ will be written to the address $\xi = \eta = 00101_b$. If one chooses a radius of 1, the SDM will activate all addresses one bit away or less from the center address. So, the datum 00101_b will be written to the addresses 00101_b, 10101_b, 01101_b, 00001_b, 00111_b, and 00100_b.

In this case, when one needs to retrieve the data, one could have an imprecise cue at most one bit away from η, since all addresses one bit away have η stored in themselves. Extending this train of thought for larger dimensions and radius, exponential numbers of addresses are activated and one can see why SDM is a distributed memory.

When reading a cue η_x that is x bits away of η, the cue shares many addresses with η. The number of shared addresses decreases

as the cue's distance to η increases, in other words, as x increases. This is shown in Figure 12. The target datum η was written in all shared addresses, thus they will bias the read output in the direction of η. If the cue is sufficiently near the target datum η, the read output will be closer to η than η_x was. Repeating the read operation increasingly gets results closer to η, until it is exactly the same. So, it may be necessary to perform more than one read operation in order to converge to the target data η.

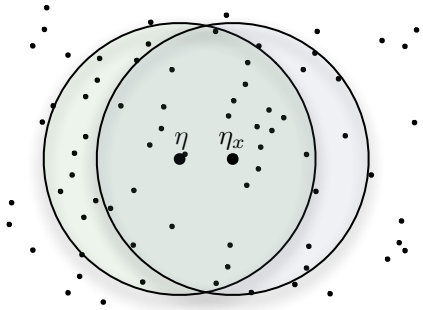


Figure 12: Shared addresses between the target datum η and the cue η_x.

The addresses of the $\{0,1\}^n$ space grows exponentially with the number of dimensions n, i.e. $N = 2^n$. For $n = 100$ we have $N \approx 10^{30}$, which is incredibly large when related to a computer memory. Furthermore, Kanerva [41] suggests n between 100 and 10,000. Recently he has postulated 10,000 as a desirable minimum N (personal communication). To solve the feasibility problem of implementing this memory, Kanerva made a random sample of $\{0,1\}^n$, in his work, having N' elements. All these addresses in the sample are called hard-locations. Other elements of $\{0,1\}^n$, not in N', are called virtual neurons. This is represented in Figure 13. All properties of read and write operations presented before remain valid, but limited to hard-locations. Kanerva suggests taking a sample of about one million hard-locations.

Using this sample of binary space, our data space does not exist completely. That is, the binary space has 2^n addresses, but the memory is far away from having these addresses available. In fact, only a fraction of this vectorial space is actually instantiated. Following Kanerva's suggestion of one million hard-locations, for $n = 100$, only $100 \cdot 10^6/2^{100} = 7 \cdot 10^{-23}$ percent of the whole space exists, and for $n = 1,000$ only $100 \cdot 10^6/2^{1000} = 7 \cdot 10^{-294}$ percent.

Kanerva also suggests the selection of a radius that will activate, on average, one one thousandth of the sample, which is 1,000 hard-locations for a sample of one million addresses. In order to achieve his suggestion, a 1,000-dimension memory uses an access radius $r = 451$, and a 256-dimensional memory, $r = 103$. We think

that a 256-dimensional memory may be important because it presents conformity to Miller's magic number [46].

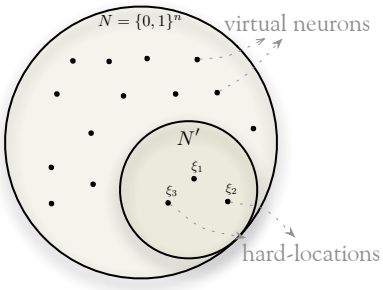


Figure 13: Hard-locations randomly sampled from binary space.

Since a cue η_x near the target bitstring η shares many hard-locations with η, SDM can retrieve data from imprecise cues. Despite this feature, it is very important to know how imprecise this cue could be while still giving accurate results. What is the maximum distance from our cue to the original data that still retrieves the right answer? An interesting approach is to perform a read operation with a cue η_x, that is x bits away from the target η. Then measure the distance from the read output and η. If this distance is smaller than x we are converging. Convergence is simple to handle, just read again and again, until it converges to the target η. If this distance is greater than x we are diverging. Finally, if this distance equals x we are in a tip-of-the-tongue process. A tip-of-the-tongue psychologically happens when you know that you know, but you can't say what exactly it is. In SDM mathematical model, a tip-of-the-tongue process takes infinite time to converge. Kanerva [41] called this x distance, where the read's output averages x, the critical distance. Intuitively, it is the distance from which smaller distances converge and greater distances diverge. In Figure 14, the circle has radius equal to the critical distance and every η_x inside the circle should converge. The figure also shows a convergence in four readings.

The $\{0,1\}^n$ space has $N = 2^n$ locations from which we instantiate N' samples. Each location in our sample is called a hard-location. On these hard-locations we do operations of read and write. One of the insights of SDM is exactly the way we read and write: using data as addresses in a distributed fashion. Each datum η is written in every activated hard-location inside the access radius centered on the address, that equals datum, $\xi = \eta$. Kanerva suggested using an access radius r having about one one thousandth of N'. As an imprecise cue η_x shares hard-locations with the target bitstring η, it is possible to retrieve η correctly. (Actually, probably more than one read is necessary to retrieve exactly η.). Moreover, if some neurons

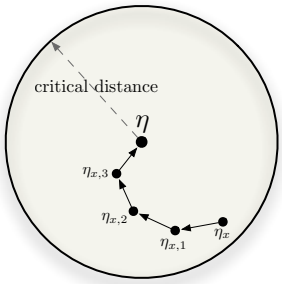


Figure 14: In this example, four iterative readings were required to converge from η_x to η.

η	0	1	1	0	1	0	0
ξ_{before}	6	-3	12	-1	0	2	4
	⇓ -1	⇓ +1	⇓ +1	⇓ -1	⇓ +1	⇓ -1	⇓ -1
ξ_{after}	**5**	**-2**	**13**	**-2**	**1**	**1**	**3**

Table 1: Write operation example in a 7-dimensional memory of data η being written to ξ, one of the activated addresses.

are lost, only a fraction of the datum is lost and it is possible that the memory can still retrieve the right datum.

A random bitstring is generated with equal probability of 0's and 1's in each bit. One can readily see that the average distance between two random bitstrings has binomial distribution with mean $n/2$ and standard deviation $\sqrt{n/4}$. For a large n, most of the space lies close to the mean and has fewer shared hard-locations. As two bitstrings with distance far from $n/2$ are very improbable, Kanerva [41] defined that two bitstrings are orthogonal when their distance is $n/2$.

The write operation needs to store, for each dimension bit which happened more (0's or 1's). This way, each hard-location has n counters, one for each dimension. The counter is incremented for each bit 1 and decremented for each bit 0. Thus, if the counter is positive, there have been more 1's than 0's, if the counter is negative, there have been more 0's than 1's, and if the counter is zero, there have been an equal number of 1's and 0's. Table 1 shows an example of a write operation being performed in a 7-dimensional memory.

The read is performed polling each activated hard-location and statistically choosing the most written bit for each dimension. It consists of adding all n counters from the activated hard-locations and, for each bit, choosing bit 1 if the counter is positive, choose bit 0 if the counter if negative, and randomly choose bit 0 or 1 if the counter is zero.

11.1 NEURONS AS POINTERS

One interesting view is that neurons in SDM work like pointers. As we write bitstrings in memory, the hard-locations' counters are updated and some bits are flipped. Thus, the activated hard-locations do not necessarily point individually to the bitstring that activated it, but together they point correctly. In other words, the read operation depends on many hard-locations to be successful. This effect is represented in Figure 15: where all hard-locations inside the circle are activated and they, individually, do not point to η. But, like vectors, adding them up points to η. If another datum ν is written into the memory near η, the shared hard-locations will have information from both of them and would not point to either. All hard-locations outside of the circle are also pointing somewhere (possibly other data points). This is not shown, however, in order to keep the picture clean and easily understandable.

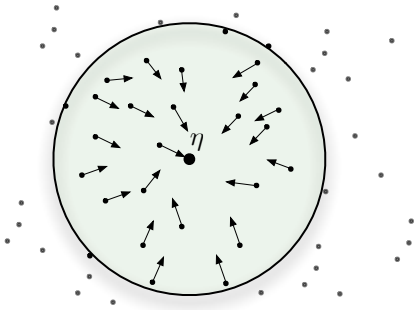


Figure 15: Hard-locations pointing, approximately, to the target bitstring.

11.2 CONCEPTS

Although Kanerva does not mention concepts directly in his book [41], the author's interpretation is that each bitstring may be mapped to a concept. Thus, unrelated concepts are orthogonal and concepts could be linked through a bitstring near both of them. For example, "beauty" and "woman" have distance $n/2$, but a bitstring that means "beautiful woman" could have distance $n/4$ to both of them. As a bitstring with distance $n/4$ is very improbable, it is linking those concepts together. Linhares et al. [46] approached this concept via "chunking through averaging".

Due to the distribution of hard-locations between two random bitstrings, the vast majority of concepts is orthogonal to all others. Consider a non-scientific survey during a cognitive science seminar, where students asked to mention ideas unrelated to the course brought up terms like birthdays, boots, dinosaurs, fever, executive order, x-rays, and so on. Not only are the items unrelated to

cognitive science, the topic of the seminar, but they are also unrelated to each other.

For any two memory items, one can readily find a stream of thought relating two such items ("Darwin gave dinosaurs the boot"; "she ran a fever on her birthday"; "isn't it time for the Supreme Court to x-ray that executive order?", ... and so forth). Robert French presents an intriguing example in which one suddenly creates a representation linking the otherwise unrelated concepts of "coffee cups" and "old elephants" [33].

This mapping from concepts to bitstrings brings us two main questions: (i) Suppose we have a bitstring that is linking two major concepts. How do we know which concepts are linked together? (ii) From a concept bitstring how can we list all concepts that are somehow linked to it? This second question is called the problem of spreading activation.

11.3 READ OPERATION

In his work, Kanerva proposed and analyzed a read algorithm called here Kanerva's read. His read takes all activated hard-locations counters and sum them. The resulting bitstring has bit 1 where the result is positive, bit 0 where the result is negative, and a random bit where the result is zero. In a word, each bit is chosen according to all written bitstrings in all hard-locations, being equal to the bit more appeared. Table 2a shows an example of Kanerva's read result bitstring.

Daniel Chada, one member of our research group, proposed another way to read in SDM, in this work called Chada's read. Instead of summing all hard-location counters, each hard-location evaluates its resulting bitstring individually. Then, all resulting bitstrings are summed again, and the same rule as Kanerva applies. Table 2b shows an example of Chada's read result bitstring. The counter's values are normalized to 1, for positive ones, or -1, for negative ones, and the original values are the same as in Table 2a.

The main difference between Kanerva's read and Chada's is that, in the former, a hard-location that has more bitstrings written has a greater weight in the decision of each bit. In the latter, all hard-locations have the same weight, because they can contribute to the sum with only one bitstring.

It is important to say that Chada's read came from Anwar and Franklin [3] which gave a misguided description of the read operation. The original description is the following:

> With our datum distributively stored, the next question is how to retrieve it. With this in mind, let us ask first how one reads from a single hard location, x. Compute ζ, the bit vector read at x, by assigning its ith bit the value 1 or 0 according as the ith counter at x is positive or negative. Thus, each bit of ζ results from a majority rule decision of all the data that have been written at x. [...] Knowing how to read from a hard location allows us to read from any of the 2^{1000} arbitrary locations. Suppose ζ is any location. The bit vector, ξ, to be read at ζ, [...] Put another way, pool the bit vectors read from hard locations accessible from ζ, and let each of their ith bits vote on the ith bit of ξ.
> — Anwar and Franklin [3, p.342]

This fact just highlihts how important it is to have a reference implementation that one may read the code to clarify one's understanding about the details of each operation.

11.3.1 *Generalized read operation*

A member of my Master's committee, professor Paulo Murilo[1], has proposed a generalized reading operation (personal communication), which covers both Kanerva's and Chada's read — and opens a new venue of potential discoveries. He proposed summing all hard-location counters raised to the power of z while holding the original sign of the counter (positive or negative). Thus, Kanerva's read would be the same as $z = 1$, while Chada's would be the same as $z = 0$. Hence, we will here explore how SDM would behave with other values of z, such as 0.5, 2, and 3. Mathematically, let A be the set of the counters of the activated hardlocation, and c_i be the counter of the i-th bit. Then,

$$s_i = \sum_{c \in A} \frac{c_i}{|c_i|} |c_i|^z$$

Finally, the i-th bit of the resulting bitstring is 1 if $s_i > 0$, or 0 if $s_i < 0$, or random if $s_i = 0$. Notice that when $z = 1$, then $s_i = \sum_{c \in A} c_i$, which is the Kanerva's read; and when $z = 0$, then $s_i = \frac{c_i}{|c_i|} = \text{sign}(c_i)$, which is the Chada's read.

1 Universidade Federal Fluminense's physicist doctor Paulo Murilo

ξ_1	-2	12	4	0	-3
ξ_2	-5	-4	2	8	-2
ξ_3	-1	0	-1	-2	-1
ξ_4	3	2	-1	3	1
$\sum$	**-5**	**10**	**4**	**3**	**-5**
	⇓	⇓	⇓	⇓	⇓
	0	1	1	1	0

(a) Kanerva's read example

ξ_1	-1	1	1	1	-3
ξ_2	-1	-1	1	1	-1
ξ_3	-1	1	-1	-1	-1
ξ_4	1	1	-1	-1	1
$\sum$	**-2**	**1**	**0**	**0**	**-2**
	⇓	⇓	⇓	⇓	⇓
	0	1	1	1	0

(b) Chada's read example

Table 2: Comparison of Kanerva's read and Chada's read. Each ξ_i is an activated hard-location and the values come from their counters. Gray cells' value is obtained randomly with probability 50%.

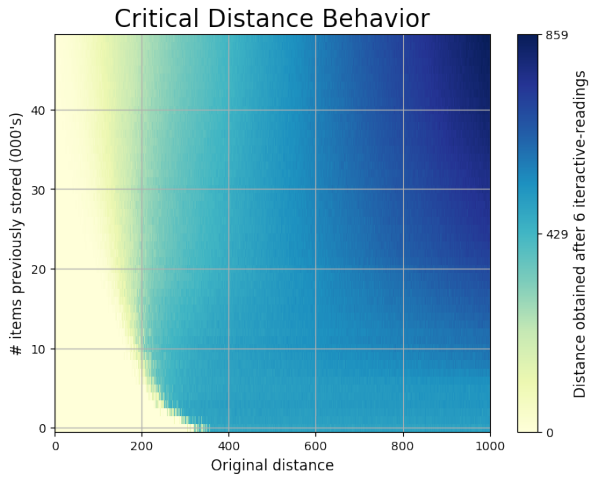
11.4 CRITICAL DISTANCE

Kanerva describes the critical distance as the threshold of convergence of a sequence of read words. It is "the distance beyond which divergence is more likely than convergence"[41]. Furthermore, Kanerva explains that "a very good estimate of the critical distance can be obtained by finding the distance at which the arithmetic mean of the new distance to the target equals the old distance to the target"[41]. In other words, the critical distance can be equated as the edge to our memory, the limit of human recollection.

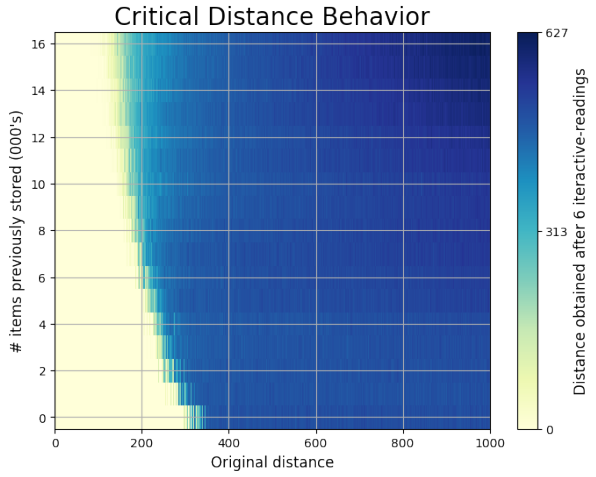
In his book, Kanerva analyzed a specific situation with $n = 1000$ ($N = 2^{1000}$), 1 million hard-locations $N' = 1,000,000$, an access-radius of 451 (within 1,000 hard-locations in each circle) and 10 thousand writes of random bitstrings in the memory. As computer resources were very poor those days, Kanerva couldn't make a more generic analysis.

Starting from the premise of SDM as a faithful model of human short-term memory, a better understanding of the critical distance may shed light on our understanding of the thresholds that bind our own memory.

Figure 16 compares the critical distance behavior under different scenarios. This replicates our previous results [14, 15] and is a first part of the process of framework validation, to which we throw our attention next.



(a) Kanerva's original model



(b) Chada's read

Figure 16: How far, in hamming distance, is a read item from the original stored item? Kanerva demonstrated that, after a small number of iterative readings (6 here), a critical distance behavior emerges. Items read at close distance converge rapidly; whereas farther items do not converge. Most striking is the point in which the system displays the tip-of-tongue behavior. Described by psychological moments when some features of the item are prominent in one's thoughts, yet the item still cannot be recalled (but an additional cue makes convergence 'immediate'). Mathematically, this is the precise distance in which, despite having a relatively high number of cues (correct bits) about the desired item, the time to convergence is infinite. Heatmap colors display the hamming distance the associative memory is able to cleanly converge to—or not. In the x-axis, the distance from the desired item is displayed. In the y-axis, we display the read operation's behavior as the number of items registered in the memory grows. These graphs are computing intensive, yet they can be easily tested by readers in our provided jupyter notebooks. Note the different scales.

12

FRAMEWORK ARCHITECTURE

The framework implements the basic operations in a Sparse Distributed Memory which may be used to create more complex operations. It is developed in C language and the OpenCL parallel framework — which may be loaded in many platforms and programming languages — with a wrapper in Python. The Python module makes it easy to create and execute simulations in a Sparse Distributed Memory and works properly in Jupyter Notebook [42]. It works in both Python 2 and Python 3.

We split the SDM memory in two parts: the hard-location addresses and the hard-location counters. Thus, the addresses (bitstrings) of the hard-locations are stored in one array, while their counters in another. This makes possible to create multiple SDMs using the same address space, which would save computational effort to scan a bitstring in all the SDMs — since they share the same address space, the activated hard-locations will be the same in all of them. As the slowest part of reading and writing operations is scanning the address space, the performance benefits are significant.

Each part may be stored either in the RAM memory or in a file. The RAM memory is interesting for quick experiments, automated tests, and others scenarios in which the SDM may be lost, while the file is interesting for a long-term SDM, like creating an SDM file with 10,000 random writes, which will be copied over and over to run multiple experiments. The file may also be sent to another researcher or may be published within the paper to let others run their own checks and verify the results. In summary, the framework fits many different uses and necessities.

Let a SDM memory with N dimensions and H hard-locations. Then, in a 64-bit computer, the array of hard-location addresses will use $H \cdot 8 \cdot \lceil N/64 \rceil$ bytes of memory, and there will be $H \cdot N$ hard-location counters. For example, in a SDM memory with 1,000 dimensions and 1,000,000 hard-locations, using 32-bit integers for the counters, the array of addresses will use 122MB of memory and the counters will use 3.8 GB of memory.

Basic operations were grouped in four sets: (i) for bitstrings, (ii) for addresses, (iii) for counters, and (iv) for memories (SDMs). Operations include creating new bitstrings, flipping bits, generating a bitstring with a specific distance from a given bitstring, scanning the address space using different algorithms, writing a bitstring to a counter, writing in an SDM, reading from an SDM, and iteratively reading from an SDM until convergence.

12.1 BITSTRING

Bitstrings are the main structure of SDM. The addresses are represented in bitstrings, as well as the data. A bitstring is stored as an array of integers. Each integer may be 16-bit, 32-bit, or 64-bit long, depending on the configuration. By default, each integer is 64-bit long.

For instance, a 1,000-bit bitstring will have $\lceil 1000/64 \rceil = 16$ integers. These integers will have a total of $16 \cdot 64 = 1,024$ bits. The remaining 24 bits are always zero, so they do not affect the result of any operation. The memory usage efficiency is $1 - 24/1024 = 97.65\%$. Bitstrings store neither how many bits they have nor the array length. These pieces of information are only stored in the address space.

12.1.1 *The distance between two bitstrings*

The distance between two bitstrings is calculated by the hamming distance, which is the number of different bits between them. It is calculated counting the number of ones in the exclusive or (xor) between the bitstrings, i.e., $d(x, y) =$ number of ones in $x \oplus y$.

There are several algorithms to calculate the number of ones [75], but the performance depends on the processor. So, we have implemented three different algorithms and one may be selected through compiling flags. The default algorithm is to use a built-in __popcnt() instruction from the compiler.

There is also the naive algorithm, which really counts the number of ones checking bit by bit. It is available only to testing purposes and should never be used.

The other algorithm available is the lookup. It pre-calculates a table with the number of ones of all possible 16-bit integers. This table is accessed a few times to calculate the number of ones of a 64-bit integer, i.e., to calculate the distance between two bitstrings, it sums the distance of each 16-bit part of the bitstrings, i.e., $d(x[0:63], y[0:63]) = d(x[0:15], y[0:15]) + d(x[16:31], y[16:31]) + d(x[32:47], y[32:47]) + d(x[48:63], y[48:63])$ where $x[i:i+15]$ and $y[i, i+15]$ are the 16-bit integers formed by the bits between i and $i+15$ of x and y, respectivelly. Each 16-bit distance is calculated through a single table access. As each distance is calculated in O(1), this algorithm runs in $O(\lceil bits/16 \rceil)$. This table uses 65MB of RAM. One may change the table from 16-bit integers to 32-bit integers, which would halve the number of accesses at the expense of 4GB of RAM (instead of 65MB).

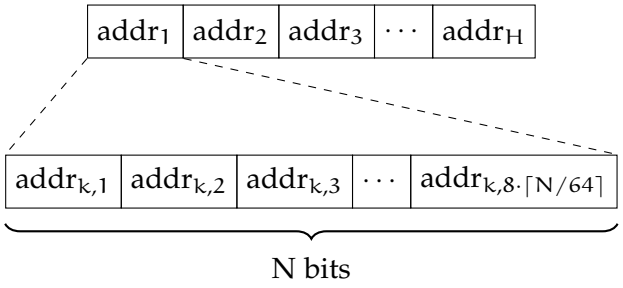


Figure 17: Address space's bitstrings are stored in a contiguous array. In a 64-bit computer, each bitstring is stored in a sub-array of 64-bit integers, with length $8 \cdot \lceil N/64 \rceil$.

12.2 ADDRESS SPACE

An address space is a fixed collection of bitstrings, and each bitstring represents a hard-location address. They store the number of bitstrings, as well as the number of bits, number of integers per bitstring, and the number of remaining bits.

Bitstrings are stored in a contiguous array of 64-bit integers, as shown in Figure 17. Hence, basic pointer arithmetic provides us with performance improvements in their access, as processors realize fetches of contiguous chunks of memory [59].

The scan for activated hard-locations is performed in an address space. It returns the indexes of the bitstrings which were inside the circle (and their distances). Then, each operation uses these pieces of information in a different way.

12.2.1 *Scanning for activated hard-locations*

Scanning for the activated hard-locations is a problem similar to well-known problems in computational geometry called "range reporting in higher dimensions". In this case, none of the known algorithms is able to solve our problem faster than $O(H)$. The algorithm which seems to best fit in our problem consumes $O(H)$ space and runs in $O(\log^n(H))$ [21], which is really slower than $O(H)$ when, for instance, $H = 1,000,000$ and $n = 1,000$. For a review of the range reporting algorithms, see Chan et al. [20].

In 2014, there was published a solution to fast search in hamming space which seems applicable to our problem Norouzi et al. [56]. It provides a fast search when $r/n < 0.11$ or $r/n < 0.06$, where r is the radius and n is the number of bits. But, in our case, for a 1,000 bits SDM, $r/n = 0.451$, which changes the runtime to $O(H^{0.993})$. This is really close to $O(H)$, but with a larger constant. Unfortunately, $O(H)$ is still faster.

It is intriguing that none of those algorithms is able to solve our scanning problem. The idea behind those computational geometry

algorithms is roughly to split the search space in half each step, which would take $O(\log(H))$ to go through the whole space. But this approach does not work because of the high number of dimensions (i.e., 1,000) and because the hard-locations' addresses are randomly sampled from the $\{0,1\}^n$ space. Although each addresses' bit itself splits the hardlocations in half, it does not split the search space in half since both halves still must be convered by the algorithm. For instance, let's say we have $n = 1,000$ dimensions with $H = 1,000,000$ hard-locations, and we are scanning within a circle with radius $r = 451$, then after checking the first bit we have two cases: (i) for the half with the same first bit, we must keep scanning with radius 451; and (ii) for the half with a different first bit, we must keep scanning with radius 450. Hence, the search space has not been split in half because both halves have been covered (and one of them should have been skipped).

Finally, as our best approach is to scan through all hard-locations, we may distribute the scan into many tasks which will be executed independently. The tasks may be executed in different processes, threads, or even computers. They may also run in the CPU or in the GPU. In this case, we may take into account both the time required to distribute the tasks and the time to receive their results.

The framework implements three main scanner algorithms: linear scanner, thread scanner, and OpenCL scanner. The linear scanner runs in a single core, is the slowest one, and was developed only for testing purposes; the thread scanner runs at the CPU in multiple threads sharing memory (and our recommendation is to use the number of threads equals to twice the number of CPU cores); and the OpenCL scanner runs in multiple GPU cores and support multiple devices. The speed of a scan depends on the CPU and GPU devices, thus the best approach to choose which scanner is best for one's setup is to run a benchmark.

The OpenCL must be initialized, which just copies the address space's bitstrings to the GPU's memory. Then, many scans may be executed with no necessity to upload the bitstrings again. The OpenCL scanner supports running into multiple devices.

12.3 COUNTERS

Each hard-location has one integer of data per bit. For instance, each hard-location of a 1,000 bits SDM has 1,000 bits. Those integers are stored in a counter.

A counter is an array of integers which stores the data of all hard-locations. So, the counter's array has $n \cdot H$ integers.

When two counters are added in a third counter, there may occur an overflow. It is not supposed to be a problem because, by default, each counter is a signed 32-bit integer that can store any number

between -2,147,483,648 and 2,147,483,647, which means they will not overflow with less writes than $2^{31} - 1$ divided by the average number of activated hard-locations. For instance, when $n = 1,000$, $H = 1,000,000$, and $r = 451$, the average number of activated hard-locations is 1,000 and it would require at least one million writes before being possible to a counter to overflow. Note also that it would be more likely to saturate the memory before any overflow.

Anyway, counters may have overflow protection depending on compiling options. By default, there is no overflow check for performance reasons (and because it does not seem necessary).

12.4 READ AND WRITE OPERATIONS

The reading and writing operations are executed in two steps: first, the address space is swept looking for the activated addresses; then, the operation is performed in the counters. Reading operation assemblies the bitstring according to the counters of the activated addresses, while the writing operation changes the counters.

The iterated reading keeps reading until it gets exactly the same bitstring (or the number of maximum interations has been reached), i.e., it performs $\eta_{i+1} = \text{read}(\eta_i)$ and stops when $\eta_{k+1} = \eta_k$. If the initial bitstring is inside the critical distance of η, it will converge to η, but, if it is not, it will diverge and reach the maximum number of iterations.

The framework has both Kanerva's read and the generalized read. The latter was implemented according to the generalization proposed by professor Paulo Murilo. The generalization brings a parameter z, which is the exponent. In this case, the results are floating point instead of integer, which considerably reduces performance. When $z = 1$, it is exactly as the Kanerva's read. When $z = 0$, it is the Chada's read. We also explored how SDM would behave for different values of z.

There is another special read operation: the weighted reading. In the weighted reading, the value of the counters are multiplied by a weight which depends only on the distance between the reading address and the hard-location address. The weight is retrieved from a lookup table of integers indexed by the distance. The rest of the read operation is exactly the same.

There is also a weighted writing operation. In this case, the weight is applied when the counters are updated, i.e., if the weight is 2, the counters are increased twice when bits are 1, and decreased twice when bits are 0. Just as in the weighted reading, the weights depend only on the distance between the writing address and the hard-location address. The weights are retrieved from a lookup table of integers indexed by the distance.

13

RESULTS (I): FRAMEWORK VALIDATION

The framework has been validated comparing its results with the expected results from Kanerva [41]. Thus, we run simulations which were then compared to the theoretical analysis conducted some decades ago.

The objective here is twofold: (i) a single command will install the framework, and (ii) another single command will run (and display) the desired figures obtained the simulation. This will allow potential users to become familiarized with the system and its underlying code with barely any learning curve beyond scientific python and jupyter notebooks.

One particular analysis of interest is that of the distance read at a point α. Suppose an SDM is trying to read an item written at α, but the cues received so far lead to a point of distance d from α. As one reads at $\alpha + d$, a new bitstring β is obtained, leading to our question: what is the new distance from α to β? Is it smaller or larger than d? That, of course, depends on the ratio between d and the number of dimensions of the memory. As we have found out, there are some deviations from Kanerva's original theoretical analysis and the results obtained by simulation.

13.0.1 *Some initial anomalous results*

As we ran the simulations reflecting some of Kanerva's graphs, one in particular struck our attention: The new distances obtained after a read operation were not perfectly predicted by the theoretical model, and we propose that this is due to interaction effects between different attractors.

Kanerva [41] originally predicted a ~500-bit distance after a point (Fig. 18). The original prediction considered that the read distance would decline when inside the critical distance in increase afterwards, converging to a ~500-bit distance. At this point, each read would lead to a different, orthogonal, ~500-bit distance point.

Our preliminary results show that the theoretical prediction is not accurate. There are interaction effects from one or more of the attractors created by the 10,000 writes, and these attractors seem to raise the distance beyond ~500 bits (Fig. 19). Our results were obtained using a 1,000 bit, 1,000,000 hard-location SDM with exactly 10,000 random bitstrings written into it, the same used by Kanerva.

But, when we reduced the number of random bitstrings written in the SDM from 10,000 to only 100, the results reflected very well the

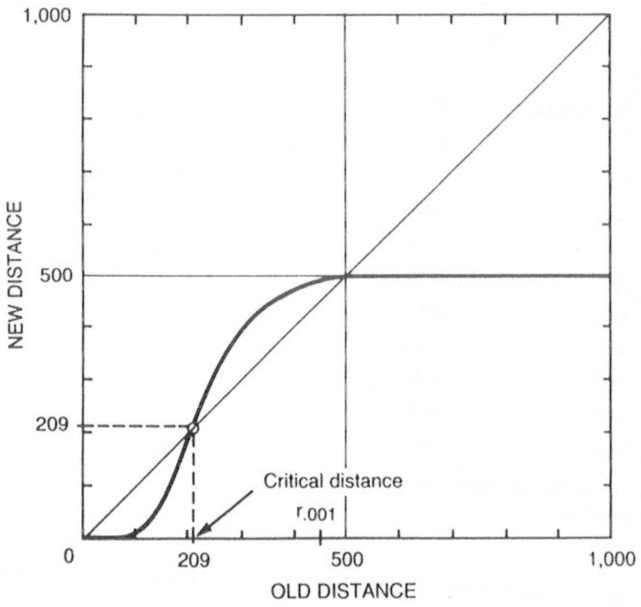


Figure 7.3
New distance to target as a function of old distance.

Figure 18: Kanerva's original Figure 7.3 (p. 70) predicting a ~500-bit distance after a point.

Kanerva's theoretical expectation (Fig. 20). This result strengthens our hypothesis that the disparities in the computational results are due to the interaction effect of high numbers of different attractors.

To obtain the results from Fig. 19 and 20, we had to write 10,000 random bitstrings to an SDM, and then randomly choose one of those bitstrings to be our origin. Finally, we randomly flipped some bits from the origin bitstring and executed a reading operation in the SDM. Thereby, in order to show the interaction effects more clearly, we wrote a handmade bitstring to the SDM which had all bits inverted in relation to the origin bitstring — their hamming distance was equal to 1,000. Our handmade bitstring was acting as an opposite attractor, and one can see the accelerating effects towards convergence to both attractors: the origin and the handmade bitstrings (Fig. 21). Here we had the exact same configuration of Figure 19, with the addition of the single opposite attractor.

Obviously, these small deviations from Kanerva's original theoretical predictions deserve a qualification. Kanerva was working in the 1980s and the 1990s, and had no access to the immense computational power that we do today. It is no surprise that some small interaction effects should exist as machines allow us to explore the ideas of his monumental work.

Physicist Paulo Murilo observed that the models of Kanerva-read ($z = 1$) and Chada-read ($z = 0$) were simple variations of the exponent

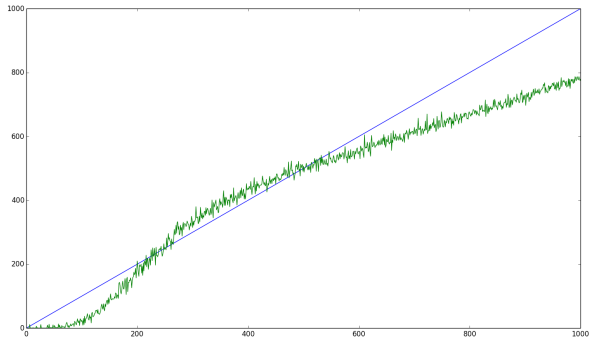


Figure 19: Results generated by the framework diverging from Kanerva's original Table 7.2. Here we had a 1,000 bit, 1,000,000 hard-location SDM with exactly 10,000 random bitstrings written into it, which was also Kanerva's configuration.

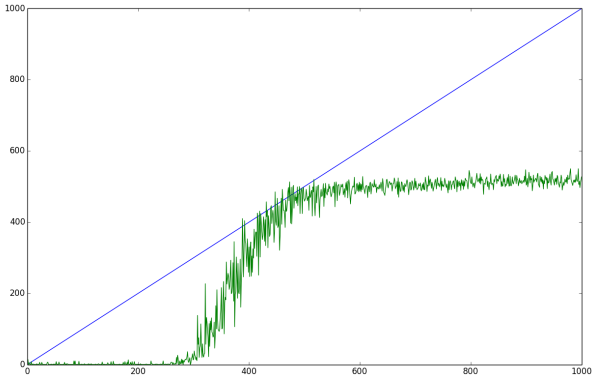


Figure 20: Results generated by the framework similar from Kanerva's original Table 7.2. It was a 1,000 bit, 1,000,000 hard-location SDM with exactly 100 random bitstrings written into it.

z, which suggests experimenting with different values. The results, however, have not yielded performance improvements. Though for $z \leqslant 1$ results are comparable to $z = 1$, for $z > 1$, the system shows a clear deterioration, with a smaller distance to convergence and higher divergence at large-distance reads. This is shown in Figure 22.

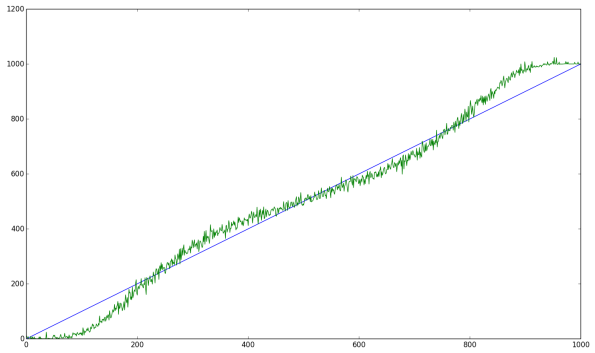
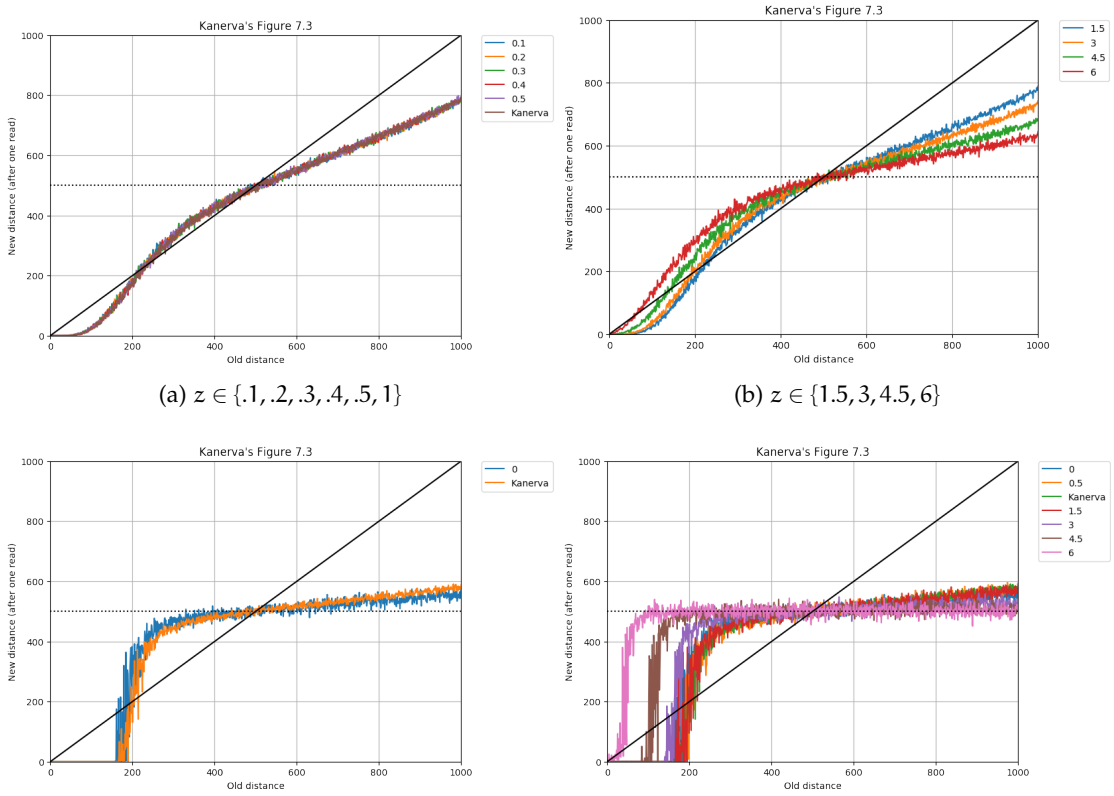


Figure 21: This graph shows the interaction effects more clearly. As we include an opposite bitstring, one can see the accelerating effects towards convergence to both attractors: the origin and the opposite. Here we have the exact same configuration of Figure 19, with the addition of the single opposite attractor.



(a) $z \in \{.1, .2, .3, .4, .5, 1\}$

(b) $z \in \{1.5, 3, 4.5, 6\}$

(c) $z \in \{0, 1\}$

(d) $z \in \{0, 0.5, 1, 1.5, 3, 4.5, 6\}$

Figure 22: (a) and (b) show the behavior of a single read; (c) and (d) present the effects of 6 iterative reads. As stated previously, we can see a deterioration of convergence, with lower critical distance as $z > 1$. Another observation can be made here, concerning the discrepancy of Kanerva's Fig 7.3 and our data. It seems that Kanerva may not have considered that a single read would only 'clean' a small number of dimensions *after the critical distance*. What we observe clearly is that with a single read, as the distance grows, the system only 'cleans' towards the orthoghonal distance 500 after a number of iterative readings.

14

RESULTS (II): PERFORMANCE

Our intention is to provide comparative performance metrics under different computation engines (CPU, GPU, etc) and different operating systems (Linux, MacOs, Windows, etc). Performance can be measured as the average number of scans of all hard locations per second, reads per second, writes per second, etc.

Our first device is a personal MacBook Pro Retina 13-inch Late 2013 with a 2.6GHz Intel core i5 processor, 6GB DDR3 RAM, and Intel Iris GPU. We also intend to test on machines such as the iMac with dedicated GPU, MacPro with dedicated GPU, and personal computers under Linux with dedicated GPUs.

Beyond that, we are running as state-of-the-art devices: (i) an Amazon EC2 p3.xlarge with Intel Xeon E5-2686v4 processor, 61GB DDR3 RAM, and NVIDIA K80 GPU, and (ii) an Amazon EC2 p3.8xlarge with Intel Xeon E5-2686v4 processor, 488GB DDR3 RAM, and 8x NVIDIA K80 GPU.

15

RESULTS (IV): SUPERVISED CLASSIFICATION APPLICATION

Supervised classification problem consists of categorize data into groups after seeing some samples from each group. First, it is presented pieces of data with their categories. The algorithm learns from these data, which is known as learning phase. Then, new pieces of data are presented and the algorithm must classify them into the already known groups. It is named supervised because the algorithm will not create the groups itself. It will learn the groups from during the learning phase, in which the groups have already been defined and the pieces of data have already been classified into them.

Although this problem has already been studied (REF), our intention here is to show that a pure SDM may also be used to classify data. Fan and Wang [32] has used SDM to solve a classification problem, recognizing handwriting letters from images, but he used a mix of genetic algorithm with SDM, which is very different from the original SDM described by [41]. Even though his algorithm has classified properly, we were intrigued whether a pure SDM would also classify successfully.

Hence, we have developed a supervised classification algorithm based on a pure SDM as our main memory. Our goal was to classify noisy images into their respective letters (case sensitive) and numbers. For some examples, see Figure 23.

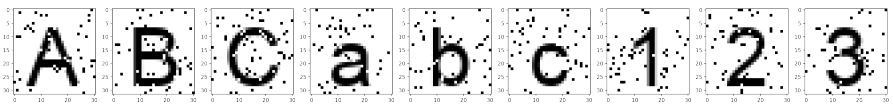


Figure 23: Examples of noisy images with uppercase letters, lowercase letters and numbers.

The images had 31 pixels of width and 32 pixels of height, totaling 992 pixels per image. Each image was mapped into a 1,000 bit bitstring in which the bits were set according to the color of each pixel of the image. So, white pixels were equal to bit 0, and black pixels to bit 1. The 8 remaining bits were all set to zero. This was a bijective mapping (or one-to-one mapping), i.e., there was only one bitstring for each image, and there was only one image for each bitstring.

A total of 62 classification groups have been trained in the SDM. For each of them, it was generated a random bitstring. Thus, the groups' bitstrings were orthogonal between any two of them. There is one

image for each of the 62 groups in Figure 24. Notice that the SDM has never seen a single image with no noise.

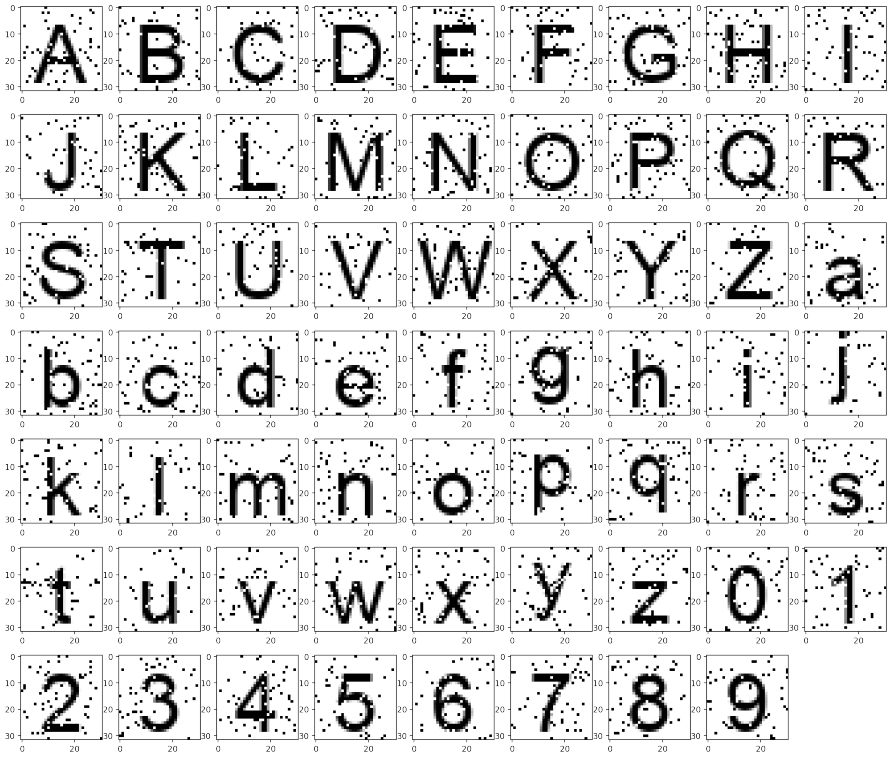


Figure 24: One noisy image for each of the 62 classification groups.

The association of images to groups was stored as sequences in SDM, as detailed by Kanerva [41] in Chapter 8. During the learning phase, the image bitstrings were stored pointing to their groups bitstrings, i.e., write(addr=bs_image, datum=bs_label). Thus, in order to classify an unknown image, we only had to read from its address and check which group has been found.

During the learning phase, we have generated 100 noisy images for each character. The images had 5% of noise, i.e., 5% of their pixels have been randomly flipped. For example, see the generated images for letter A in Figure 25. Then, we have wrote the classification group bitstring into the bitstring associated to each noisy image, i.e., write(bs_image, bs_label). For a complete image training set, see Appendix XYZ.

Finally, we have assess the performance of our classifier. We had done it in three different scenarios: high noise (20%), low noise (5%) and no noise. See Figures 26 and 27 for images with 20% noise and no noise. The low noise scenario had the same noise as the training set. For each scenario, we had classified 620 unknown images with 10 images per group.

The performance was calculated as the percentage of hits for each group. We did not expected the same performance for all groups

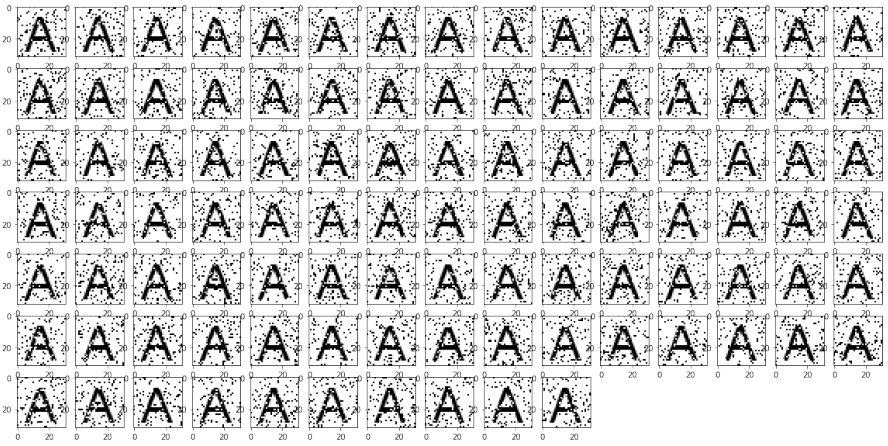


Figure 25: 100 noisy images generated to train label A.

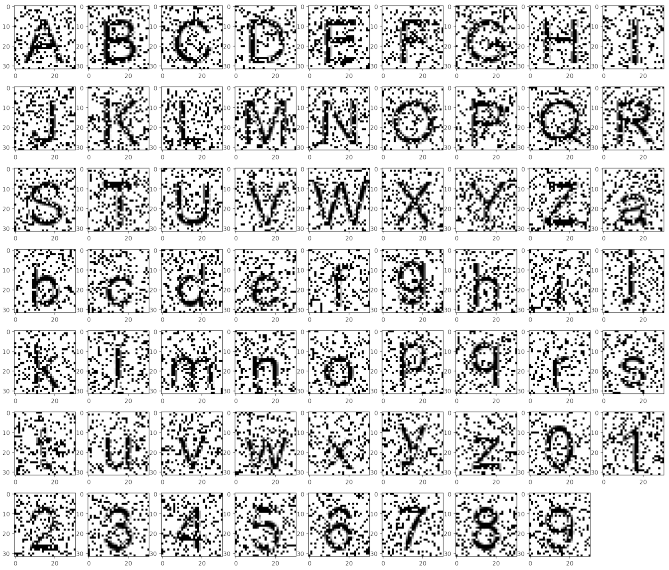


Figure 26: Images generated using a 20% noise for the high noise scenario.

because some groups become very similar to other depending on the noise level, and this similarity may even confuse a person (see Figure 28).

In the no noise scenario, the classifier has hit all characters, except letter "l" which was wrongly associated to the group of "i". We believe that it happened because the classifier had never seen an image with no noise and the difference between the images of "l" and "i" is smaller than the critical distance. So, both groups have been merged and it would converge to only one of them. In our simulation, it happened to be the group of "i".

In the low noise scenario, it has made few mistakes. It correctly classified all images but some from characters "b", "e", "f", "l", "t", and "9". It completely classified "l" images to the "i" group. In the

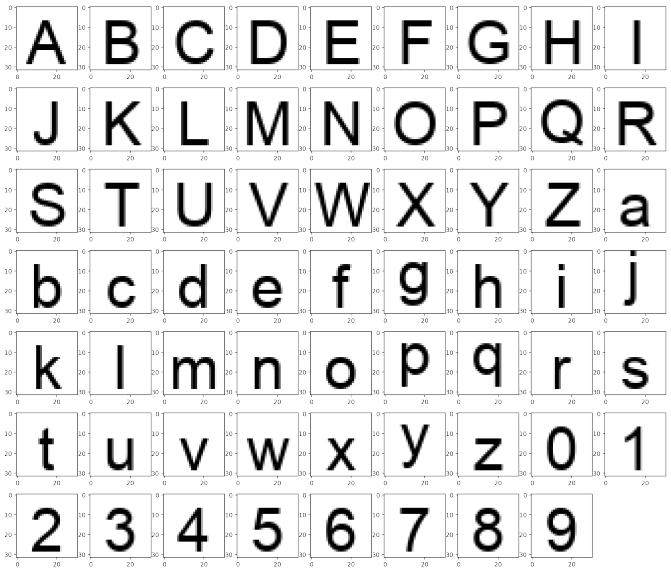


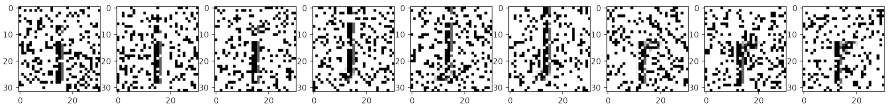
Figure 27: Images generated for the no noise scenario.

other cases, it made just a few mistakes. See Figure 29 to check the images and their classification.

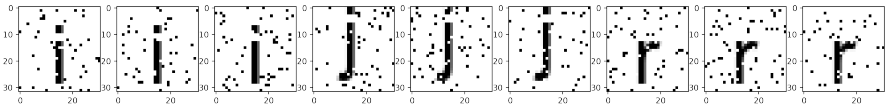
The high noise scenario is the most interesting, because, even in a high noise level, the classifier has hit most of the characters. It has hit all images for 44 out of 62 groups, and made at least one miss for the other 18 groups. The misses may be seen in details in Figure **??**.

The critical distance plays an important role in the classification error. As we have 62 groups and each have been trained with 100 images, there were 6,200 writes to the memory. When an image is being classified, it will have to converge to a group, and the convergence depends on the distance between this image and the images from the training set, i.e, in the noise level.

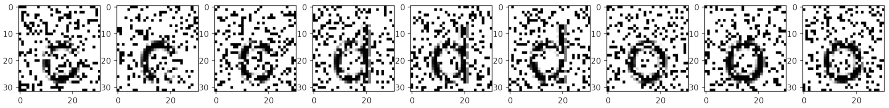
These results show that the SDM may be used as a supervised classification algorithm. Although we do not believe that the mapping between images and bitstrings are even close to the way human cognition deals with images, we believe the results are interesting and useful to many possible real world problems.



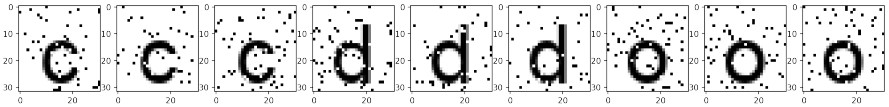
(a) “i”, “l”, and “r” with 20% noise.



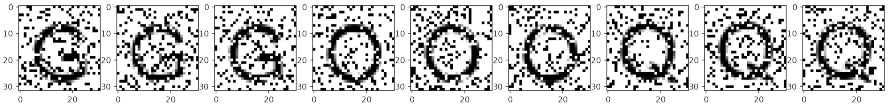
(b) “i”, “l”, and “r” with 5% noise.



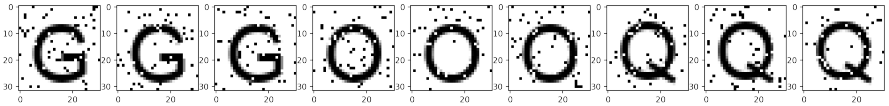
(c) “c”, “d”, and “o” with 20% noise.



(d) “c”, “d”, and “o” with 5% noise.

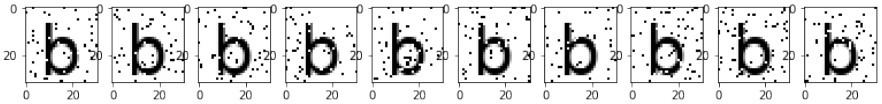


(e) “G”, “O”, and “Q” with 20% noise.

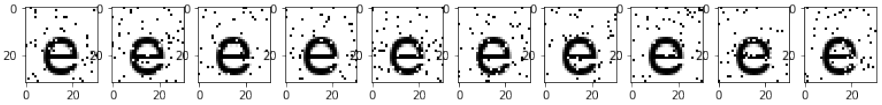


(f) “G”, “O”, and “Q” with 5% noise.

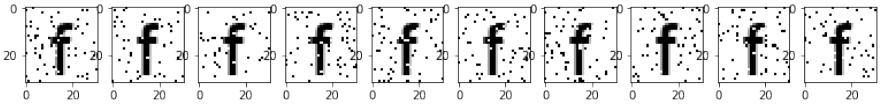
Figure 28: Images of different characters which may be confusing depending on the noise level.



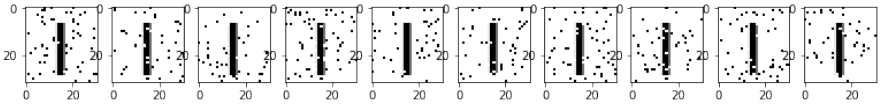
(a) Images from character "b which were classified as [b, b, b, h, b, o, b, h, b, b], respectively. It has made 3 misses.



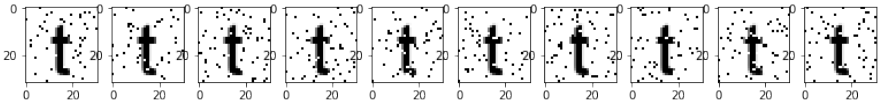
(b) Images from character "e which were classified as [e, e, e, e, e, e, e, e, o, e], respectively. It has made 1 miss.



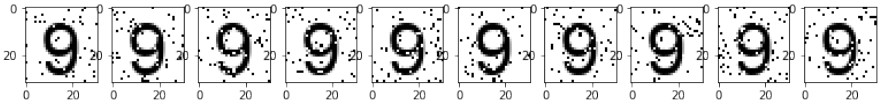
(c) Images from character "f which were classified as [i, f, f, I, I, I, f, f, f, f], respectively. It has made 4 misses.



(d) Images from character "l" which were classified as [i, i, i, i, i, i, i, i, i, i], respectively. It has missed them all, as if both groups have been merged.

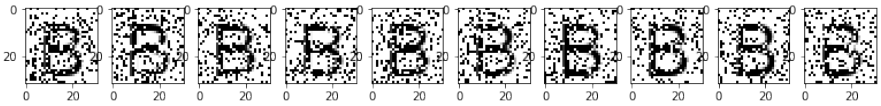


(e) Images from character "t" which were classified as [t, t, t, t, t, t, t, i, t, t], respectively. It has made 1 miss.

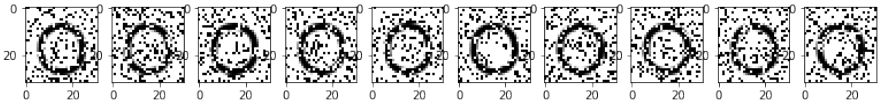


(f) Images from character "9" which were classified as [9, 9, o, 9, 9, 9, o, o, 9, 9], respectively. It has made 3 misses.

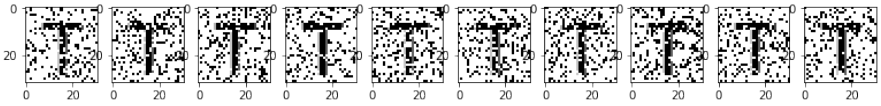
Figure 29: Characters in the low noise scenario in which the classifier has made at least one mistake. In all the other cases, it correctly classified the images. We may notice that the groups of "i" and "l" have been completely merged by the classifier, because it cannot distinguish them, not even with no noise.



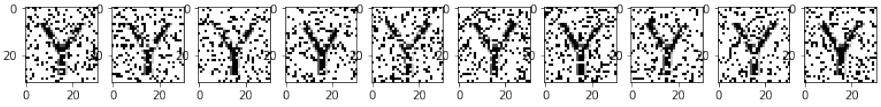
(a) Images from character “B” which were classified as [S, B, B, B, B, B, B, B, B, B]. It has made 1 mistake.



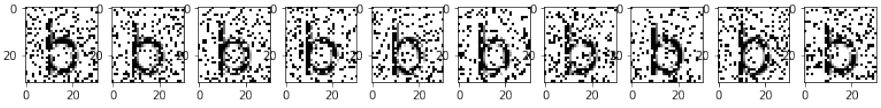
(b) Images from character “O” which were classified as [G, G, O, O, O, O, O, O, O, O]. It has made 2 mistakes.



(c) Images from character “T” which were classified as [T, T, T, T, T, I, T, T, T, T]. It has made 1 mistake.



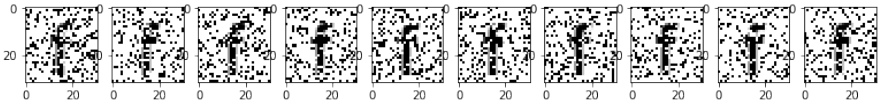
(d) Images from character “Y” which were classified as [Y, I, Y, Y, Y, Y, Y, Y, Y, Y]. It has made 1 mistake.



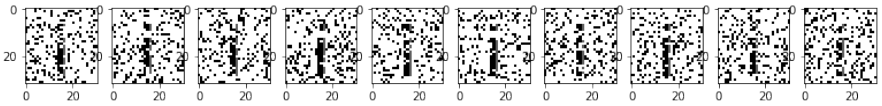
(e) Images from character “b” which were classified as [o, o, o, b, o, h, h, b, b, o]. It has made 7 mistakes.

(f) Images from character “c” which were classified as [c, c, c, c, c, o, c, c, c, o]. It has made 2 mistakes.

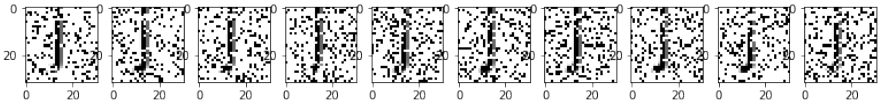
(g) Images from character “e” which were classified as [e, o, e, o, o, o, e, o, o, e]. It has made 6 mistakes.



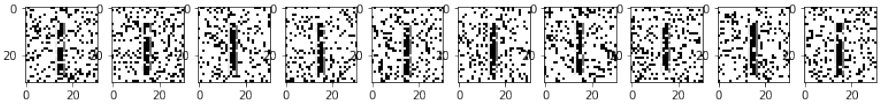
(h) Images from character “f” which were classified as [I, I, I, I, i, I, I, I, I, I]. It has missed them all.



(i) Images from character "i" which were classified as [i, i, i, I, i, i, i, i, I, i]. It has made 2 mistakes.

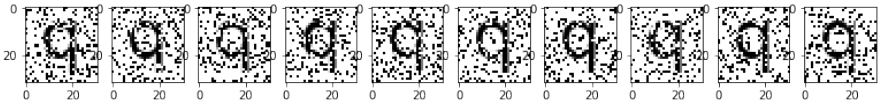


(j) Images from character "j" which were classified as [j, j, j, I, I, j, j, j, I]. It has made 3 mistakes.

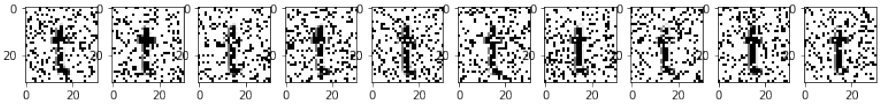


(k) Images from character "l" which were classified as [I, i, I, I, I, I, i, I, I, i]. It has missed them all.

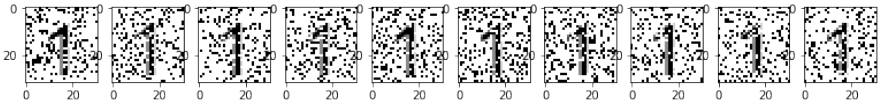
(l) Images from character "n" which were classified as [u, n, n, n, n, n, u, u, u, h]. It has made 5 mistakes.



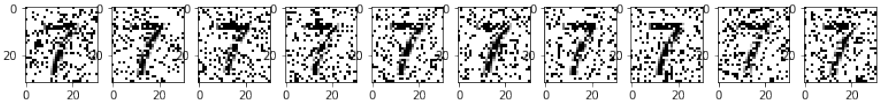
(m) Images from character "q" which were classified as [q, q, q, q, q, q, q, q, q, g]. It has made 1 mistake.



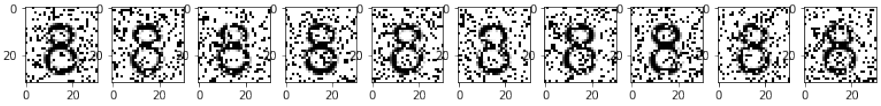
(n) Images from character "t" which were classified as [I, r, I, i, I, i, i, I, i]. It has missed them all.



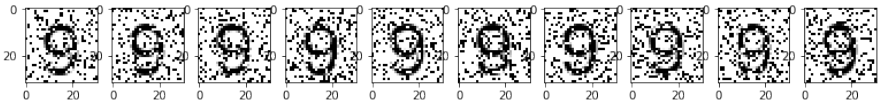
(o) Images from character "1" which were classified as [1, I, 1, I, 1, 1, I, I, 1, I]. It has made 5 mistakes.



(p) Images from character "7" which were classified as [7, 7, 7, I, 7, I, I, 7, 7, 7]. It has made 3 mistakes.



(q) Images from character "8" which were classified as [8, 6, 6, 6, 8, d, 8, 8, d, 6]. It has made 6 mistakes.



(r) Images from character "9" which were classified as [9, 0, 6, 0, 9, 0, 0, 9, 0, 0]. It has made 7 mistakes.

Figure 28: Characters in the high noise scenario in which the classifier has made at least one mistake. In all the other cases, it correctly classified the images.

16

RESULTS (III): SUPERVISED IMAGE NOISE FILTERING APPLICATION

Image noise filtering consists in removing the noise from an input, in out case an image. Our images are black & white images and the noise is generated randomly flipping some of their pixels from black to while and vice versa. In Figure 29, we may see an image with different levels of noise, from 0% to 45% in steps of 5%. It makes no sense to apply 50% of noise because it would absolutely randomize the image.

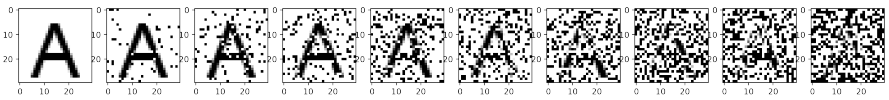


Figure 29: Progressive noise into letter "A", from 0% to 45% in steps of 5%.

The images have 30 x 30 pixels, totaling 900 pixels per image. Each image is mapped into a 1,000 bit bitstring in which the bits are set according to the color of each pixel of the image. White pixels are equal to bit 0, and black pixels to bit 1. The 100 remaining bits are all set to zero. This is a bijective mapping (or one-to-one) from images and bitstrings, i.e., there is one, and only one, bitstring for each image, and vice versa.

In the learning phase, noisy images are generated and they are written into SDM chunked with their labels. The chunk was calculated using the exclusive or (XOR) operator. So, the image bitstring was written to the address of its bitstrings XOR its label bitstring — write(addr=bs_image XOR bs_label, datum=bs_image).

Finally, in order to remove the noise of a new image, first we have to classify it (possibly using the already presented classification algorithm), and then we just have to read from the chunked address until it converges.

17

RESULTS (V): THE POSSIBILITY OF UNSUPERVISED REINFORCEMENT LEARNING

Reinforcement learning has increasing prominence in the media after AlphaZero has won all games from both the best chess grandmasters in the world and the best chess engines. What is incredible about these victories is that AlphaZero has almost no knowledge about chess game and has learned all its movement playing against itself for 4 hours. Basically, it knowns only the valid movements and had to learn everything from scratch, which it did using a reinforcement learning algorithm.

Reinforcement learning is a machine learning algorithm which learns from the rewards of its actions. So, it receives the game state as input, then it decides which action will be taken, and finally it learns from the rewards of all the actions it has chosen. In theory, it learns after each reward feedback it receives, improving its decision over time and presenting intelligent behavior. A positive reward would indicate that the chosen action should be encouraged. While a negative reward would indicate the opposite. In some algorithms, there may be a neutral reward which would indicate that the chosen action was neither positive nor negative. How each type of reward should be handled depends on each algorithm.

We have done some experiments with an SDM as a memory for a TicTacToe player. Basically, it receives the current board state and returns which action should be played. In the end of the game, it receives the sequences of boards and the winner, and is supposed to learn from them.

Our algorithm to decide what should be player is very simples: it read the current board from SDM. If the reading converges to another board, it chooses the movement which would bring the current board to the one read from SDM. If the reading does not converge, it just play randomly.

After a game has finished, it is time to learn from its decisions. Thus, if SDM wins the game, it will write the whole sequence of boards to SDM. Let $b_0, b_1, b_2, \ldots, b_n$ be the board sequence of the game (see Figure 30). Then it will write $b_0 \to b_1 \to b_2 \to \cdots \to b_n$, with possibly different weights for each transition. If it loses, it will reverse the board (replace X by O and vice versa), and will act as if it had won. Hence, it will learn which sequences lead to victory. When a new board appears, it may have already seen that situation and will decide according to the sequences which goes towards victory. This is our positive reward learning.

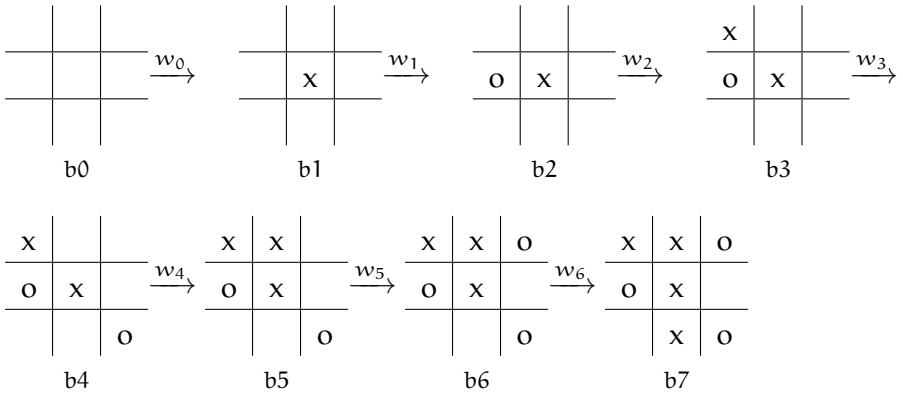


Figure 30: Example of a game with 7 movements in which X wins.

It is also important to learn when a draw happens — after all, it is better to tie than to lose, right? In this case, the sequence of boards is also written to SDM, but with no weight at all. So, if the board has appeared both in a tie sequence and in a winning sequence, it would be more likely to choose the winning one because it was written with greater weight. This is our neutral reward learning.

Finally, we also want to prevent losing games. So, when it loses a game, it will stimulate movements different from the chosen ones. Thus, for each transition $b_k \to b_{k+1}$ made by its action, it will write all possible transitions from b_k but b_{k+1}.

Internally, every board is mapped into a random bitstring and passed to SDM. Thus, SDM knows nothing about the boards themselves. It knowns only about their transition and which ones would lead to either a victory or a draw. As every two boards are orthogonal, SDM does not known whether two boards are consecutives or not. The only link between two boards is the transition written in SDM.

After all, SDM knowns nothing about the boards themselves and yet it may learn how to play TicTacToe.

In order to properly run the discussed algorithms, it is necessary to have two SDMs: a 0-fold and a 1-fold SDM. In the 0-fold SDM, every bitstring is written to its own address. In the 1-fold SDM, every bitstring points somewhere else. So, the transitions are written in the 1-fold SDM, while the boards themselves are written to the 0-fold SDM. The boards are written only once in the 0-fold, no matter how many times they appear. The transitions may be written more than once in the 1-fold SDM, because it would reinforce that transition.

In more details, the next movement decision consists in one read from the 1-fold SDM, resulting in a bitstring. Then this bitstring is used in an interative reading from the 0-fold SDM, which will converge to the bitstring associated with the next board. If it does

not converge to any board, than SDM will choose a random movement and learn from it.

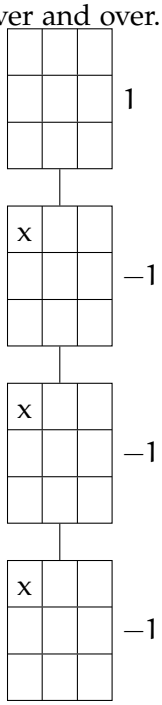
The weight used when writing a winning sequence is calculated using ...

— talk about player generations —

17.0.1 *Training*

It is an unsupervised algorithm because SDM learns playing against an opponent, who may be another SDM player, a human, or a player whose movements are always aleatory.

Thus, in order to train a SDM player, we just have to keep it playing over and over.



17.0.2 *Results*

18

RESULTS (VI): INFORMATION-THEORETICAL WRITE OPERATION

My advisor, Alexandre Linhares, has proposed another read operation: an information-theoretical weighted reading. In it, the sum of the counter's value is weighted based on the distance between each hard-location's address and the reading address. The logic behind it is to vary the importance of each hard-location inside the circle. It is only natural that one encodes an item in near hard locations with a stronger signal, and a natural candidate for this signal function is the amount of information contained in the distance between the item and each hard location. Closer hard locations have lower probabilies and therefore should encode more information.

Consider the following. Information Theory [25] let us compute the precise amount of information in an event, when given its probability p, through the measure of *self-information*:

$$I(p) = -\log_2(p).$$

Now, given any two n-sized bitstrings, the probability of their Hamming distance being d is given by,
$p(H = d) = 2^{-n}\binom{n}{d}$

And the probability of it being at most d is

$$p(H \leqslant d) = 2^{-n}\sum_{i=0}^{d}\binom{n}{i},$$

and, consequently,

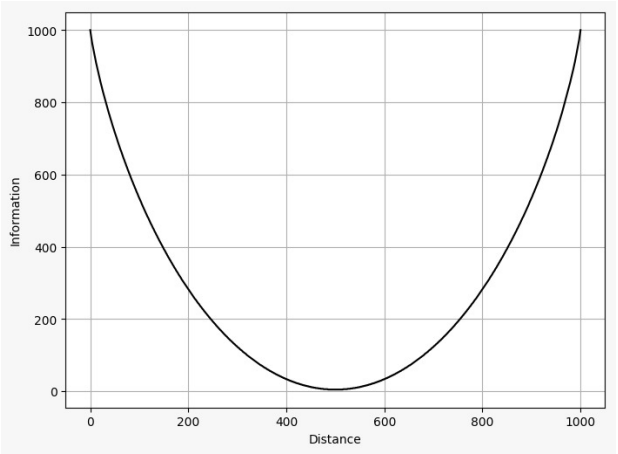
$$p(H \geqslant n-d) = 2^{-n}\sum_{i=n-d}^{n}\binom{n}{i},$$

$$p(d+1 \leqslant H \leqslant n-d-1) = 2^{n} - 2^{1-n}\sum_{i=0}^{d}\binom{n}{i}, \forall d < n/2.$$

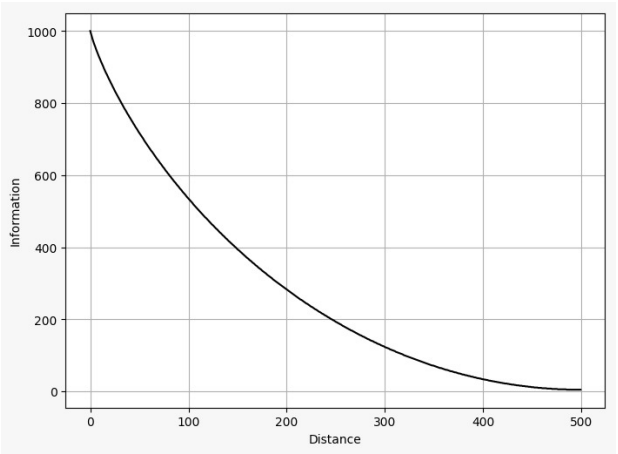
Hence the weighted write would, on each hard location, sum (or subtract) the following:

$w(d) = -\log_2\left(2^{-n}\binom{n}{d}\right) = n - \log_2\binom{n}{d}$, as seen in Figure 31.

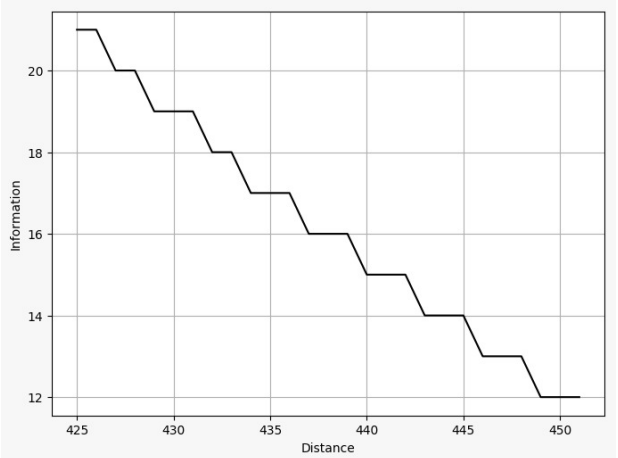
It is easy to interpret this data though a binary tree approach. How many binary questions would be needed to precisely define a bitstring?



(a) $w(d), d \in \{1, 2, ..., n\}$.

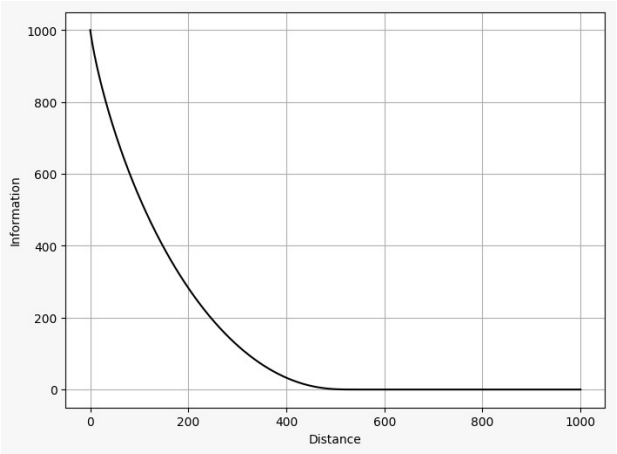


(b) $w(d)$ for the desired range.

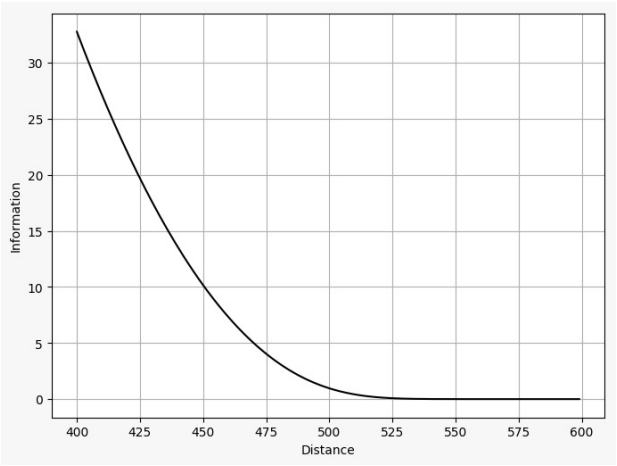


(c) stepwise $\lfloor w(d) \rfloor$ for fast integer computation.

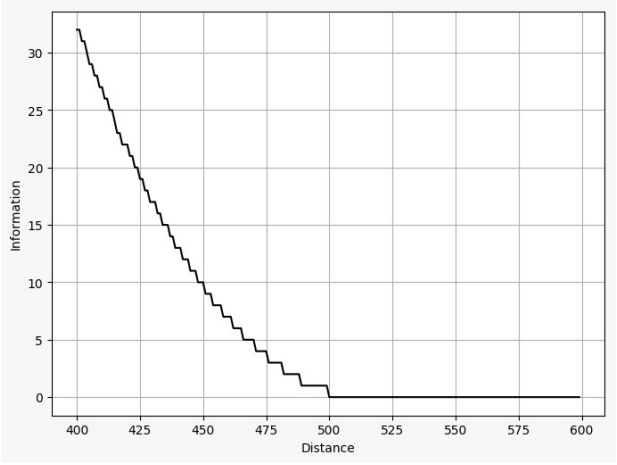
Figure 31: Computing the amount of information of a signal to each hard location in its access radius. (a) entirety of the space; (b) region of interest; (c) Fast computation is possible through a stepwise function.



(a) $w(d), d \in \{1, 2, ..., n\}$.

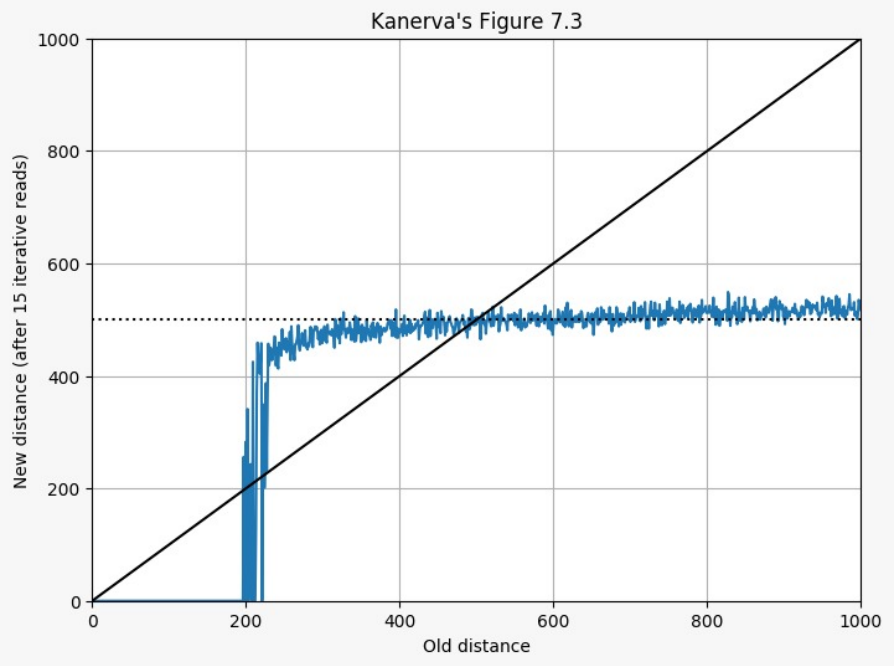


(b) $w(d)$ for the desired range.

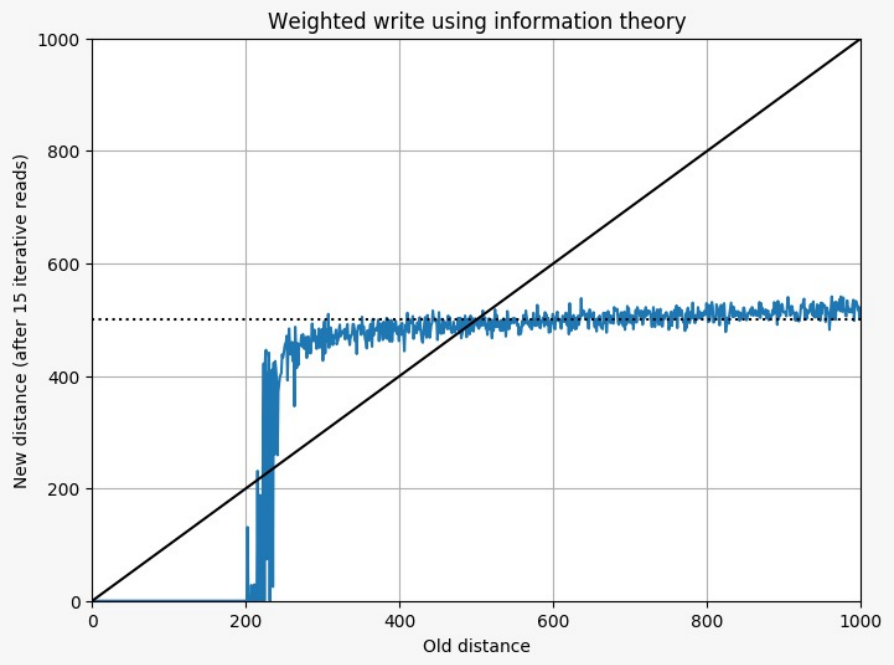


(c) stepwise $\lfloor w(d) \rfloor$ for fast integer computation.

Figure 32: Computing the sum of low-likelihood signals. (a) entirety of the space; (b) region of interest; (c) Fast computation through a stepwise function.



(a) Kanerva's model



(b) Write process weighted by the amount of information contained in the distance between the written bitstring and each hard location

Figure 33: (a) and (b) show the behavior of the critical distance under Kanerva's model and the information-theoretic one, respectively.

Another possibility would be to use the sum of all distances closer (and less likely) locations within the weighting function $w(d)$,

$$w(d) = -\log_2\left(2^{-n}\sum_{i=0}^{d}\binom{n}{i}\right) = n - \log_2\sum_{i=0}^{d}\binom{n}{i}.$$

This can be seen in 32.

The results can be seen in Figure 33 and seem promising. It seems that the critical distance increases by a number of bits. Note that 10 additional bits imply an attractor 2^{10} of the size of the original. Another point to keep in mind is that, since the modulus of the vectors are not uniform in this approach, that the shape of the attractor may have asymmetries.

Note, finally, that this is not the first time in which a weighted function has been applied to writing in SDM — Hely et al. [38] suggest a rather complex spreading model based on floating point signals in the interval [0.05, 1.0] — they were, however, only able to test their model with 1,000 hard locations.

19 CONCLUSION

Sparse Distributed Memory is a viable model of human memory, yet it does require researchers to (re-)implement a number of parallel algorithms in different architectures.

We propose to provide a new, open-source, cross-platform, highly parallel framework in which researchers may be able to create hypotheses and test them computationally through minimal effort. The framework is well-documented for public release at this time (http://sdm-framework.readthedocs.io), it has already served as the backbone of Chada's Ph.D. thesis. The single-line command "pip install sdm" will install the framework on posix-like systems, and single-line commands will let users test the framework, generate some of the figures from Kanerva's theoretical predictions in their own machines, and — if interested enough —, test their own theories and improve the framework, and the benchmarks used to evaluate the framework, in open-source fashion. It is our belief that such work is a necessary component towards accelerating research in this promising field.

19.1 FUTURE WORK

Here are interesting questions that have been considered during this work, but have had to be left for future research.

19.1.1 *Multiple levels*

19.1.2 *i versus l*

19.1.3 *Magic numbers*

Kanerva suggests, in his book, the use of 1,000 dimensions and 1,000,000 hard locations. More recently, he suggested the use of 10,000 dimensions.

Each parameter set choice like this will lead to particular numbers — many of them emergent—, such as the access radius size, critical distance, and so forth.

One intriguing question here is: is there a 'better' number of dimensions and of hard locations? If so, can such numbers better studied analitically, or numerically?

How should these parameters be compared? What are the tradeoffs that should be considered? What are the 'best' benchmarks possible?

19.1.4 *Classification with context using sequences — for words instead of only letters*

19.1.5 *Symmetrical, rapidly accessible, Hard Locations*

A hypercube with n dimensions can be divided by two hypercubes with $n-1$ dimensions. Is there an algorithm that separates the area of each hard-location in such a form that there exists a function mapping each bitstring in $\{0,1\}^n$ to the set of hard locations it 'belongs to'? Though this would break Kanerva's assumption of a randomly yet uniformly distributed set of hard locations — for a perfectly symmetrical set of hard locations —, there could be large performance gains if such a mapping function from a bitstring to its corresponding set of nearest hard locations exists.

$\forall b \in \{0,1\}^n$, we want an algorithm A that yields the particular list of hard locations for b and all hard locations respect the desired properties of the memory.

19.1.6 *Docker image and jupyter notebooks*

We have generated a Docker image, which makes it even easier to explore the framework. After running the container, a Jupyter Notebook is available with sdm-framework and other tools already installed. The simulations run in this thesis are promptly available to be re-executed and explored. We invite readers to take a look and explore a little bit.

19.1.7 *From theory to a platform.*

Platforms in the history of computing.

Opens 10 doors.

20

APPENDIX

Part IV

DIFFUSION AND DISMISSAL OF INNOVATION: FORECASTING THE NUMBER OF FACEBOOK'S ACTIVE USERS

21 INTRODUCTION

The way innovations diffuse in the market is an important and useful topic in marketing, which was made popular through Rogers' work [66] and has influenced many marketing researchers. Within innovation diffusion, Bass [7] proposed a model which forecasts how many people will have adopted new products or technologies by a given point in time. INFORMS members have voted this model as one of the Top 10 Most Influential Papers published in the 50-year history of Management Science in connection with the 50th anniversary of the journal [8].

The Bass [7] model was designed to forecast only innovation adoption, which is the first time one consumes the innovation. In the model, either the consumer has or has not consumed the innovation by a given point in time. Thus, recurrent customers are considered only once, because they have already consumed the innovation before. The model has only three parameters, which are estimated through the number of adoptors of the innovation. Though very simple, it is considered very robust.

Although it is clear that the marketing investment, the product prices, the economy itself, and many other variables affect the diffusion process, the Bass [7] model does not contemplate these variables and yet it is still able to describe the empirical adoption curve of a large number of new products and technological innovations. In order to explain the robustness of the model, Bass et al. [9] developed a general model including these variables, and they showed that this general model reduces to the Bass model as a special case. They also showed that the shape of the diffusion of innovation process is always the same, an S-curve. Norton and Bass [57] analyzed the diffusion of innovation for product substitution, explaining some unexpected changes in innovation adoption which were still unclear.

The motivation behind the present work is that there may be people who reject a particular innovation. Such people do not recommend the innovation, on the contrary, they may publicly complain about it and bad-mouth it. This negative word-of-mouth effect of rejection has always existed [65, 12, 69, 17] but it is becoming more and more important as information can spread more easily and faster among people through the usage of new technologies [39, 36, 4]. Nowadays, before making a decision, people may search the internet for reviews and feedbacks about the innovation, and what they find affects their decision

[22, 26, 31, 27, 43, 61]. A number of firms have already perceived this change caused in large part by the social media and have adapted to this new condition, like Starbucks [34], for example.

There is an extensive literature on innovation diffusion. Numerous extensions to the Bass [7] model have been proposed (for reviews, see Meade and Islam [48] and Peres et al. [60]), among which Mahajan and colleagues were the first to propose a model that includes the negative word-of-mouth [47]. The latter and other extensions that include negative word-of-mouth are much more complex than the Bass [7] model, and their parameters must be estimated using the number of people who have already adopted the innovation at a given time. A problem is that most recent innovations, like Facebook, Twitter, and Netflix do not disclose their total number of users. Actually, they deem this number confidential. They only disclose the number of active users, not including the number of users who have rejected them.

In this work, I propose an extension to the Bass model which (i) includes the negative effect of the rejections, (ii) is as simple as the Bass [7] model, and (iii) its parameters can be estimated using the number of people who have adopted and have not posteriorly rejected the innovation, i.e., the number of *active adopters*. An important difference between the number of *active adopters* and the *total adopters* is that first may decrease over time, while the latter cannot. First, I discuss the Bass [7] model and its parameters; then I describe the model extension and analyze four models of rejection; next I detail the estimation method; after that I estimate the models by using Facebook's active users dataset; and finally, I discuss the results and conclude.

The main contribution of this work is that the proposed extension is the first to include the effect of the rejections that can be estimated using the number of *active adopters* instead of the number of *total adopters*. The model can be applied to forecast the number of active adopters of these companies in the next quarters, which becomes an important tool for analysts, investors, and the companies themselves. As the number of active adopters is related to the market cap of these companies, these forecasts may be useful to estimate the future value of the firms. At the time of this writing, Facebook's market cap is \$222.69B, Twitter's is \$23.18B, and Netflix's is \$20.49B[1].

1 Data obtained from Yahoo! Finance website at December 1st, 2016.

22

THE BASS MODEL

The Bass [7] model is a simplification of the diffusion of innovation process proposed by Rogers [66]. The Rogers' classification of adopters has five classes: (i) innovators; (ii) early adopters; (iii) early majority; (iv) late majority; and (v) laggards. Bass simplified them to only two classes: innovators and imitators. The innovators are the ones who start using an innovation regardless of who else and how many other people are already using it. The imitators are the ones who concern themselves about who is using the innovation and, as long as many other people are using it, they are more inclined to adopt it. Thus, at the beginning of the diffusion of innovation, the majority of adopters are innovators. As more and more people adopt the innovation, the majority of new adopters shift to imitators.

Mathematically, the model presents itself with the following set of equations:

$$S(t) = mf(t) \tag{2}$$

$$Y(t) = mF(t) \tag{3}$$

$$\frac{f(t)}{1 - F(t)} = p + qF(t), F(0) = 0 \tag{4}$$

Both $S(t)$ and $Y(t)$ are related to the absolute amount of adopters; while $S(t)$ is the number of new adopters at time t, $Y(t)$ is the number of people who had already adopted the innovation by time t, thus $S(t) = \frac{d}{dt}Y(t)$. The model also has three positive parameters: (i) the potential market size m; (ii) the innovators parameter p; and (iii) the imitators parameter q. There are also $f(t)$ and $F(t)$ which are related to the percentage of the potential market: $f(t)$ is the percentage of the potential market which is adopting the innovation at time t, while $F(t)$ is the percentage of the potential market which had already adopted it at time t, thus $f(t) = \frac{d}{dt}F(t)$.

Therefore, $S(t)$ and $f(t)$ are related to the adoption rate at time t, while $Y(t)$ and $F(t)$ are related to the accumulated adopters at time t. In the beginning of the diffusion of innovation, there are no adopters at all, thus $Y(0) = F(0) = 0$. As the number of adopters can only increase over time, both $Y(t)$ and $F(t)$ are monotonically increasing functions, and both $S(t)$ and $f(t)$ are always greater or equal to zero.

The non-linear ordinary differential equation 4 is the main equation in the Bass model. Its left side is known as the hazard function and it expresses the probability of someone adopting the innovation, provided that he/she has not chosen to adopt it yet, i.e.,

the rate of adoption. Its right side means that this probability is at least p and increases linearly with the percentage of people who have already adopted the innovation, i.e., $F(t)$.

Solving the differential equation, Bass found a closed formula for the diffusion, which is $F(t) = \frac{1-e^{-(p+q)t}}{1+\frac{q}{p}e^{-(p+q)t}}$. This closed formula always has the famous shape of the S-curve, regardless of the values of $p > 0$ and $q > 0$. From the closed formula of $F(t)$, it is trivial to obtain the equations of $S(t)$, $Y(t)$, and $f(t)$.

The potential market size m is the unknown number of people who will have adopted the innovation after a very long time. It is not exactly the target market of the innovation, but a subset of it, as no product difuses over its entire target market. If a company estimates and updates the model more than once for their product, the change in m is a change in the potential market and could help the company to understand whether their decisions in the meantime have increased or decreased the number of future adopters. As, $\lim_{t\to\infty} Y(t) = m$, the whole potential market will have adopted the innovation at some point.

The innovator parameter p is related to the proportion of people in the potential market who adopt the innovation regardless the others. In other words, their decision to adopt is not influenced by the social system, but by other external factors. The bigger the p, the larger the number of innovators, thus the faster the diffusion at the beginning.

The imitator parameter q is related to the influence of those actually using the innovation on those who are not using it yet. This is why this parameter multiplies $F(t)$, which is the proportion of the market which had already adopted it. This influence is mainly understood as a result of the word-of-mouth recommendation. In other words, the more people use the innovation, the more other people will adopt it. The bigger the q, the larger the imitator effect, thus, the faster the diffusion.

Practitioners have been using this model to forecast future demand. First, they measure the number of adopters over time. Then, they estimate the parameters m, p, and q. Finally, they extrapolate $S(t)$ out of the measured time window and use its value as the forecast demand. They also calculate $m - Y(t)$ as a forecast of how many people have not adopted the innovation yet.

23

THE EXTENDED MODEL

I propose adding a new term in the differential equation 4 in order to include the effect of rejection, as in equation 5. Hereafter I will refer to: (i) the people who have adopted the innovation as *total users*; (ii) the people who have adopted the innovation and remain using it as *active users*; and (iii) the people who rejected the innovation as *inactive users*. Clearly, the function $Y(t)$ is the number of *total users*, which is equal to the sum of the number of *active users* with the number of *inactive users*.

$$\frac{f(t)}{1-F(t)} = p + qF(t) - wR(t), F(0) = 0, R(0) = 0 \tag{5}$$

The function $R(t)$ is the percentage of accumulated *inactive users* at time t. Thus, $A(t) = F(t) - R(t)$ is the percentage of accumulated *active users* at time t. Multiplying by m, $mA(t) = Y(t) - mR(t)$ is the number of *active users* at time t. Since $A(t) \geqslant 0$, $F(t) \geqslant R(t)$, which makes sense because it is not possible to have more *inactive users* than *total users*.

The negative word-of-mouth parameter w is related to how much the *inactive users* really affect the new adopters decision in the diffusion process. The bigger the w, the greater the negative influence of these *inactive users* on the new adopters. Another possible understanding is that w is related to how much the *inactive users* are bad-mouthing the innovation. The bigger the w, the more they bad-mouth the innovation.

Equation 5 could be rewritten as $\frac{f(t)}{1-F(t)} = p + qA(t) + (q-w)R(t)$. This form is useful in order to understand the impact of *active users* and *inactive users* on the rate of adoption at time t.

If $w = q$, then the rate of adoption increases linearly with the *active users*, since $\frac{f(t)}{1-F(t)} = p + qA(t)$. In other words, the positive word-of-mouth has exactly the same influence as the negative word-of-mouth on the new adopters. It also means that the rate of adoption is always greater than zero, thus the whole potential market will have adopted the innovation sooner or later.

If $w < q$, then the new adopters are more influenced by the number of *total users* than by the number of *inactive users*. It is just as if the *inactive users* do not bad-mouth the innovation so much, or at all. Again, the rate of adoption is always greater than zero, thus the whole potential market will have adopted the innovation sooner or later.

If $w > q$, then the proposed extension really differs from the Bass model. In this case, the influence of the *inactive users* is greater than

the influence of *total users*. So, if the rate of adoption were equal to zero ($wR(t) = p + qF(t)$), the innovation might not be adopted by the whole potential market, i.e., $\lim_{t\to\infty} F(t) < 1$.

The main contribution of this work is to have the choice to use the number of *active users*, which is the information that most of the companies disclose, in order to estimate the parameters of the proposed extension model. With that, both the number of *inactive users* and *total users* could be forecast. It is important to notice that the number of *active users* ($mA(t)$) could decrease over time. In fact, forecasting when this is going to happen may be crucial for corporations.

24

MODELS FOR R(t)

The proposed extended model already includes the effect of rejection through the $R(t)$ function and the w parameter. In order to complete the model, $R(t)$ has to be well defined. Let $r(t) = \frac{d}{dt}R(t)$ be the rate of new *inactive users* at time t. The proposed differential equations for $R(t)$ are the following:

$$\text{Model 1: } r(t) = \nu f(t) \tag{6}$$

$$\text{Model 2: } \frac{r(t)}{1 - R(t)} = \nu f(t) \tag{7}$$

$$\text{Model 3: } r(t) = \nu[F(t) - R(t)] \tag{8}$$

$$\text{Model 4: } \frac{r(t)}{1 - R(t)} = \nu[F(t) - R(t)] \tag{9}$$

These four models can be grouped in two families, one for the equations 6 and 7, and another for the equations 8 and 9. The former relates the rejection to the rate of new people adopting the innovation, as if people decide whether they will use or reject the innovation when they try it. Then, they do not change their position anymore. The latter assumption relates the rejection to the number of *active users*, as if the *active users* first adopt the innovation and then they continuously reject it.

The rejection parameter ν has a different interpretation in each family. In equations 6 and 7, it is the proportion of new adopters who will reject the innovation. In equations 8 and 9, it is the proportion of active users who are continuously rejecting the innovation.

Therefore, for all these models of rejection, the complete diffusion of innovation model has five parameters to be estimated, namely m, p, q, w, and ν.

24.1 MODEL 1

In this model, the rate of new *inactive users* at time t is proportional to the percentage of people adopting the innovation at time t, as if people decide whether they will use or reject the innovation when they are adopting it.

The differential equation 6 can be easily solved integrating both sides. Thus, $R(t) = \nu F(t)$, $A(t) = (1 - \nu)F(t)$, and $f(t)/[1 - F(t)] = p + (q - w\nu)F(t)$. As the imitator coefficient must be positive, we must have $w\nu < q$.

The solution shows that this model has exactly the same explanatory power as the Bass model, neither better nor worse. This happens because the model's solution has exactly the same equation after the linear transformation $q^* = q - w\nu$.

As $\lim_{t\to\infty} F(t) = 1$, thus $\lim_{t\to\infty} R(t) = \nu$. Hence, the proportion of *inactive users* is exactly equal to the rejection parameter.

Solving the differential equation for $F(t)$, it gets $F(t) = (1 - e^{-(p+q-w\nu)t})/(1 + \frac{(q-w\nu)}{p}e^{-(p+q-w\nu)t})$. Finally, as $R(t) = \nu F(t)$, thus $R(t) = \nu(1 - e^{-(p+q-w\nu)t})/(1 + \frac{(q-w\nu)}{p}e^{-(p+q-w\nu)t})$.

Unfortunately, it is not possible to estimate this model. The problem is that $\forall\nu \in \mathbb{R}^+$, $\exists\hat{\nu} \in \mathbb{R}^+$ such as the set of parameters (m, p, q, w, ν) and $(m, p, q, w\nu/\hat{\nu}, \hat{\nu})$ have exactly the same residuals when estimated. That is, the model can be estimated for any value arbitrarily set for ν. Intuitively, as both $F(t)$, $A(t)$, and $R(t)$ have the same shape, the parameters can be estimated with an empirical *active users* dataset and then you can slide up or down $F(t)$ just changing the values of ν and w.

This result is interesting because it shows that the Bass model can already explain the diffusion of innovations which follows this model of rejection. Hence, it just confirms the robustness of the Bass model.

24.2 MODEL 2

The right side of the differential equation 7 is the rate of rejection, i.e., the probability of someone who rejecting the innovation, provided that he/she has not rejected it yet. Thus, in this model, the rate of rejection is proportional to the percentage of people adopting the innovation at time t, i.e., the more people adopt the innovation, the more they reject it. But if no one is adopting, there would be no rejection also, which would hold the number of *active users* the same.

The differential equation 7 can also be solved for $R(t)$ algebrically. Using the fact that $-\frac{d}{dt}\log[1 - R(t)] = r(t)/[1 - R(t)] = \nu f(t)$, and integrating both sides of this equation yields:

$$-\frac{d}{dt}\int_0^t \log[1 - R(\tau)]d\tau = \nu\int_0^t f(\tau)d\tau \tag{10}$$

$$-\log[1 - R(t)] = \nu F(t) \tag{11}$$

$$1 - R(t) = e^{-\nu F(t)} \tag{12}$$

$$R(t) = 1 - e^{-\nu F(t)} \tag{13}$$

Finally, $f(t)/[1 - F(t)] = p + qF(t) - w[1 - e^{-\nu F(t)}]$ and $\lim_{t\to\infty} R(t) = 1 - e^{-\nu}$.

As $0 \leqslant F(t) \leqslant 1 \Rightarrow 0 \leqslant \nu F(t) \leqslant \nu$, we can do a good approximation of $e^{-\nu F(t)}$ using a Taylor series around the point $\nu/2$ for small values of ν.

From the Taylor series centered around $\nu/2$, we know that $e^{-x} \approx e^{-\nu/2}(1+\nu/2-x)$. Thus, we have $1-e^{-\nu F(t)} \approx 1-e^{-\nu/2}(1+\nu/2)+e^{-\nu/2}\nu F(t)$, and, finally, $f(t)/[1-F(t)] = [p-w-we^{-\nu/2}(1+\nu/2)]+(q-we^{-\nu/2}\nu)F(t)$.

Therefore, for small values of ν, this model has approximately the same explanation power as the Bass model and we can write $f(t) = p^* + q^*F(t)$, where $p^* = p-w-we^{-\nu/2}(1+\nu/2)$ and $q^* = q-we^{-\nu/2}\nu$.

In contrast to model 1, no parameter could be arbitrarily set in this model, thus it can be estimated using an empirical *active users* dataset.

24.3 MODEL 3

In this model, the rate of new *inactive users* increases linearly with the number of *active users*, since $A(t) = F(t) - R(t)$. Thus, while there are *active users*, a fraction ν of them will be rejecting the innovation. Hence, everyone will have reject the innovation sooner or later.

The differential equation 8 can be rewritten as the following first order linear differential equation, which has to be solved:

$$\frac{d}{dt}R(t) + \nu R(t) = \nu F(t) \tag{14}$$

The solution to this differential equation is:

$$R(t) = \nu e^{-\nu t}\int_0^t e^{\nu\tau}F(\tau)d\tau \tag{15}$$

$$= \nu\left[F(u) * e^{-\nu u}\right](t) \tag{16}$$

Or, as $\frac{d}{dt}\left(e^{\nu t}F(t)\right) = \nu e^{\nu t}F(t) + e^{\nu t}f(t)$, $R(t)$ can be rewritten as:

$$R(t) = F(t) - e^{-\nu t}\int_0^t e^{\nu\tau}f(\tau)d\tau \tag{17}$$

$$= F(t) - \left[f(u) * e^{-\nu u}\right](t) \tag{18}$$

As $F(t) = \int_0^t f(\tau)d\tau$ and $e^{\nu\tau} \geqslant 1$, we have that:

$$\int_0^t e^{\nu\tau}f(\tau)d\tau \geqslant F(t) \tag{19}$$

$$-e^{-\nu t}\int_0^t e^{\nu\tau}f(\tau)d\tau \leqslant -e^{-\nu t}F(t) \tag{20}$$

$$F(t) - e^{-\nu t}\int_0^t e^{\nu\tau}f(\tau)d\tau \leqslant F(t) - e^{-\nu t}F(t) \tag{21}$$

From equation 17:

$$R(t) \leqslant F(t) - e^{-\nu t}F(t) \tag{22}$$
$$R(t) \leqslant F(t)(1 - e^{-\nu t}) \tag{23}$$

Finally, $R(t) < F(t)$, $r(t) > 0$, and $\lim_{t\to\infty} R(t) \leqslant 1$.

I did not manage to prove that $\lim_{t\to\infty} R(t) = 1$, but this result appeared in all performed simulations. If that is true, then all people will reject the innovation at some point in time - a fact that makes sense.

Unfortunately, it seems that there is no closed formula for $F(t)$. Using equation 15, the final differential equation is:

$$\frac{f(t)}{1 - F(t)} = p + qF(t) - w\nu e^{-\nu t}\int_0^t e^{\nu\tau}F(\tau)d\tau \tag{24}$$

Or, using 17, it becomes:

$$\frac{f(t)}{1 - F(t)} = p + (q - w)F(t) + we^{-\nu t}\int_0^t e^{\nu\tau}f(\tau)d\tau \tag{25}$$

The condition $w \leqslant p + q$ is sufficient to ensure $f(t) \geqslant 0$, since $w \leqslant p + q \Rightarrow wR(t) \leqslant pR(t) + qR(t) \leqslant p + qR(t) \leqslant p + qF(t) \Rightarrow p + qF(t) - wR(t) = f(t)/[1 - F(t)] \geqslant 0 \Rightarrow f(t) \geqslant 0$. Assuming that $\lim_{t\to\infty} R(t) = 1$, then it is easy to prove that this condition is also necessary.

24.4 MODEL 4

In this model, the rate of rejection increases linearly with the number of *active users*. Thus, while there are *active users*, the rate of rejection will be greater than zero. Hence, everyone will have reject the innovation sooner or later.

Although equation 9 is a Ricatti equation [10], none of the available techniques could solve the differential equation and it seems that there is no closed formula for $F(t)$. Hence, the equation will be analyzed through a linearization around the fixed points.

$$\begin{cases} f(F, R) = (p + qF - wR)(1 - F) \\ r(F, R) = \nu(F - R)(1 - R) \end{cases} \tag{26}$$

Solving the system $f(F, R) = r(F, R) = 0$, the following solutions are found:

$$u_1^* = (1, 1) \tag{27}$$

$$u_2^* = \left(\frac{p}{w-q}, \frac{p}{w-q}\right) \tag{28}$$

$$u_3^* = \left(\frac{w-p}{q}, 1\right) \tag{29}$$

The only valid solutions are u_1^* and u_2^*. The solution u_3^* is not valid because $p + q - w > 0 \Rightarrow (w-p)/q < 1 \Rightarrow F < R$ which is not possible because it would imply a negative number of *active users*.

Finally, the linearization around u^* is:

$$\begin{bmatrix} f(R,T) - f(u^*) \\ r(R,T) - r(u^*) \end{bmatrix} = J|_{u^*} \left(\begin{bmatrix} R \\ T \end{bmatrix} - u^* \right) \tag{30}$$

$$J = \begin{bmatrix} q(1-F) - (p + qF - wR) & -w(1-F) \\ \nu(1-R) & -\nu[(1-R) + (F-R)] \end{bmatrix} \tag{31}$$

Now, let's analyze the jacobian matrices and their eigenvalue for each valid solution.

$$J|_{u_1^*} = \begin{bmatrix} -(p+q-w) & 0 \\ 0 & 0 \end{bmatrix} \tag{32}$$

As the eigenvalues of $J|_{u_1^*}$ are 0 and $-(p+q-w) < 0$, the point $u_1^* = (1,1)$ is a sink, i.e., the neighborhood converges to u_1^* when $t \to \infty$. It may be interpreted that all users will have rejected the innovation after a long time.

25

ESTIMATION METHOD

The parameters of the model should be estimated using empirical data in order to check the explanation power of the model. Bass [7] used a discrete version of his differential equation with ordinary least squares. While it worked well for him, it has not in the present work. There are several well known problems in the estimation of parameters, most of them related to approximation of derivatives and instability of the estimators. These problems have been noticed by many authors [67, 72, 76].

In the present work, the parameters of the models were estimated using a maximum likelihood function on the residuals between $A(t) = F(t) - R(t)$ from the model and the empirical values from the dataset. The residuals were assumed to be normally distributed with $\mu = 0$, which leads to the same results as the ordinary least square method. In order to calculate the residuals, $F(t)$ and $R(t)$ were calculated based on their differential equations using the 4th order Runge Kutta (RK4) numerical method [16] with $\Delta t = 0.01$.

The empirical data format was (t_i, x_i), where t_i is the time and x_i is the value, and the measurements were not equally spaced over time. The following Log Likelihood equation was used:

$$\text{residual}(t_i, x_i \mid m, p, q, w, \nu) = x_i - m \cdot [F(t_i \mid p, q, w) - R(t_i \mid \nu)] \tag{33}$$

$$\text{Log Likelihood}(\vec{t}, \vec{x} \mid m, p, q, w, \nu) = -\sum_{i=1}^{N} [\text{residual}(t_i, x_i \mid m, p, q, w, \nu)]^2 \tag{34}$$

During the evaluation of $F(t)$ and $R(t)$ using the Runge Kutta numerical method, sometimes the exact value of t_i was not reached because of the chosen Δt. In these cases, the value of x_i was calculated using a linear approximation with the nearest points. Let $(\hat{t}_k, \hat{x}_k)$ and $(\hat{t}_{k+1}, \hat{x}_{k+1})$ be values calculated from the Runge Kutta method, such that $\hat{t}_k < t_i < \hat{t}_{k+1}$. Then, the calculated value at t_i was $\hat{x}_k + \left(\frac{\hat{x}_{k+1} - \hat{x}_k}{\hat{t}_{k+1} - \hat{t}_k}\right) \cdot (t_i - \hat{t}_k)$.

Since there is no explicit solution for the parameters m, p, q, w, and ν which maximize the LogLikelihood function, the parameters were estimated using the Truncated Newton Constrained (TNC) method [28, 53, 52] from the SciPy Python Library [40]. The constrains were $m > 0$, $p > 0$, $q > 0$, $w \geqslant 0$, and $\nu \geqslant 0$ for all models. The initial guess for the TNC method was the same for all models estimation.

Sometimes, the method did not converge and another initial guess had to be used.

Even though it has not been done yet, the confidence interval, estimator average and estimator variance for each parameter will be calculated using the bootstrap method.

26

PRELIMINARY RESULTS

The models parameters were estimated using the number of Facebook's *active users* from December 2004 to March 2013 [73]. In the dataset, x_i was the number of Facebook's *active users* at time t_i. The dataset had 23 non-equally time spaced measures. The users who have accessed Facebook at least once in each month were counted in the number of *active users* in that month.

The model 1 has not been estimated because it is not possible to estimate it.

The estimated models can be seen at figures 34, 35, and 36. These figures also have forecasts for the number of *active users*, *inactive users*, and *total users* of Facebook for the next 4 years (from $t = 100$ to $t = 140$).

In spite of the favorable goodness of fit using model 2 (see figure 34), the model does not seem to provide a plausible forecast, because it would mean that Facebook is reaching a stable number of *active users* and the rejections are near the end.

Models 3 and 4 have very similar outcomes (see figures 35 and 36). Their Bayesian Information Criterion (BIC) are also close, but model 4 has a better fit with the data. Their forecast makes more sense than the forecast of model 2. It predicts that Facebook is very close to the peak of *active users* and, in approximately 3 years, it is going to decline. It is also interesting to notice that, according to these outcomes, Facebook may not reach its total potential market.

The difference between the outcomes of model 2 and models 3 and 4 could be explained by the fact that they have different rationales behind their models of rejection. While differential equation of the model 2 uses the rate of new *total users*, the differential equations of the models 2 and 3 use the proportion of *active users*.

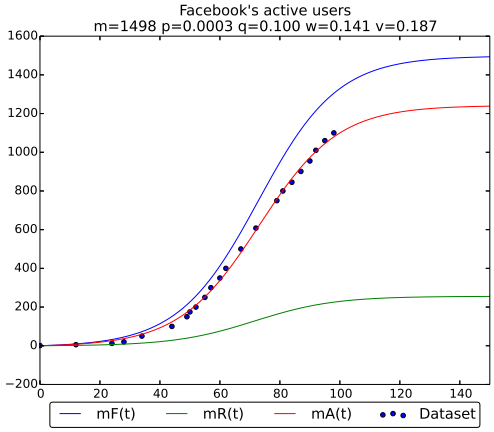


Figure 34: Fit of Model 2 with Facebook's active users dataset. $mF(t)$ is the total users, $mR(t)$ is the inactive users, and $mA(t)$ is the active users. The unit of these functions are thousands of people. The parameters are $m = 1,497.50$, $p = 0.000331$, $q = 0.100088$, $w = 0.140595$, and $\nu = 0.187188$. The goodness of fit are $R^2 = 99.84\%$ and BIC=10,566.52.

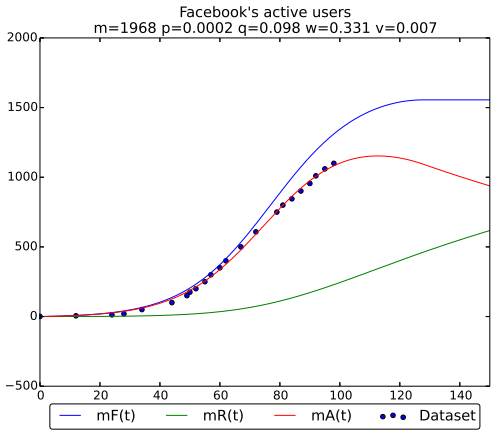


Figure 35: Fit of Model 3 with Facebook's active users dataset. $mF(t)$ is the total users, $mR(t)$ is the inactive users, and $mA(t)$ is the active users. The unit of these functions are thousands of people. The parameters are $m = 1,967.64$, $p = 0.000184$, $q = 0.097867$, $w = 0.330511$, and $\nu = 0.006912$. The goodness of fit are $R^2 = 99.83\%$ and BIC=11,485.68

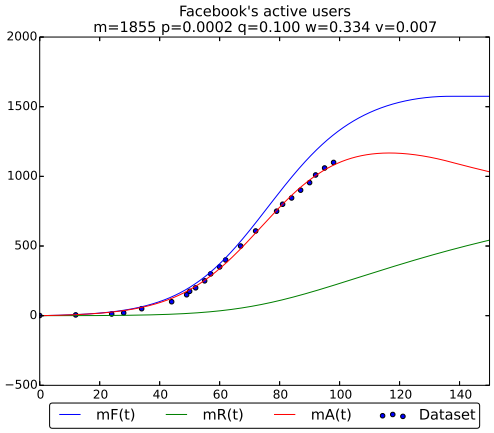


Figure 36: Fit of Model 4 with Facebook's active users dataset. $mF(t)$ is the total users, $mR(t)$ is the inactive users, and $mA(t)$ is the active users. The unit of these functions are thousands of people. The parameters are $m = 1,854.85$, $p = 0.000183$, $q = 0.099738$, $w = 0.334454$, and $v = 0.007007$. The goodness of fit are $R^2 = 99.84\%$ and BIC=10,724.55

27

CONCLUSION

The main contribution of this work is the parameter estimation through the empirical number of *active users* dataset, forecasting the number of *total users*, the number of *active users*, and the number of *inactive users*.

If the adopters who have rejected the innovation follow the equations of model 1 and 2, then the proposed extended model is transformed into the Bass model through a linear transformation of the parameters. This confirms the Bass model robustness.

Model 2 does not seem to be a good model of rejection, since the number of *active users* never decreases which does not seem to be plausible.

Models 3 and 4 had very similar results when fitting the Facebook dataset. The lack of analytical solutions for them, however, is a barrier to better understand their behavior, and to know whether they will always have similar outcomes or they will diverge depending on the data. Model 3 seems to be more analytically manageable.

It is important to notice that, in models 3 and 4, the innovation may not be adopted by the whole potential market, but it would in the Bass model. Whether it will be adopted by the whole potential market or not depends on the parameters w and ν. For instance, it seems that $mF(t)$ is not converging to m at figures 35 and 36. It is a major difference between the proposed extended model and the Bass model.

As this is a working paper, it is also intended to include the analyses of other datasets, like either Twitter's number of *active users*, or WhatsApp's, or Netflix's, or Reddit's, or Dropbox's, or Waze's. This would enhance the proposed model power of forecasting.

It is also intended to run a back test with the available data. First, the parameters of the model is estimated using a subset of the dataset. Then, through extrapolation, the number of *active uses* is forecast. Finally, it is compared to this part of the dataset - which must not have been used in the estimation.

The main limitation of this work is that it has no theory to support which of the models of rejection best fit with empirical data. Although there is an extensive literature on negative word-of-mouth, this literature does not predict which model would be the best. But, if any of these companies discloses the number of *total users* and *active users*, the estimation method could be adapted to estimate the parameters using both pieces of information at the same time, which

would make possible to verify which of the models of rejection is the best.

Future work could explore other models of rejection and also other estimation methods, like nonlinear least squares [72] and Kalman filter [76].

Part V

CONCLUSION

28

CONCLUSION

Software is eating the World.

— Mark Andreesen [2]

Modern management and high technology interact in multiple, profound, ways. Software, in particular, seems to have an immense power of entering arenas which seemed, at some point, to require either specific hardware or the skill of humans. One of the members of this thesis committee, Dr. Nichols, will participate through teleconferencing over the open web, with no use of hardware specific for the task. The corporate biography of Tonny Martins, President of IBM Brasil, mentions his successes with blockchain, AI and cognitive technology... as an executive, not as a research scientist or specialized engineer (https://www-03.ibm.com/press/br/pt/biography/53561.wss). Professor Andrew Ng tells students at Stanford's Graduate School of Business that "AI is the new electricity" Ng [54], as his way to emphasize the potential transformational power of the technology. It is not impossible that a purely digital form of money may exist. It is not impossible that machines may become intelligent. Moreover, it is not impossible that these two processes may have already begun.

It is worthwhile, in this concluding section, to reflect on some ideas on what this thesis is and what it is that we, as computational management scientists, can obtain from this sort of study. Clemenceau once said that "war is too important to be left to the generals". I believe it is not far-fetched to state that technology has become too important to be isolated to the realm of computer science, or engineering, or applied mathematics, or any single discipline. The emergence of scientific journals with names such as Computational Management Science; INFORMS Journal on Computing; Ledger; Computational Statistics; ACM Transactions on Economics and Computation, and so forth, show that there are growing communities deeply interested in the intersection of business and the computer sciences. To whom, for instance, does the OpenAI project belong? To computing or to business? Recall that the project was created as a risk-management strategy against the far-fetched, but not impossible, possibility of having machines yielding too much power. What about corporations like Uber? AirBnB? Imagine a new method that increases profits by 50% at a

tech company. Should this method, if implementable as an algorithm (like PageRank Brin and Page [13]) or a data structure (like a blockchain) be discussed in conferences of 'computer science' or 'business'? It seems quite arbitrary to name a single group, as a whole new ecosystem seems to be emerging within those two. That is why this thesis is computational and why it is business. This work explores topics that seem, on the surface, to belong to computer science, but their applicability and impact to businesses seem too large to be delegated away, something "for the nerds in the fifth floor". As technical decisions become central to the organization of man's life, the technician becomes the visionary, the innovator, the decision-making arbiter, sometimes the billionaire.

We have started this study with two possible forms of organization of a purely digital money system; a blockchain and a directed acyclic graph; we then moved to an analysis of the adoption of new technologies.

The possibility that there will be some form of purely digital money has become very real. Consider, just as a matter of comparison, Brazil's most important company: Petrobrás. As of this writing, the "market cap" of Ethereum exceeds that of Petrobras by ten billion dollars, while Bitcoin's is valued at more than double of Petrobras (195B usd vs 83B usd). These technologies should, at a minimum, be taken seriously.

We have explored Kanerva's Sparse Distributed Memory. In AI, SDM seems to be a particularly interesting area for study. The model plausibly reflects a number of well known aspects of psychology and neuroscience. For example, neurons can easily compute the address decoding scheme of the system. Neurons are fragile and may be lost, whereas the information remains preserved, due to the distributed character of the model. The "tip-of-the-tongue" behavior emerges naturally, and so does Miller's magic number.

There are three contributions made on SDM: First, I have illuminated a discrepancy between Kanerva's theoretical model and the real system dynamics; Also, we have seen that pattern classification through supervised learning is possible without presuming any new SDM mechanism. This is in contrast with the literature, that presumes additional mechanisms, like genetic algorithms, to account for supervised learning. Finally, we now have a tested open-source framework that offers parallelism and can become a de-facto standard in SDM research. The framework (i) carefully reproduces crucial figures from Kanerva's theoretical book; (ii) shows how noise filtering and (iii) supervised learning can be done, and, through the use of (iv) Jupyter Notebooks, enables the reader to easily reproduce all the results on their own machines. This respects all constraints posed by Robert M. French in his article

on 'Computational Modeling in Cognitive Science: A Manifesto for Change' [1].

The ability to rapidly reproduce results, and to build on prior work, is, I believe, fundamental to modern science. Consider, for instance, the groundbreaking successes in the arena of deep learning. Having standard computer libraries to work with has brought together a community, which reinforces the system, as users also gradually improve these libraries. It may be possible to achieve new results with multiple layers of a SDM, yet, having to start development from scratch takes a large opportunity cost from most scientists — especially those who are less concentrated on the computer science aspects, but still would be able to contribute meaningfully.

Finally, we have studied how variations of the Bass Model may reflect systems or technologies that may wither in time. Though some innovations, such as the radio, have gained widespread use in a sustainable form... One may want to review the Bass model when one is concerned with rapidly-evolving technological ecosystems. Hardly anyone remembers the names AskJeeves, World Wide Web Worm, Lycos, WebCrawler, or AltaVista, early web search engines; later replaced, in the market and by the market, by the almost unnoticed url `http://google.stanford.edu` [13].

Another possibility would be to compare the proposed model with a computation of the momentum of Metcalfe's law in between competitors. As the reader may remember, Metcalfe's law states that the value of a network grows $O(n^2)$ with n being the number of network nodes. If the proposed model and Metcalfe's network effects reflect reality, then there could be an integrated mathematical model that explains and represents both Metcalfe's law and the variation of the Bass model presented herein.

With this, I submit this thesis in the hope that all readers, present and future, may find the aforementioned studies as useful, genuine, and legitimate contributions to the thriving field of Computational Management Science.

Part VI

APPENDIX

A

APPENDIX TEST

Lorem ipsum at nusquam appellantur his, ut eos erant homero concludaturque. Albucius appellantur deterruisset id eam, vivendum partiendo dissentiet ei ius. Vis melius facilisis ea, sea id convenire referrentur, takimata adolescens ex duo. Ei harum argumentum per. Eam vidit exerci appetere ad, ut vel zzril intellegam interpretaris.

Errem omnium ea per, pro congue populo ornatus cu, ex qui dicant nemore melius. No pri diam iriure euismod. Graecis eleifend appellantur quo id. Id corpora inimicus nam, facer nonummy ne pro, kasd repudiandae ei mei. Mea menandri mediocrem dissentiet cu, ex nominati imperdiet nec, sea odio duis vocent ei. Tempor everti appareat cu ius, ridens audiam an qui, aliquid admodum conceptam ne qui. Vis ea melius nostrum, mel alienum euripidis eu.

A.1 APPENDIX SECTION TEST

Ei choro aeterno antiopam mea, labitur bonorum pri no. His no decore nemore graecis. In eos meis nominavi, liber soluta vim cu. Sea commune suavitate interpretaris eu, vix eu libris efficiantur.

More dummy text.

Nulla fastidii ea ius, exerci suscipit instructior te nam, in ullum postulant quo. Congue quaestio philosophia his at, sea odio autem vulputate ex. Cu usu mucius iisque voluptua. Sit maiorum propriae at, ea cum primis intellegat. Hinc cotidieque reprehendunt eu nec. Autem timeam deleniti usu id, in nec nibh altera.

A.2 ANOTHER APPENDIX SECTION TEST

Equidem detraxit cu nam, vix eu delenit periculis. Eos ut vero constituto, no vidit propriae complectitur sea. Diceret nonummy in has, no qui eligendi recteque consetetur. Mel eu dictas suscipiantur, et sed placerat oporteat. At ipsum electram mei, ad aeque atomorum mea.

Ei solet nemore consectetuer nam. Ad eam porro impetus, te choro omnes evertitur mel. Molestie conclusionemque vel at, no qui omittam expetenda efficiendi. Eu quo nobis offendit, verterem scriptorem ne vix.

LABITUR BONORUM PRI NO	QUE VISTA	HUMAN
fastidii ea ius	germano	demonstratea
suscipit instructior	titulo	personas
quaestio philosophia	facto	demonstrated

Table 3: Autem usu id.

Listing 1: A floating example

```
for i:=maxint to 0 do
begin
{ do nothing }
end;
```

BIBLIOGRAPHY

[1] Caspar Addyman and Robert M. French. Computational modeling in cognitive science: A manifesto for change. *Topics in Cognitive Science*, 4(3):332–341, 2012. ISSN 1756-8765. doi: 10.1111/j.1756-8765.2012.01206.x. URL http://dx.doi.org/10.1111/j.1756-8765.2012.01206.x.

[2] Mark Andreesen. Why software is eating the world. URL https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

[3] Ashraf Anwar and Stan Franklin. Sparse distributed memory for 'conscious' software agents. *Cognitive Systems Research*, 4(4): 339–354, 2003.

[4] Ana Babic, Francesca Sotgiu, Kristine de Valck, and Tammo HA Bijmolt. The effect of electronic word of mouth on sales: A meta-analytic review of platform, product, and metric factors. *Journal of Marketing Research*, 2015.

[5] Norman TJ Bailey. On queueing processes with bulk service. *Journal of the Royal Statistical Society. Series B (Methodological)*, pages 80–87, 1954.

[6] Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun. Bitter to better—how to make bitcoin a better currency. In *International Conference on Financial Cryptography and Data Security*, pages 399–414. Springer, 2012.

[7] Frank M Bass. A new product growth for model consumer durables. *Marketing science*, 15(5):215–227, 1969.

[8] Frank M Bass. Comments on "a new product growth for model consumer durables the bass model". *Management science*, 50 (12_supplement):1833–1840, 2004.

[9] Frank M Bass, Trichy V Krishnan, and Dipak C Jain. Why the bass model fits without decision variables. *Marketing science*, 13 (3):203–223, 1994.

[10] Sergio Bittanti, Alan J Laub, and Jan C Willems. *The Riccati Equation*. Springer-Verlag New York, Inc., 1991.

[11] Blockchain.info. Bitcoin blockchain size. https://blockchain.info/charts/blocks-size. Last accessed on July 14, 2017.

[12] Paula Fitzgerald Bone. Word-of-mouth effects on short-term and long-term product judgments. *Journal of business research*, 32(3): 213–223, 1995.

[13] Sergey Brin and Lawrence Page. The anatomy of a large-scale hypertextual web search engine. *Computer networks and ISDN systems*, 30(1-7):107–117, 1998. URL http://infolab.stanford.edu/~backrub/google.html.

[14] M. S. Brogliato. Understanding the critical distance in sparse distributed memory. Master's thesis, Escola Brasileira de Administração Pública e de Empresas - EBAPE, Fundação Getulio Vargas, 2011.

[15] Marcelo S Brogliato, Daniel M Chada, and Alexandre Linhares. Sparse distributed memory: understanding the speed and robustness of expert memory. *Frontiers in Human Neuroscience*, 8: 222, 2014.

[16] John Charles Butcher. *The numerical analysis of ordinary differential equations: Runge-Kutta and general linear methods*. Wiley-Interscience, 1987.

[17] Francis A Buttle. Word of mouth: understanding and managing referral marketing. *Journal of strategic marketing*, 6(3):241–254, 1998.

[18] John Cannarella and Joshua A Spechler. Epidemiological modeling of online social network dynamics. *arXiv preprint arXiv:1401.4208*, 2014.

[19] Daniel de Magalhães Chada. *Are you experienced? Contributions towards experience recognition, cognition, and decision making*. PhD thesis, 2016.

[20] Timothy M Chan, Kasper Green Larsen, and Mihai Pătraşcu. Orthogonal range searching on the ram, revisited. In *Proceedings of the twenty-seventh annual symposium on Computational geometry*, pages 1–10. ACM, 2011.

[21] Bernard Chazelle. A functional approach to data structures and its use in multidimensional searching. *SIAM Journal on Computing*, 17(3):427–462, 1988.

[22] Pei-Yu Chen, Shin-yi Wu, and Jungsun Yoon. The impact of online recommendations and consumer feedback on sales. *ICIS 2004 Proceedings*, page 58, 2004.

[23] CoinMarketCap. Bitcoin market capitalizations. http://coinmarketcap.com/currencies/bitcoin/. Last accessed on July 14, 2017.

[24] Thomas H Cormen. *Introduction to algorithms*. MIT press, 2009.

[25] Thomas M Cover and Joy A Thomas. *Elements of information theory*. John Wiley & Sons, 2012.

[26] Chrysanthos Dellarocas. The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Management science*, 49(10):1407–1424, 2003.

[27] Chrysanthos Dellarocas, Xiaoquan Michael Zhang, and Neveen F Awad. Exploring the value of online product reviews in forecasting sales: The case of motion pictures. *Journal of Interactive marketing*, 21(4):23–45, 2007.

[28] Ron S Dembo and Trond Steihaug. Truncated-newtono algorithms for large-scale unconstrained optimization. *Mathematical Programming*, 26(2):190–212, 1983.

[29] Discussion. Dag, a generalized blockchain, 2014. https://nxtforum.org/proof-of-stake-algorithm/dag-a-generalized-blockchain/ (registration at nxtforum.org required).

[30] Hans Dobbertin, Antoon Bosselaers, and Bart Preneel. Ripemd-160: A strengthened version of ripemd. In *Fast Software Encryption*, pages 71–82. Springer, 1996.

[31] Wenjing Duan, Bin Gu, and Andrew B Whinston. Do online reviews matter?—an empirical investigation of panel data. *Decision Support Systems*, 45(4):1007–1016, 2008.

[32] Kuo-Chin Fan and Yuan-Kai Wang. A genetic sparse distributed memory approach to the application of handwritten character recognition. *Pattern Recognition*, 30(12):2015–2022, 1997.

[33] R. M. French. When coffee cups are like old elephants, or why representation modules dont make sense. In A. Riegler and M. Peschl, editors, *Proceedings of the 1997 International Conference on New Trends in Cognitive Science*, pages 158–163. Austrian Society for Cognitive Science, 1997.

[34] John Gallaugher and Sam Ransbotham. Social media and customer dialog management at starbucks. *MIS Quarterly Executive*, 9(4):197–212, 2010.

[35] Henri Gilbert and Helena Handschuh. Security analysis of sha-256 and sisters. In *International workshop on selected areas in cryptography*, pages 175–193. Springer, 2003.

[36] David Godes and Dina Mayzlin. Using online conversations to study word-of-mouth communication. *Marketing science*, 23(4): 545–560, 2004.

[37] Frank Harary, John P Hayes, and Horng-Jyh Wu. A survey of the theory of hypercube graphs. *Computers & Mathematics with Applications*, 15(4):277–289, 1988.

[38] Tim A Hely, David J Willshaw, and Gillian M Hayes. A new approach to kanerva's sparse distributed memory. *IEEE transactions on Neural Networks*, 8(3):791–794, 1997.

[39] Bernard J Jansen, Mimi Zhang, Kate Sobel, and Abdur Chowdury. Twitter power: Tweets as electronic word of mouth. *Journal of the American society for information science and technology*, 60(11): 2169–2188, 2009.

[40] Eric Jones, Travis Oliphant, Pearu Peterson, et al. SciPy: Open source scientific tools for Python, 2001–. URL http://www.scipy.org/. [Online; accessed 2014-12-16].

[41] P. Kanerva. *Sparse Distributed Memory*. MIT Press, 1988.

[42] Thomas Kluyver, Benjamin Ragan-Kelley, Fernando Pérez, Brian E Granger, Matthias Bussonnier, Jonathan Frederic, Kyle Kelley, Jessica B Hamrick, Jason Grout, Sylvain Corlay, et al. Jupyter notebooks-a publishing format for reproducible computational workflows. In *ELPUB*, pages 87–90, 2016.

[43] Mira Lee and Seounmi Youn. Electronic word of mouth (ewom) how ewom platforms influence consumer product judgement. *International Journal of Advertising*, 28(3):473–499, 2009.

[44] Sergio Demian Lerner. Dagcoin: a cryptocurrency without blocks, 2015. Available at https://bitslog.wordpress.com/2015/09/11/dagcoin/.

[45] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. Inclusive block chain protocols, 2015. Available at http://www.cs.huji.ac.il/~avivz/pubs/15/inclusivebtc.pdf.

[46] A. Linhares, D. M. Chada, C. N. Aranha, and . The emergence of miller's magic number on a sparse distributed memory. *Public Library of Science (PLOS) One*, 6(1):e15592, Jan 2011. doi: 10.1371/journal.pone.0015592.

[47] Vijay Mahajan, Eitan Muller, and Roger A Kerin. Introduction strategy for new products with positive and negative word-of-mouth. *Management Science*, 30(12):1389–1404, 1984.

[48] Nigel Meade and Towhidul Islam. Modelling and forecasting the diffusion of innovation–a 25-year review. *International Journal of forecasting*, 22(3):519–545, 2006.

[49] Mateus Mendes, Manuel Crisóstomo, and A Paulo Coimbra. Robot navigation using a sparse distributed memory. In *Robotics and automation, 2008. ICRA 2008. IEEE international conference on*, pages 53–58. IEEE, 2008.

[50] Meng et al. A modified sparse distributed memory model for extracting clean patterns from noisy inputs. *Proceedings of International Joint Conference on Neural Networks*, June 2009.

[51] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. Available at https://bitcoin.org/bitcoin.pdf.

[52] Stephen G Nash. Newton-type minimization via the lanczos method. *SIAM Journal on Numerical Analysis*, 21(4):770–788, 1984.

[53] Stephen G Nash. A survey of truncated-newton methods. *Journal of Computational and Applied Mathematics*, 124(1):45–59, 2000.

[54] Andrew Ng. Artificial intelligence is the new electricity, 2017. URL https://www.youtube.com/watch?v=21EiKfQYZXc.

[55] Kenneth A Norman and Randall C O'reilly. Modeling hippocampal and neocortical contributions to recognition memory: a complementary-learning-systems approach. *Psychological review*, 110(4):611, 2003.

[56] Mohammad Norouzi, Ali Punjani, and David J Fleet. Fast exact search in hamming space with multi-index hashing. *IEEE transactions on pattern analysis and machine intelligence*, 36(6):1107–1119, 2014.

[57] John A Norton and Frank M Bass. A diffusion theory model of adoption and substitution for successive generations of high-technology products. *Management science*, 33(9):1069–1086, 1987.

[58] A Pinar Ozisik, George Bissias, and Brian N Levine. Estimation of miner hash rates and consensus on blockchains. Technical report, Tech. rep., PDF available from arxiv. org and https://www. cs. umass. edu/ brian/status-reports. pdf (June 2017).

[59] Ram Pai, Badari Pulavarty, and Mingming Cao. Linux 2.6 performance improvement through readahead optimization. In *Proceedings of the Linux Symposium*, volume 2, pages 105–116, 2004.

[60] Renana Peres, Eitan Muller, and Vijay Mahajan. Innovation diffusion and new product growth models: A critical review and research directions. *International Journal of Research in Marketing*, 27(2):91–106, 2010.

[61] Jürgen Pfeffer, T Zorbach, and KM Carley. Understanding online firestorms: Negative word-of-mouth dynamics in social media

networks. *Journal of Marketing Communications*, 20(1-2):117–128, 2014.

[62] Serguei Popov and Jinn Labs. The tangle. 2016. Available at https://iota.org/IOTA_Whitepaper.pdf.

[63] Rajesh Rao and Olac Fuentes. Hierarchical learning of navigational behaviors in an autonomous robot using a predictive sparse distributed memory. *Machine Learning*, pages 87–113, 1998.

[64] Rajesh PN Rao and Dana H Ballard. Natural basis functions and topographic memory for face recognition. In *IJCAI*, pages 10–19, 1995.

[65] Marsha L Richins. Negative word-of-mouth by dissatisfied consumers: A pilot study. *The journal of marketing*, pages 68–78, 1983.

[66] Everett M Rogers. *Diffusion of innovations*. The Free Press, New York, 1st edition, 1962.

[67] David C Schmittlein and Vijay Mahajan. Maximum likelihood estimation for an innovation diffusion model of new product acceptance. *Marketing science*, 1(1):57–78, 1982.

[68] Helen Shen. Interactive notebooks: Sharing the code. *Nature News*, 515(7525):151, 2014.

[69] Robert E Smith and Christine A Vogt. The effects of integrating advertising and negative word-of-mouth communications on message processing and response. *Journal of Consumer Psychology*, 4(2):133–151, 1995.

[70] Javier Snaider and Stan Franklin. Extended sparse distributed memory. Paper presented at the Biological Inspired Cognitive Architectures 2011, Washington D.C. USA.

[71] Yonatan Sompolinsky and Aviv Zohar. Accelerating bitcoin's transaction processing. fast money grows on trees, not chains, 2013. Available at https://eprint.iacr.org/2013/881.pdf.

[72] V Srinivasan and Charlotte H Mason. Technical note-nonlinear least squares estimation of new product diffusion models. *Marketing science*, 5(2):169–178, 1986.

[73] The Associated Press. Number of active users at facebook over the years, May 2013. URL http://news.yahoo.com/number-active-users-facebook-over-230449748.html.

[74] David Vorick. Getting rid of blocks, 2015. Available at slides.com/davidvorick/braids.

[75] Henry S Warren. *Hacker's delight*. Pearson Education, 2013.

[76] Jinhong Xie, X Michael Song, Marvin Sirbu, and Qiong Wang. Kalman filter estimation of new product diffusion models. *Journal of Marketing Research*, pages 378–393, 1997.