McCulloch-Pitts Brains and Pseudorandom Functions

Vašek Chvátal
chvatal@cse.concordia.ca
Mark Goldsmith
markgoldsmith@gmail.com
Nan Yang
nan.yang@me.com
Department of Computer Science and Software Engineering, Concordia University, Montreal, QC H3G 1M8, Canada

In a pioneering classic, Warren McCulloch and Walter Pitts proposed a model of the central nervous system. Motivated by EEG recordings of normal brain activity, Chvátal and Goldsmith asked whether these dynamical systems can be engineered to produce trajectories that are irregular, disorderly, and apparently unpredictable. We show that they cannot build weak pseudorandom functions.

Electroencephalogram recordings of normal brain (or of an epileptic brain well before a seizure) are usually irregular and disorderly, with no apparent pattern (Liu, Hahn, Heldt, & Coen, 1992; Lehnertz et al., 2001; Da Silva et al., 2003; Iasemidis, Shiau, Sackellares, Pardalos, & Prasad, 2004; Chaovalitwongse, 2009; Ocak, 2009; Altunay, Telatar, & Erogul, 2010). Chvátal and Goldsmith (2012) asked whether the McCulloch-Pitts model of the brain can be engineered to exhibit similar behavior. The same question, although without its physiological interpretation, was also asked in Elyada and Horn (2005). We begin by briefly describing the McCulloch-Pitts model.

A linear threshold function is a function $f : \mathbf{R}^n \to \{0, 1\}$ such that for some real numbers $w_1, \ldots, w_n$ and θ,

$$f(x_1, \ldots, x_n) = H\left(\sum_{j=1}^{n} w_j x_j - \theta\right),$$

where H is the Heaviside step function defined by $H(d) = 1$ for all nonnegative d and $H(d) = 0$ for all negative d. Warren McCulloch and Walter Pitts (1943) proposed a model of the central nervous system built from linear threshold functions. When this system has n neurons and no peripheral afferents, its McCulloch-Pitts model is a mapping $\Phi : \{0, 1\}^n \to \{0, 1\}^n$ defined by

Neural Computation **28, 1042–1050** (2016) © 2016 Massachusetts Institute of Technology
doi:10.1162/NECO_a_00841

$$\Phi(x) = (f_1(x), \ldots, f_n(x))$$

for some linear threshold functions $f_1, \ldots, f_n$. We will refer to such mappings Φ as *McCulloch-Pitts dynamical systems*.

Chvátal and Goldsmith (2012) asked whether these dynamical systems can produce trajectories that are irregular, disorderly, and apparently unpredictable in the sense of generating random numbers. In making the meaning of their question precise, they took the point of view of the practitioners, who mean by a "random number generator" any deterministic algorithm that, given a short sequence of numbers called a *seed*, returns a longer sequence of numbers; such a random number generator is considered to be good if it passes statistical tests from some commonly agreed on battery. (This point of view is expounded in Knuth, 1998.)

In this note, we take the point of view of the theorists: we are going to prove that McCulloch-Pitts dynamical systems cannot produce trajectories that are irregular, disorderly, and apparently unpredictable in the sense of providing weak pseudorandom functions. These have been introduced in Naor and Reingold (1995) and subsume pseudorandom functions, introduced in Goldreich, Goldwasser, and Micali (1986) under the original name of *poly-random collections*. Roughly speaking, a weak pseudorandom function is a probability distribution on a set F_n of functions from $\{0, 1\}^n$ to $\{0, 1\}^n$ with the following property: if $x^1, \ldots, x^m$ are chosen independently and uniformly at random from $\{0, 1\}^n$, then no polynomial-time randomized algorithm can distinguish with a nonnegligible probability between (1) a sequence $(x^1, f(x^1), \ldots, x^m, f(x^m))$ where f is chosen at random from F_n and (2) a sequence $(x^1, y^1, \ldots, x^m, y^m)$ where $y^1, \ldots, y^m$ are chosen independently and uniformly at random from $\{0, 1\}^n$. (Distinguishing between these two is a trivial matter when f is known, and that is why an unknown f must be drawn from a probability distribution on F_n.) Our result shows that weak pseudorandom functions cannot be built from McCulloch-Pitts dynamical systems:

Theorem 1. *There is a polynomial-time deterministic algorithm that, given a sequence* $(x^1, y^1, \ldots, x^m, y^m)$ *of n-bit vectors, returns either the message* `McCulloch-Pitts` *or the message* `not McCulloch-Pitts` *in such a way that*

- *i. If* $y^1 = \Phi(x^1), \ldots, y^m = \Phi(x^m)$ *for some McCulloch-Pitts dynamical system* Φ*, then the algorithm returns* `McCulloch-Pitts`.
- *ii. If* $x^1, \ldots, x^m$ *are chosen independently and uniformly at random from* $\{0, 1\}^n$*, if* $y^1, \ldots, y^m$ *are chosen independently and uniformly at random from* $\{0, 1\}^n$*, and if* $m \geq (2 + \varepsilon)n$ *for some positive constant* ε*, then the algorithm returns* `not McCulloch-Pitts` *with probability at least* $1 - e^{-\delta n}$*, where* δ *is a positive constant depending only on* ε*.*

A dichotomy of a set X is its partition into two disjoint sets. Unlike Cover (1965), for whom a dichotomy is an unordered pair of sets, we view every dichotomy as an ordered pair of sets. A dichotomy (X^+, X^-) of a subset of $\mathbf{R}^n$ is linearly separable if there are numbers $y_1, \ldots, y_{n+1}$ such that

$$\sum_{j=1}^{n} x_j y_j > y_{n+1} \quad \text{whenever } (x_1, \ldots, x_n) \in X^+,$$

$$\sum_{j=1}^{n} x_j y_j < y_{n+1} \quad \text{whenever } (x_1, \ldots, x_n) \in X^-. \tag{1}$$

When f is a function from $\{0, 1\}^n$ to $\{0, 1\}$ and $x^1, \ldots, x^m$ are points in $\{0, 1\}^n$, the dichotomy $(\{x^i : f(x_i) = 0\}, \{x^i : f(x_i) = 1\})$ is linearly separable if and only if f is a threshold function. Our proof of theorem 1 evolves from the propositions that linearly separable dichotomies are easy to recognize and linearly separable dichotomies are rare:

Lemma 1. *Linearly separable dichotomies of m-point subsets of $\{0, 1\}^n$ can be recognized in time polynomial in m and n.*

Lemma 2. *For every positive ε, there is a positive γ with the following property: if X is a finite subset of $\boldsymbol{R}^n$ such that $|X| \geq (2 + \varepsilon)n$, then a dichotomy chosen uniformly at random from all dichotomies of X is linearly separable with probability at most $e^{-\gamma n}$.*

Following the seminal report (Rosenblatt, 1957), the subject of learning a hyperplane that separates, or at least nearly separates, the two parts of a dichotomy received much attention in the machine learning community. None of it is relevant to the following standard argument, implicit in the linear programming proof of Minkowski's separating hyperplane theorem for convex polytopes (Tucker, 1955).

Proof of Lemma 1. Deciding whether a prescribed dichotomy of an m-point subset of $\{0, 1\}^n$ is linearly separable amounts to solving system (1) of m strict linear inequalities in variables $y_1, \ldots, y_{n+1}$, where each coefficient x_j is 0 or 1; the epoch-making result of Khachiyan (1979) guarantees that this can be done in time polynomial in m and n.

Proof of Lemma 2. Without loss of generality, we may assume that $0 < \varepsilon \leq 1$. Let m denote $|X|$ and let p denote the probability that a dichotomy chosen uniformly at random from all dichotomies of X is linearly separable.

Of the 2^m dichotomies of X, at most $2\sum_{i=0}^{n}\binom{m-1}{i}$ are linearly separable (this is at least implicit in Winder, 1966, and Cover, 1965), and so

$$p \leq 2^{-m+1} \sum_{i=0}^{n} \binom{m-1}{i} \leq 2^{-m+1} \sum_{i=0}^{n} \binom{m}{i}.$$

Since $m \geq (2+\varepsilon)n$ and $0 < \varepsilon \leq 1$, we have $n \leq (0.5 - \varepsilon/6)m$. A special case of the well-known bound on the tail of the binomial distribution (see, e.g., Hoeffding, 1963, theorem 1) guarantees that for every positive α smaller than 0.5, there is a positive β such that

$$\sum_{i \leq (0.5-\alpha)m} \binom{m}{i} \leq 2^m e^{-\beta m}.$$

Setting $\alpha = \varepsilon/6$, we conclude that $p \leq 2e^{-\beta m}$, which proves the lemma.

An alternative proof of lemma 2, proposed by one of the reviewers, relies on the Sauer-Shelah lemma (Sauer, 1972; Shelah, 1972): *If a family of subsets of an m-point set has Vapnik-Chervonenkis dimension d, then it includes at most* $\sum_{i=0}^{d} \binom{m}{i}$ *sets.* Its other ingredient is the following corollary of Radon's theorem (Radon, 1921): *If* $\mathcal{H}$ *is a family of half-spaces in* $\mathbf{R}^n$ *and if* X *is a finite subset of* $\mathbf{R}^n$*, then family* $\{X \cap Y : Y \in \mathcal{H}\}$ *has Vapnik-Chervonenkis dimension at most* $n+1$. Putting the two together, we conclude that X has at most $2\sum_{i=0}^{n+1} \binom{m}{i}$ linearly separable dichotomies. This upper bound, although weaker than our $2\sum_{i=0}^{n} \binom{m-1}{i}$, also yields the lemma's conclusion.

Proof of Theorem 1. The algorithm goes as follows: Let α^i denote the first bit of y^i and define

$$\begin{aligned} X^+ &= \{x^i : 1 \leq i \leq m,\ \alpha^i = 1\},\\ X^- &= \{x^i : 1 \leq i \leq m,\ \alpha^i = 0\}. \end{aligned}$$

If this dichotomy is linearly separable, then return *McCulloch-Pitts*; else return *not McCulloch-Pitts*.

Lemma 1 guarantees that the algorithm can be implemented to run in polynomial time.

To prove assertion i, assume that $y^1 = \Phi(x^1), \ldots, y^m = \Phi(x^m)$ for some McCulloch-Pitts dynamical system $\Phi : \{0,1\}^n \to \{0,1\}^n$ defined by $\Phi(x) = (f_1(x), \ldots, f_n(x))$. Now $\alpha^i = f_1(x^i)$ for all $i = 1, \ldots, m$, which means that f_1 takes value 1 on all points of X^+ and value 0 on all points of X^-; since f_1 is a threshold function, the dichotomy (X^+, X^-) is linearly separable, and so the algorithm returns *McCulloch-Pitts*.

To prove assertion ii, assume that $x^1, \ldots, x^m$ are chosen independently and uniformly at random from $\{0,1\}^n$, that $y^1, \ldots, y^m$ are chosen independently and uniformly at random from $\{0,1\}^n$, and that $m \geq (2+\varepsilon)n$ for some positive constant ε. Since the probability that the algorithm returns *not McCulloch-Pitts* increases as m increases, we may replace the assumption that $m \geq (2+\varepsilon)n$ by the assumption that $m = \lceil (2+\varepsilon)n \rceil$. Write $X = X^+ \cup X^-$. Since $x^1, \ldots, x^m$ are chosen independently and uniformly from $\{0,1\}^n$, they are pairwise distinct with probability $2^n(2^n-1)\cdots(2^n-m+1)/2^{nm}$. Since

$$\frac{2^n(2^n-1)\cdots(2^n-m+1)}{2^{nm}} \geq \left(\frac{2^n-m}{2^n}\right)^m = \left(1-\frac{m}{2^n}\right)^m \geq 1-\frac{m^2}{2^n},$$

this probability is at least $1-5n^2 2^{-n}$. When $|X|=m$, the assumption that $y^1,\ldots,y^m$ are chosen independently and uniformly from $\{0,1\}^n$ implies that the dichotomy (X^+,X^-) of X is chosen uniformly from all dichotomies of X, in which case lemma 2 guarantees that (X^+,X^-) is linearly separable with probability at most $e^{-\gamma n}$ for some positive constant γ depending only on ε. We conclude that the algorithm returns *not McCulloch-Pitts* with probability at least $1-5n^2 2^{-n}-e^{-\gamma n}$, which is at least $1-e^{-\delta n}$ for some positive constant δ depending only on ε.

There is an obvious refinement of the algorithm used in the proof of theorem 1: with y^i_j standing for the jth bit of y^i, test each of the n dichotomies,

$$(\{x^i : 1\leq i\leq m,\ y^i_j=1\}, \{x^i : 1\leq i\leq m,\ y^i_j=0\}) \quad (j=1,\ldots,n),$$

and return *McCulloch-Pitts* if and only if all n of them are linearly separable. In the context of distinguishing McCulloch-Pitts functions from truly random functions, the extra work required in this refinement is pointless. The probability of returning *McCulloch-Pitts* when $y^1,\ldots,y^m$ are chosen independently and uniformly at random from $\{0,1\}^n$ is at most $e^{-\delta n}$ in the original version, and that is good enough. Reducing it further to $e^{-\delta n^2}$ in the refinement is nice but unnecessary. In addition, the assumption $m\geq(2+\varepsilon)n$ cannot be significantly relaxed even in the refinement: it is at least implicit in Winder (1966) and Cover (1965) that a dichotomy chosen uniformly at random from all dichotomies of a set of fewer than $(2-\varepsilon)n$ points in $\mathbf{R}^n$ is linearly separable with probability at least $1-e^{-\delta n}$.

Theorem 1 implies that certain simple devices (namely, McCulloch-Pitts dynamical systems) cannot generate pseudorandomness. In the opposite direction, it has been proved that certain simple devices can generate pseudorandomness: examples can be found in Naor, Pinkas, and Reingold (1999), Krause and Lucks (2001), Nielsen (2002), Naor and Reingold (2004), and Applebaum, Ishai, and Kushilevitz (2010).

The question of whether McCulloch-Pitts networks can produce trajectories that are irregular, disorderly, and apparently unpredictable remains open: all depends on the interpretation of the terms *irregular, disorderly, and apparently unpredictable*. When clinical neurologists visually inspect an electroencephalogram, their vague criteria for declaring it random-like are a far cry from the distinguishers that cryptographers use to separate deterministic sequences from random sequences. As Avi Wigderson (2009, p. 6) put it, "Randomness is in the eye of the beholder, or more precisely, in its computational capabilities. . . . A phenomenon (be it natural or artificial) is deemed "random enough," or pseudorandom, if the class of observers/applications we care about cannot distinguish it from random!"

Many examples of generators that appear random to observers with restricted computational powers are known. In particular, pseudorandom generators for polynomial size constant-depth circuits have been constructed in Ajtai and Wigderson (1985); later, this work was greatly simplified and improved in Nisan (1991). O'Connor (1988) proved that an infinite binary sequence appears random to all finite-state machines if and only if it is ∞-distributed. Pseudorandom generators for space-bounded computation have been constructed in Nisan (1992). It is conceivable that McCulloch-Pitts dynamical systems could fool neurologists into finding their trajectories unpredictable just as they find normal electroencephalograms unpredictable. Proving this in a formal setting with a suitable definition of *neurologists* is an interesting challenge.

A variation on our theme comes from the idea that in a brain of n neurons, only m neurons may be visible to the observer and the remaining $n-m$ are hidden from view. Formally, given positive integers m, n such that $m \leq n$ and given a McCulloch-Pitts dynamical system $\Phi : \{0, 1\}^n \rightarrow \{0, 1\}^n$, we may consider the mapping $\Phi_m : \{0, 1\}^n \rightarrow \{0, 1\}^m$ such that $\Phi_m(x)$ is the m-bit prefix of $\Phi(x)$. Can such mappings provide pseudorandomness? Our theorem 1 shows that the answer is negative when $m = n$; one of the reviewers argued that under the usual assumption that one-way functions exist, the answer is close to affirmative when $m = 1$. Here is the argument. Every one-way function f (as every Boolean function) can be computed by a threshold circuit (Parberry, 1994). When this circuit has n gates and depth d, it can be embedded in a McCulloch-Pitts dynamical system $\Phi : \{0, 1\}^n \rightarrow \{0, 1\}^n$, where the results of its computation show up with the time delay of d units. Now f is represented in the d-fold iteration of Φ and there is an appropriate projection π, the hard-core bit (Goldreich & Levin, 1989), such that the sequence $\pi(x), \pi(f(x)), \pi(f(f(x))), \ldots$ is pseudorandom.

Statistical properties of Φ_1 have been studied in Goldsmith (2015). For instance, there is a McCulloch-Pitts dynamical system $\Phi : \{0, 1\}^{37} \rightarrow \{0, 1\}^{37}$ such that the restriction of the trajectory of Φ on the first bit passes all 10 statistical tests of the battery `SmallCrush` implemented in the software library TestU01 of L'Ecuyer and Simard (2007, 2009).

Acknowledgments

This research was undertaken in part with funding from the Canada Research Chairs program and from the Natural Sciences and Engineering Research Council of Canada. We are grateful to Péter Gács for helpful comments on a draft of this note and to Avi Wigderson for telling us about

Nisan's papers (Nisan, 1991, 1992). We also thank the two anonymous reviewers for their thoughtful comments that helped us improve the presentation considerably.

References

Ajtai, M., & Wigderson, A. (1985). Deterministic simulation of probabilistic constant depth circuits. In *Proceedings of the 26th Annual Symposium on Foundations of Computer Science* (pp. 11–19). Piscataway, NJ: IEEE.

Altunay, S., Telatar, Z., & Erogul, O. (2010). Epileptic EEG detection using the linear prediction error energy. *Expert Systems with Applications*, *37*, 5661–5665.

Applebaum, B., Ishai, Y., & Kushilevitz, E. (2010). Cryptography by cellular automata or how fast can complexity emerge in nature? In Innovations in Computer Science 2009 (pp. 1–19). Beijing: Tsinghua University Press.

Chaovalitwongse, W. A. (2009). Optimization and data mining in epilepsy research: A review and prospective. In P. M. Pardalos, M. Panos, & H. E. Romeijn (Eds.), *Handbook of optimization in medicine* (pp. 1–32). New York: Springer.

Chvátal, V., & Goldsmith, M. (2012). Can brains generate random numbers? arXiv:1208.6451 [math, q-bio].

Cover, T. (1965). Geometrical and statistical properties of systems of linear inequalities with applications in pattern recognition. *IEEE Transactions on Electronic Computers, EC-14*(3), 326–334.

Da Silva, F. L., Blanes, W., Kalitzin, S. N., Parra, J., Suffczynski, P., & Velis, D. N. (2003). Epilepsies as dynamical diseases of brain systems: Basic models of the transition between normal and epileptic activity. *Epilepsia*, *44*, 72–83.

Elyada, Y. M., & Horn, D. (2005). Can dynamic neural filters produce pseudo-random sequences? In W. Duch, E. Oja, & S. Zadrozny (Eds.), *Artificial neural networks: Biological inspirations–ICANN 2005* (pp. 211–216). New York: Springer.

Goldreich, O., Goldwasser, S., & Micali, S. (1986). How to construct random functions. *Journal of the ACM*, *33*(4), 792–807.

Goldreich, O., & Levin, L. A. (1989). A hard-core predicate for all one-way functions. In D. S. Johnson (Ed.), *Proceedings of the 21st Annual ACM Symposium on Theory of Computing* (pp. 25–32). New York: ACM.

Goldsmith, M. (2015). *Neural networks as pseudorandom number generators*. Unpublished doctoral dissertation, Concordia University.

Hoeffding, W. (1963). Probability inequalities for sums of bounded random variables. *Journal of the American Statistical Association*, *58*(301), 13–30.

Iasemidis, L. D., Shiau, D.-S., Sackellares, J. C., Pardalos, P. M., & Prasad, A. (2004). Dynamical resetting of the human brain at epileptic seizures: Application of nonlinear dynamics and global optimization techniques. *IEEE Transactions on Bio-Medical Engineering*, *51*(3), 493–506.

Khachiyan, L. G. (1979). A polynomial algorithm in linear programming. *Doklady Akademii Nauk SSSR*(244), 1093–1096. (in Russian)

Knuth, D. E. (1998). *The art of computer programming, vol. 2: Seminumerical algorithms* (3rd ed.). Upper Saddle River, NJ: Pearson Education.

Krause, M., & Lucks, S. (2001). Pseudorandom functions in TC^0 and cryptographic limitations to proving lower bounds. *Computational Complexity*, *10*(4), 297–313.

L'Ecuyer, P., & Simard, R. (2007). TestU01: A C library for empirical testing of random number generators. *ACM Trans. Math. Softw.*, *33*(4).

L'Ecuyer, P., & Simard, R. (2009). *TestU01: A software library in ANSI C for empirical testing of random number generators. User's guide, compact version.* http://www.iro.umontreal.ca/∼simardr/testu01/guideshorttestu01.pdf.

Lehnertz, K., Andrzejak, R. G., Arnhold, J., Kreuz, T., Mormann, F., Rieke, C., … Elger, C. E. (2001). Nonlinear EEG analysis in epilepsy: Its possible use for interictal focus localization, seizure anticipation, and prevention. *Journal of Clinical Neurophysiology*, *18*(3), 209–222.

Liu, A., Hahn, J. S., Heldt, G. P., & Coen, R. W. (1992). Detection of neonatal seizures through computerized EEG analysis. *Electroencephalography and Clinical Neurophysiology*, *82*(1), 30–37.

McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics*, *5*(4), 115–133.

Naor, M., Pinkas, B., & Reingold, O. (1999). Distributed pseudo-random functions and KDCs. In *Advances in Cryptology–EUROCRYPT99* (pp. 327–346). New York: Springer.

Naor, M., & Reingold, O. (1995). Synthesizers and their application to the parallel construction of pseudo-random functions. In *Proceedings of the 36th Annual Symposium on Foundations of Computer Science* (pp. 170–181). Piscataway, NJ: IEEE.

Naor, M., & Reingold, O. (2004). Number-theoretic constructions of efficient pseudorandom functions. *Journal of the ACM*, *51*(2), 231–262.

Nielsen, J. B. (2002). A threshold pseudorandom function construction and its applications. In *Advances in Cryptology-Crypto 2002* (pp. 401–416). New York: Springer.

Nisan, N. (1991). Pseudorandom bits for constant depth circuits. *Combinatorica*, *11*, 63–70.

Nisan, N. (1992). Pseudorandom generators for space-bounded computation. *Combinatorica*, *12*, 449–461.

Ocak, H. (2009). Automatic detection of epileptic seizures in EEG using discrete wavelet transform and approximate entropy. *Expert Systems with Applications*, *36*(2, Part 1), 2027–2036.

O'Connor, M. (1988). An unpredictability approach to finite-state randomness. *Journal of Computer and System Sciences*, *37*, 324–336.

Parberry, I. (1994). *Circuit complexity and neural networks*. Cambridge, MA: MIT Press.

Radon, J. (1921). Mengen konvexer körper, die einen gemeinsamen punkt enthalten. *Mathematische Annalen*, *83*(1), 113–115.

Rosenblatt, F. (1957). The perceptron—a perceiving and recognizing automation (Report 85-460-1). Ithaca, NY: Cornell Aeronautical Laboratory.

Sauer, N. (1972). On the density of families of sets. *Journal of Combinatorial Theory, Series A*, *13*(1), 145–147.

Shelah, S. (1972). A combinatorial problem; Stability and order for models and theories in infinitary languages. *Pacific Journal of Mathematics*, *41*(1), 247–261.

Tucker, A. W. (1955). Linear inequalities and convex polyhedral sets. In *Proc. of 2nd Symp. Linear Programming* (pp. 569–602). Washington, DC: National Bureau of Standards.

Wigderson, A. (2009). Randomness and pseudorandomness. *Institute Letter*. http://www.ias.edu/files/pdfs/publications/letter-2009-summer.pdf

Winder, R. (1966). Partitions of *N*-space by hyperplanes. *SIAM Journal on Applied Mathematics*, *14*(4), 811–818.

Received April 7, 2015; accepted February 21, 2016.