CDMTCS Research Report Series

Opening the Book of Randomness (Extended Version)

Cristian S. Calude
Michael J. Dinneen
Department of Computer Science
University of Auckland
Auckland, New Zealand

Anna M. Gardner
Artist
Auckland, New Zealand

CDMTCS-393
October 2010

Centre for Discrete Mathematics and
Theoretical Computer Science

Opening the Book of Randomness (Extended Version)

Cristian S. Calude, Michael J. Dinneen, Anna M. Gardner

Abstract

In this note we try to establish visual representations of various types of random binary sequences. The main focus is on comparing quantum randomness and algorithmic generated psuedo-randomness.

1 Commentary

The concept of randomness is as old as humankind. While feared as a cause of disarray and misfortune, randomness is revered for its role in the evolution and renewal of life and as source of innovation. Random numbers have been around for more than 4,000 years, but never have they been in such demand as in our time. People use random numbers everywhere: for holding drawings, lotteries and sweepstakes, for gaming and gambling, for scientific computing, for running (routing) and using (banking) the Internet, and for visual arts and music.

But, are random numbers, random? In the last century important progress has been made in understanding the concept of randomness and, as a consequence, in random number generation. This was possible because of the advent of algorithmic mathematics, computer science and quantum mechanics.

Randomness plays an essential role in probability theory, the mathematical calculus of random events. The power and weakness of this theory resides in the fact that it assumes that random individual objects (events) exist, but it does not define them. Algorithmic information the-

ory, developed in the 1960s, defines and studies individual random objects, like finite bit strings or infinite sequences. [1]

"Pure randomness" or "true randomness" does not exist from a mathematical point of view. In a sense the concept of randomness is like the concepts of health or beauty. They don't exist in a pure, true form; we know of them only through symptoms. Symptoms like unpredictability, lack of patterns or correlations, incompressibility, incomputability and irreproducibility suggest randomness, but cannot guarantee it. Randomness cannot be mathematically proved: one can never be sure. There are only forms and degrees of randomness. Algorithmic randomness, the closest form of randomness to true randomness, is everywhere, even in the heart of mathematics itself.[2]

Computers can generate "random numbers" produced by algorithms. However, computer scientists needed a long time to realise that randomness produced by software is not random, but pseudo-random. This form of randomness mimics well the human perception of randomness, but its quality is rather low because computability destroys many symptoms of randomness, e.g. unpredictability. Pseudo-randomness reflects its creators "understanding" of randomness. This understanding, as with most people, is notoriously bad. For example, psychologists have known for a long time that people tend to distrust streaks in a series of random bits, hence they imagine a coin flipping sequence alternates between heads and tails much too often for its own sake of "randomness". A simple illustration of this phenomenon, called the gambler's fallacy, is the belief that after a coin has landed on tails ten consecutive times there are more chances that the coin will land on heads at the next flip.

No computer or software manufacturer claims today that its products can generate truly random numbers. However, such claims have re-appeared for randomness produced with physical experiments. For example, RANDOM.ORG[3] "offers true random numbers to anyone on the Internet." Similarly, the April 2010 issue of *Nature*[4] announced, "Truly random numbers have been generated at last". Do they really produce true/truly random numbers? Of course not. Why not? Because, as we have already pointed out, true randomness does not exist.

Quantum mechanics has the most credible claim to be one of (if not) the best form of randomness. There are many quantum phenomena which can be used for random number generation: nuclear decay radiation sources, the quantum mechanical noise source in electronic circuits

[1] C. S. Calude, G. J. Chaitin. What is ... a halting probability? Notices of the American Mathematical Society 57, 2 (2010), 236-237.

[2] G. J. Chaitin. Randomness and mathematical proof, Scientific American 232, No. 5 (May 1975), 47-52.

[3] `http://www.random.org`.

[4] doi:10.1038/news.2010.181.

(known as shot noise) or photons travelling through a semi-transparent mirror. The Quantis[5] device uses photons sent one by one through such a semi-transparent mirror or beam splitter; these are then detected in two exclusive positions (reflection/transmission), the device produces a stream of up to 16 Mega quantum random bits per second.

Understanding quantum randomness is not easy. First and foremost, understanding quantum mechanics itself is not simple business: according to Nobel Prize laureate Richard Feynman[6], "I think I can safely say that nobody understands quantum mechanics". Secondly, in the standard model of quantum mechanics, randomness[7] is postulated, not mathematically defined nor derived. Worse, not everybody believes in quantum randomness. In Einstein's words: "I am convinced that He (God) does not play dice".

Although one (probably) cannot prove that quantum randomness is algorithmically random, it is possible to assess, to some degree, its quality. One way to achieve this is to use the so-called "value indefiniteness". The book you are now reading has a weight irrespective of whether you measure it or not. In sharp contrast, some sets of quantum measurement measurables have no definite values before measurement. As a consequence one can show *that there is no way to provably compute the value of the next quantum bit before it is measured.*[8] This gives mathematical grounding to the postulated unpredictability of each individual measurement, as well as to the independence of successive measurements: one can rule out any computable causal link within the system which may give rise to the measurement outcome. *Quantum randomness is better than pseudo-randomness.* Even more, computers using quantum random bits can trespass the Turing barrier[9]: they compute the (Turing) incomputable.

Is it possible to have experimental evidence of the strong incomputability feature of quantum randomness? An affirmative answer was recently presented.[10] Tests of various symptoms of randomness have been performed on 2^{32} strings of "random" bits produced with software (Mathematica and Maple) and quantum experiments (run in the lab of the Vienna Institute for Quantum Optics and Quantum Information and with the commercial device Quantis produced at Geneva University). Most tests did not distinguish between quantum generated randomness and

[5] `http://www.idquantique.com/true-random-number-generator`

[6] The Character of Physical Law, MIT Press, 1965, Chapter 2.

[7] The irreducible indeterminacy of individual quantum processes, Born's law.

[8] C. S. Calude, K. Svozil. Quantum randomness and value indefiniteness, Advanced Science Letters 1 (2008), 165-168.

[9] Turings mathematical work on computability set up the limits of classical computation: only a tiny part of mathematical questions can be solved by computers.

[10] C. S. Calude, M. J. Dinneen, M. Dumitrescu, K. Svozil. Experimental evidence of quantum randomness incomputability, Physical Review A, 82, 022102 (2010), 1-8.

pseudo-randomness, but some did. One of them was the walk test which is based on the fact that a symptom of non-randomness of a string is detected when the plot generated by viewing the string as a 1D walk meanders “less away” from the starting point. We first present the random walks generated by four strings (of length 2 to the power 20, i.e. 1,048,576) drawn from each of the above classes. Although differences are visible on the plots, one can wonder whether there is a better way to visualise the different behaviour of quantum randomness compared with pseudo-randomness?

At the point that the artwork enters the conversation, there has already been one beginning the photon flow has been measured, its beam split. Waves of possibility have collapsed into a series of definite measures: 1s, 0s. And yet, before this book of randomness is opened there is contained inside it a new series of shifting possibilities, a second beginning of sorts.

After the first start (but before the book is opened), there has been the imposition of some new guidelines upon these definite measures. The numbers are made to wear their leashes and limits as they walk the page. For pseudo-randomness, this walk turns forever towards the limit of grey. Though its wander bends and oscillates towards white or black, pseudo randomness carries its middle grey like a burdensome memory, a limit imposed by a programmers hesitant imagining of randomness. Quantum random data has a walk that has no such steadying anchor and no locus. Its graphic origin is arbitrary while its walk may appear to go towards white or towards black, or towards grey without any ties of memory or origin, this walk is not really directional at all.

One of these sets of guidelines pushes the data quietly across the page into a series of gradients. This process is like a paint roller slowly emptying itself before reaching its certain threshold of greyness. We have found that some refuse to produce a smooth and featureless gradient, rather, they stutter a little, and heave as if the paint never covered the roller evenly in the first place.

2 Images of Random Sequences

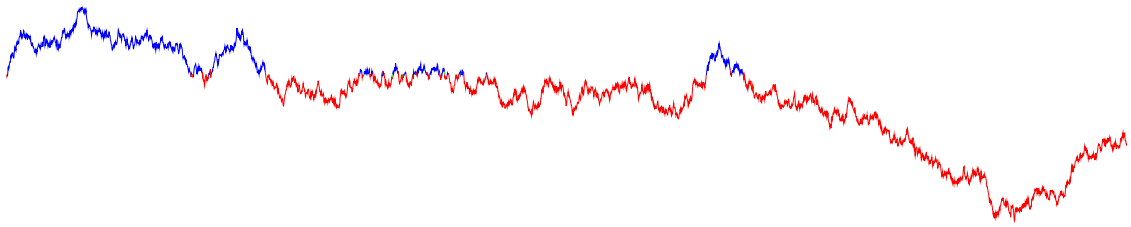

Figure 1: Horizontal linear up/down plots of the Maple sequence (intial 2^{20} bits).

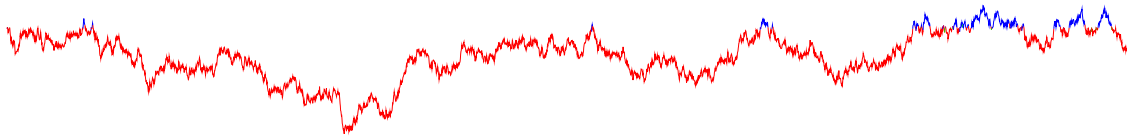

Figure 2: Horizontal linear up/down plots of the Mathematica sequence (initial 2^{20} bits).

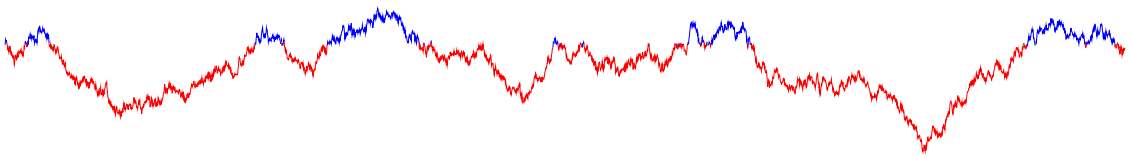

Figure 3: Horizontal linear up/down plots of the Pi sequence (initial 2^{20} bits).

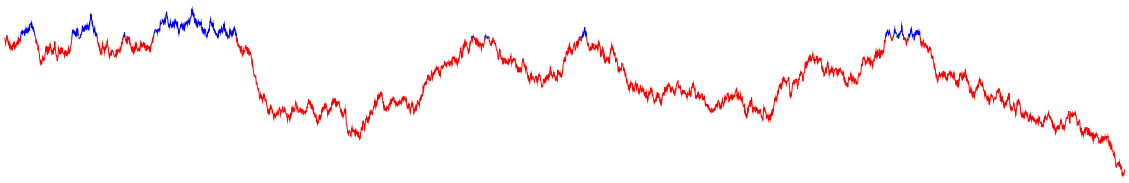

Figure 4: Horizontal linear up/down plots of the Quantis sequence (initial 2^{20} bits).

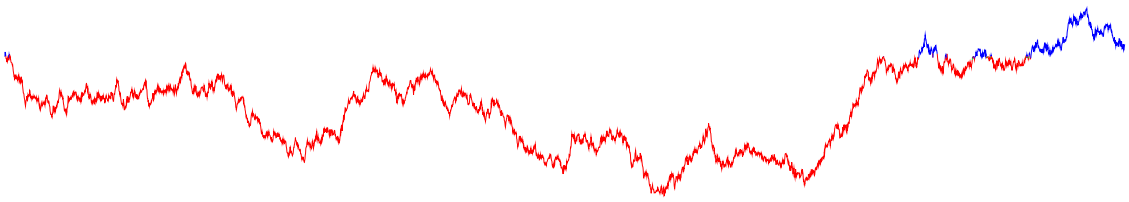

Figure 5: Horizontal linear up/down plots of the Vienna sequence (initial 2^{20} bits).

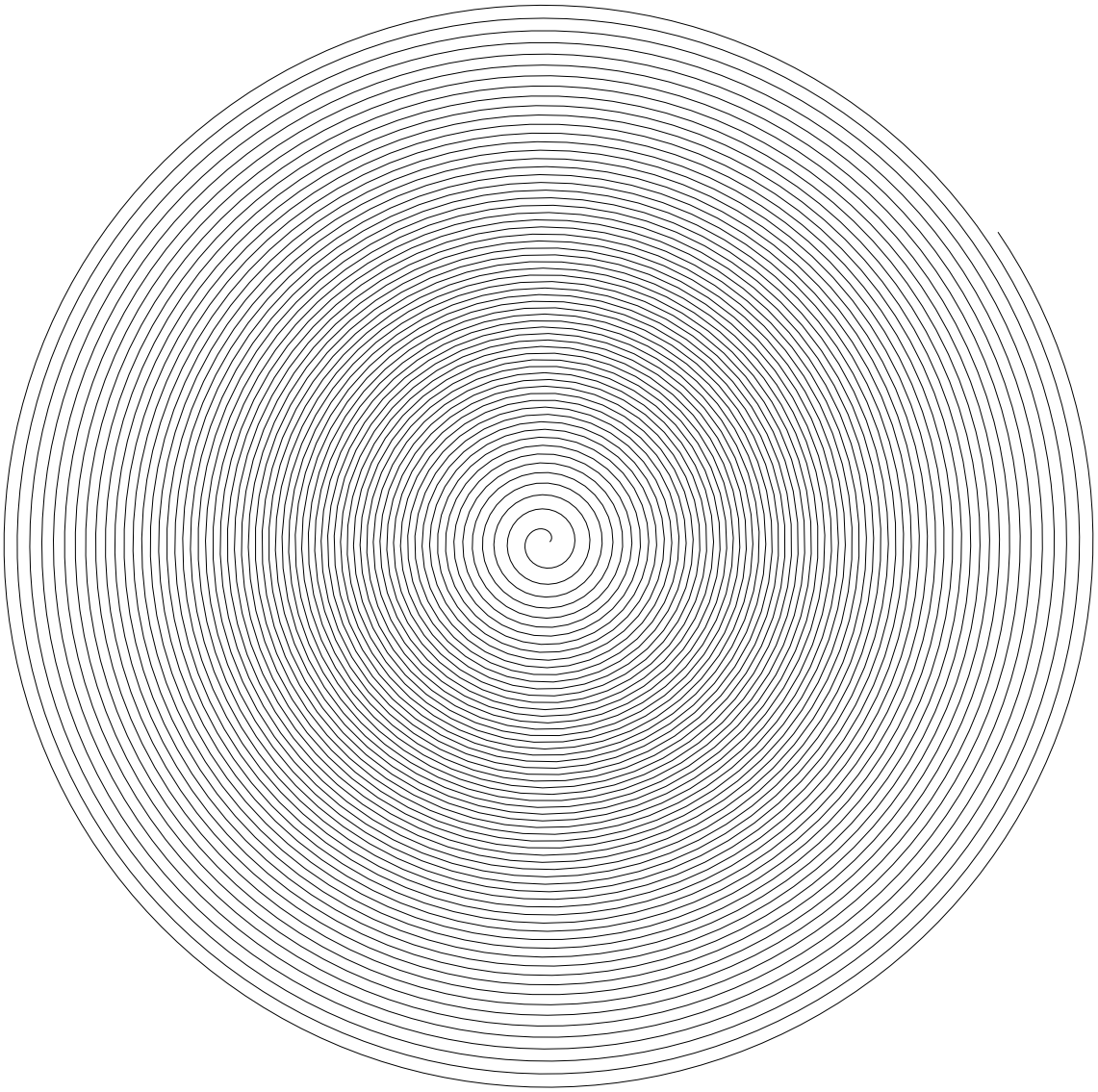

Figure 6: A base-line spiral for plotting up/down random walks to show more detail of the bits.

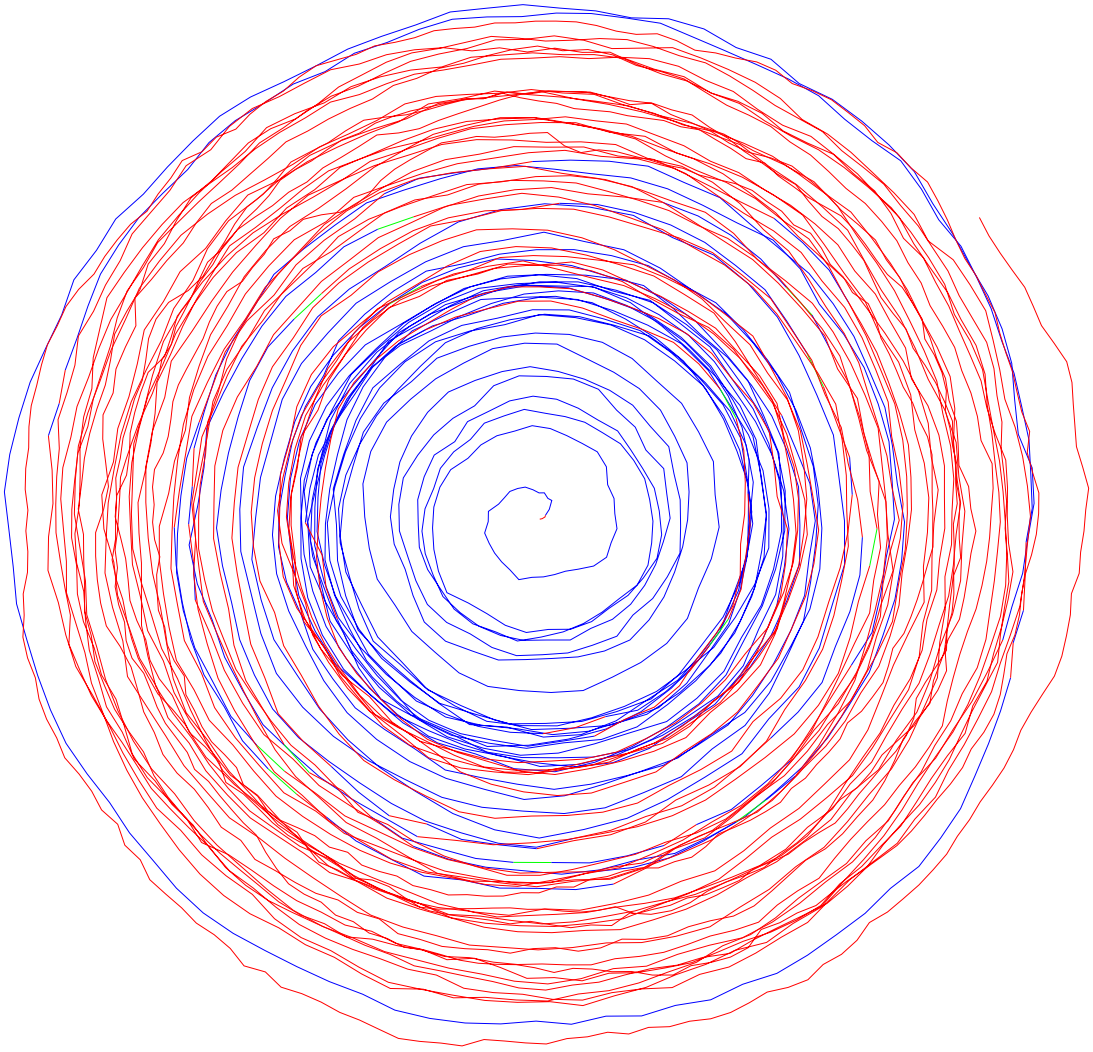

Figure 7: Wrapped Maple 2^{20} bits about a spiral.

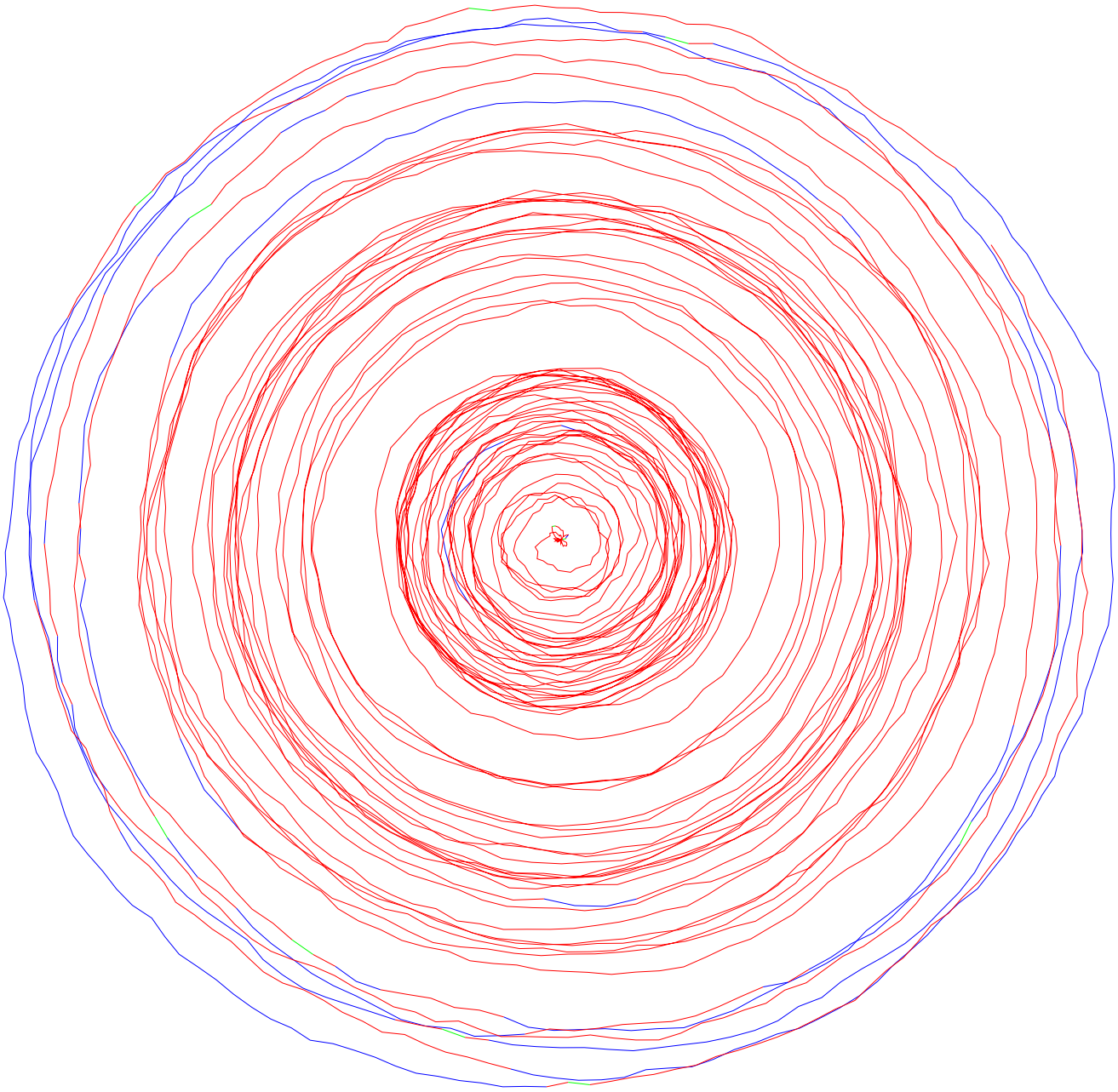

Figure 8: Wrapped Mathematica 2^{20} bits about a spiral.

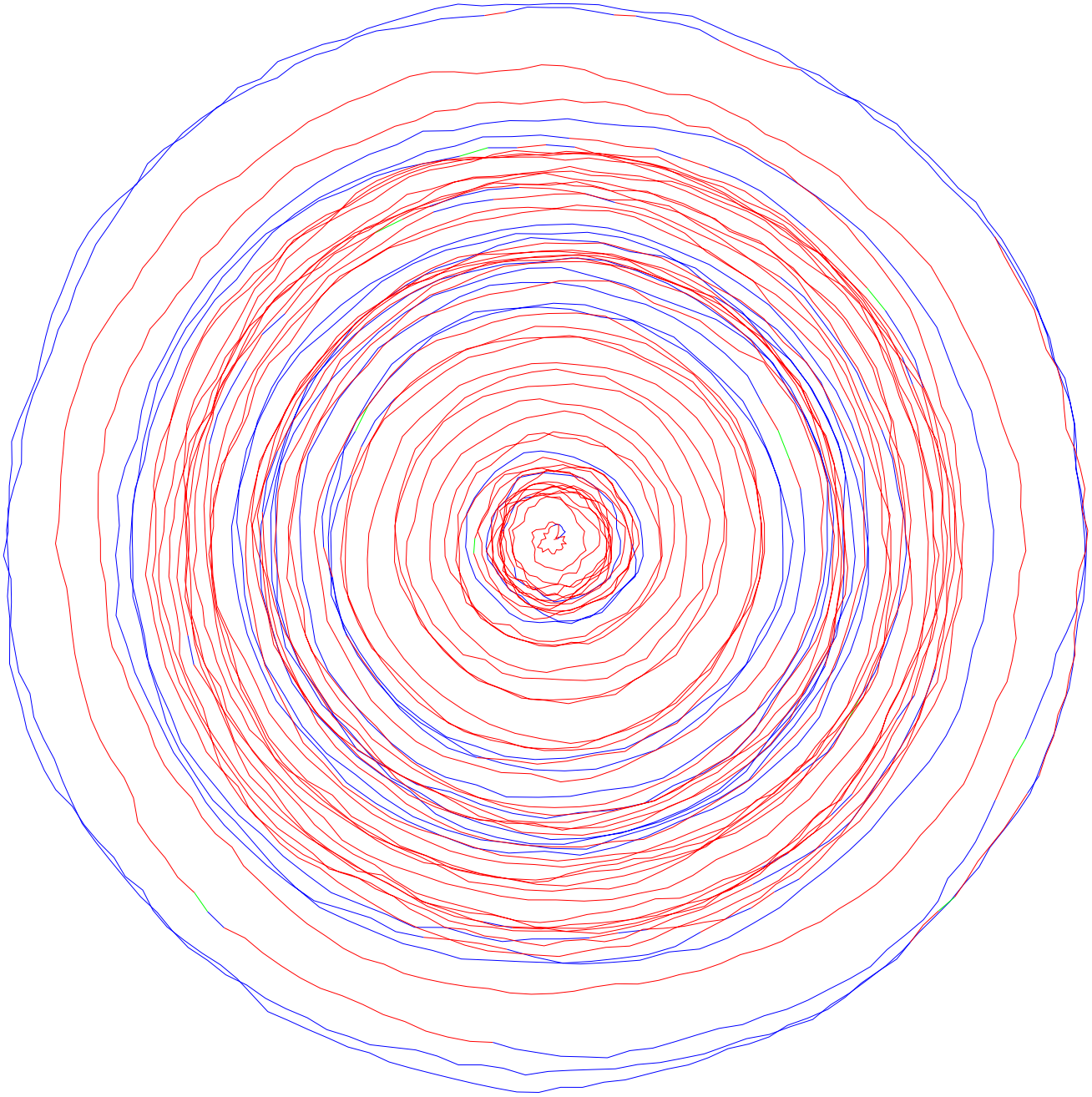

Figure 9: Wrapped Pi 2^{20} bits about a spiral.

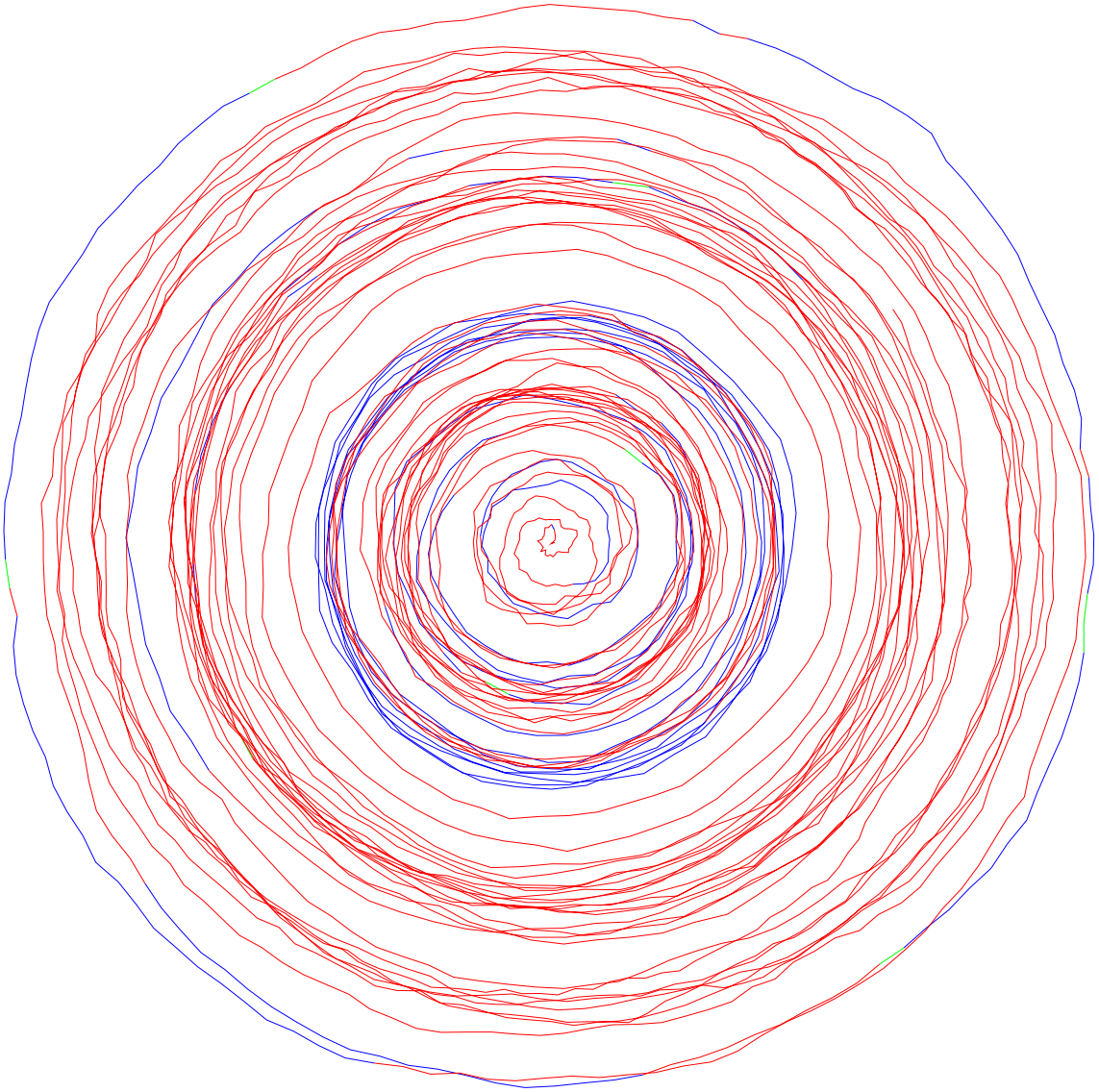

Figure 10: Wrapped Quantis 2^{20} bits about a spiral.

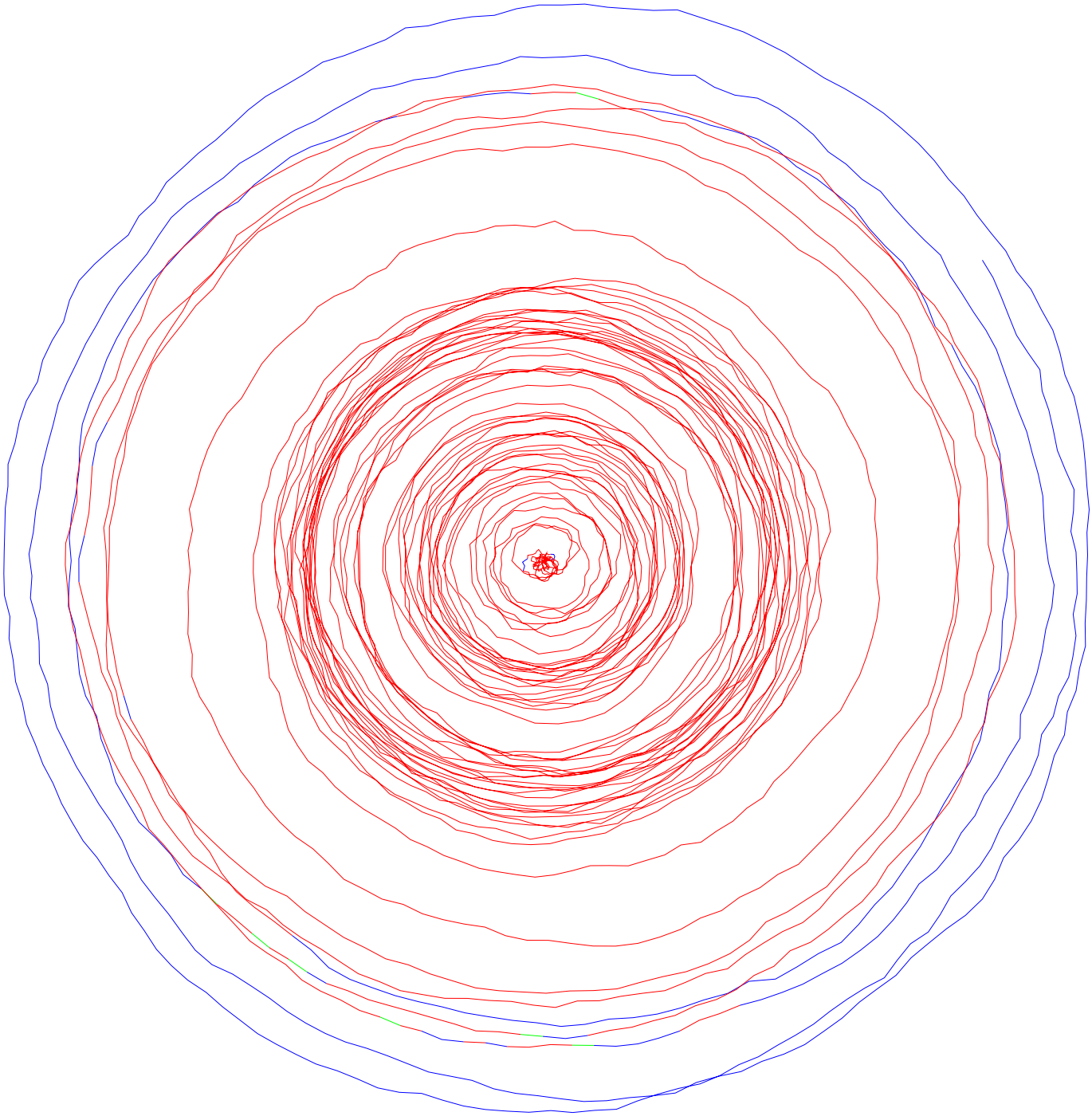

Figure 11: Wrapped Vienna 2^{20} bits about a spiral.

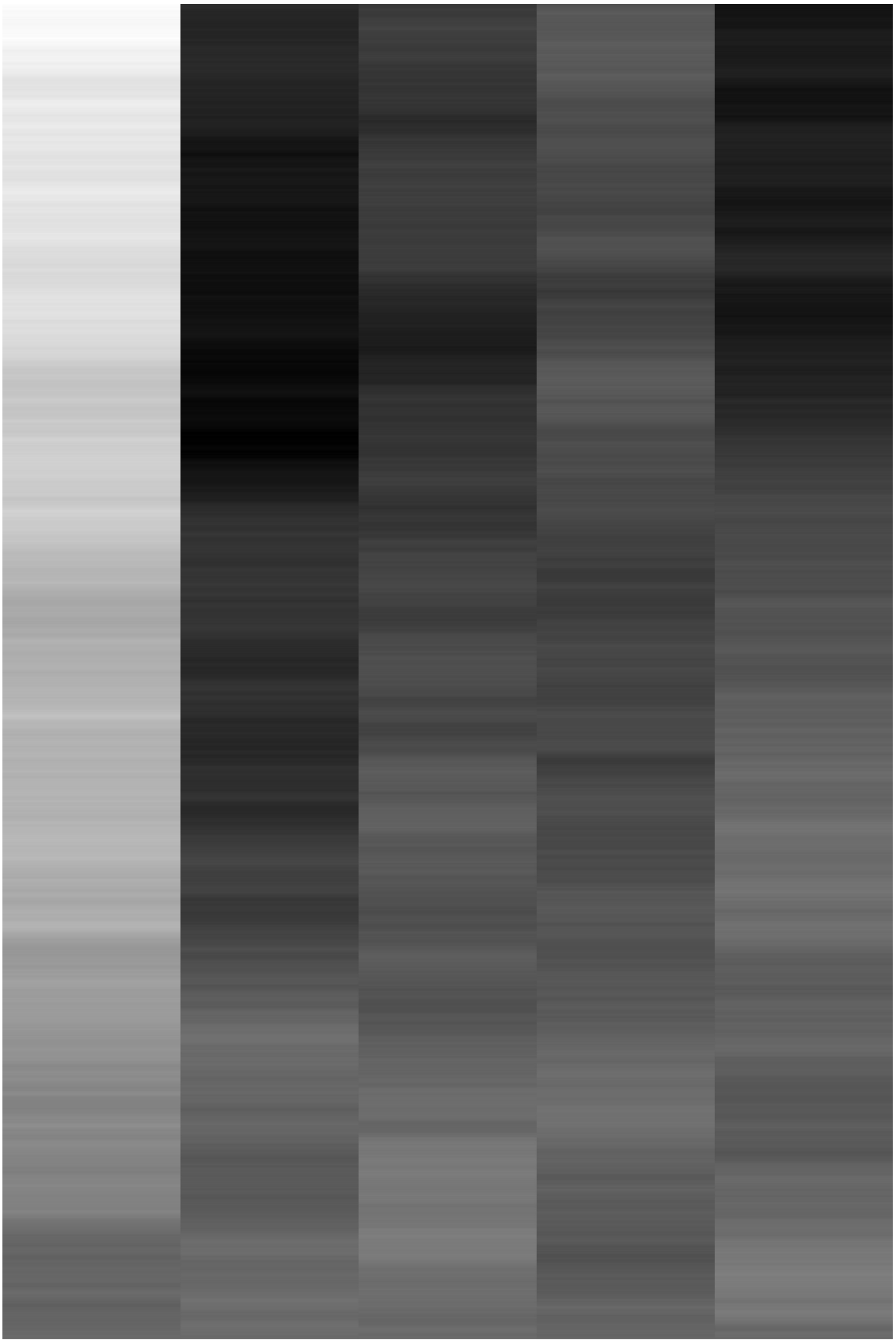

Figure 12: Greyscale random walk: From left-to-right: Maple, Mathematica, Pi, Quantis, Vienna, each 5000 bits.

Figure 13: Maple 2^{20} 2D walk with angle of walk generated from successive 8 bits.

Figure 14: Mathematica 2^{20} 2D walk with angle of walk generated from successive 8 bits.

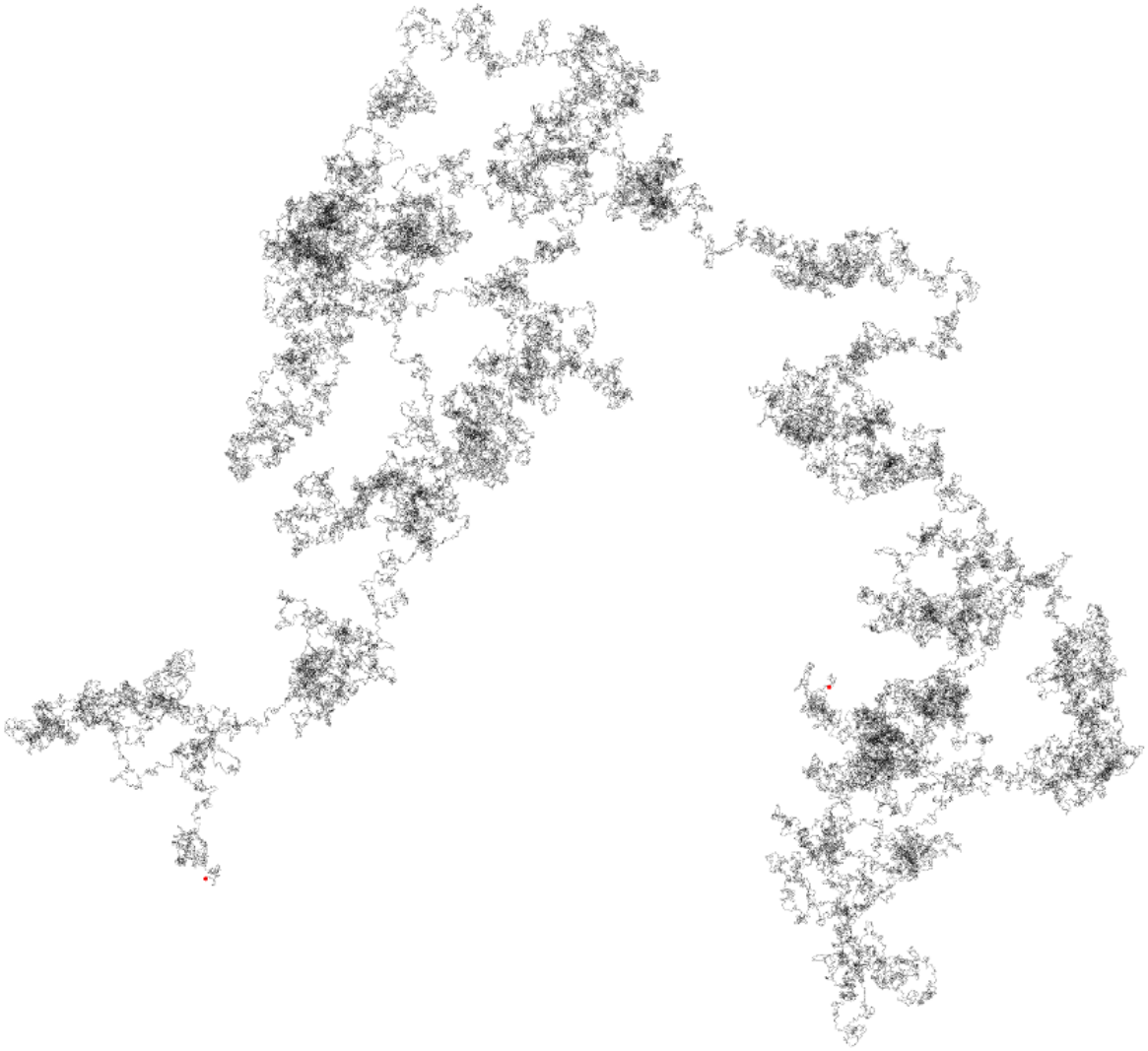

Figure 15: Pi 2^{20} 2D walk with angle of walk generated from successive 8 bits.

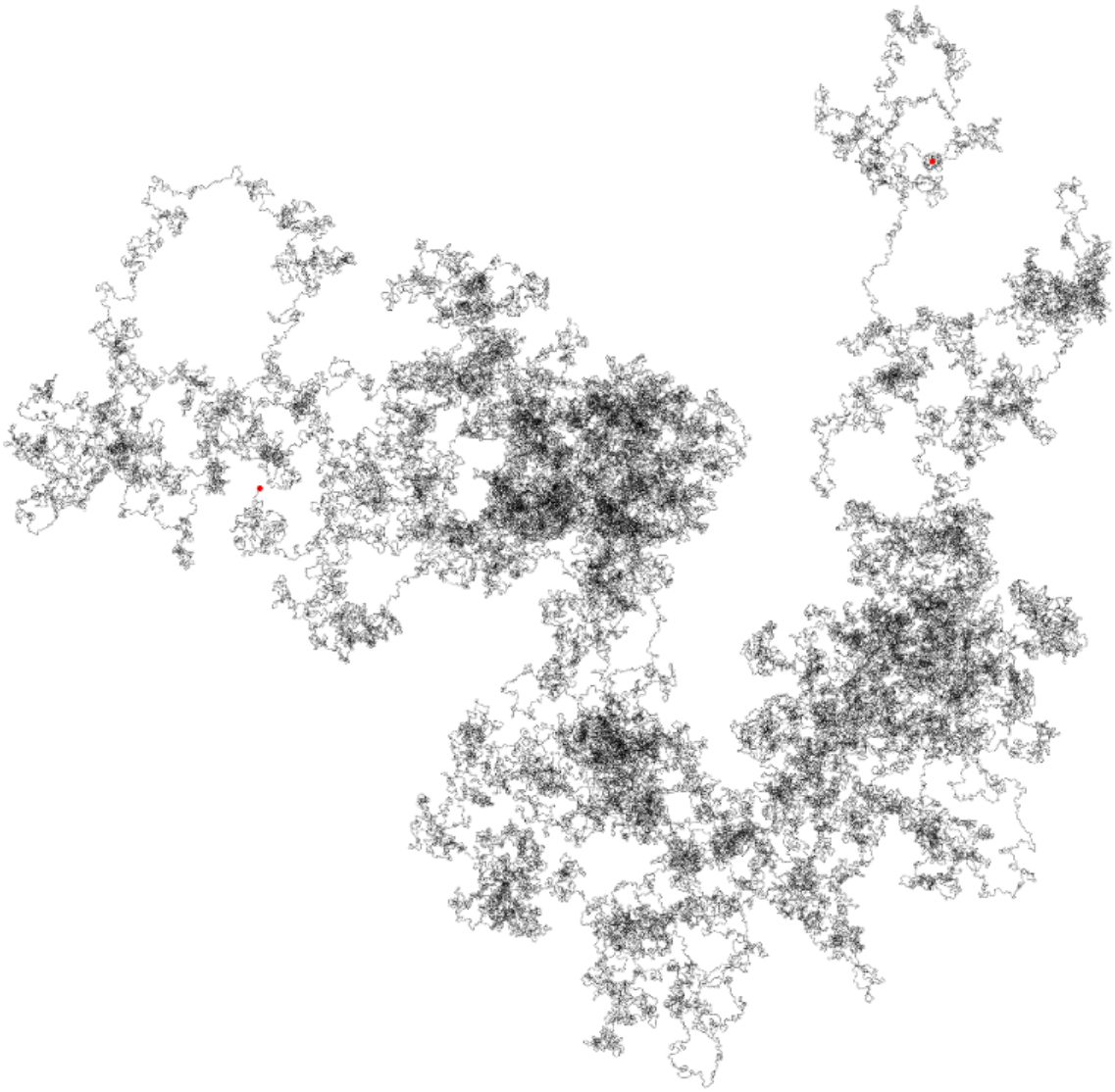

Figure 16: Quantis 2^{20} 2D walk with angle of walk generated from successive 8 bits.

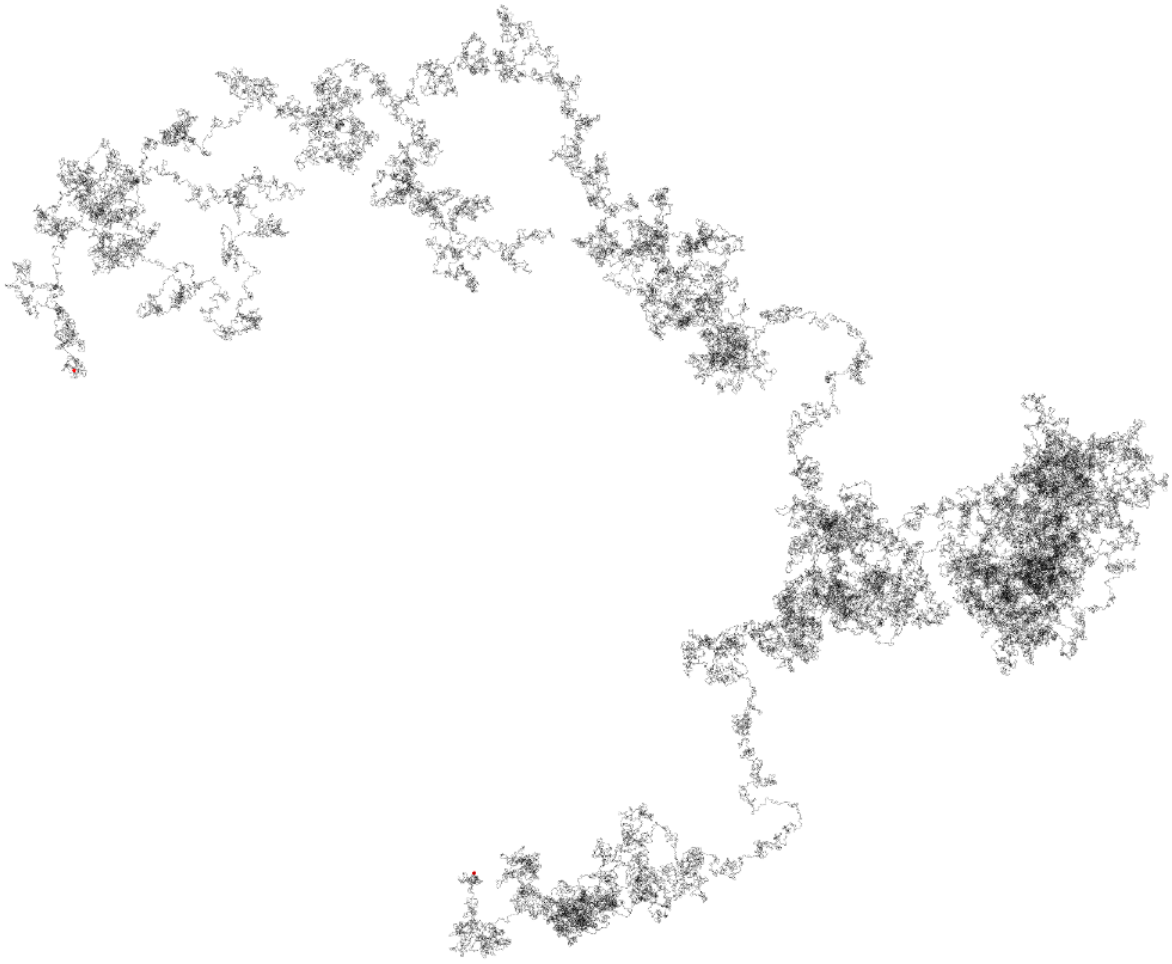

Figure 17: Vienna 2^{20} 2D walk with angle of walk generated from successive 8 bits.

Figure 18: Graph illustrating the magnitude of meander of 2^{20} Maple bits from the origin point.

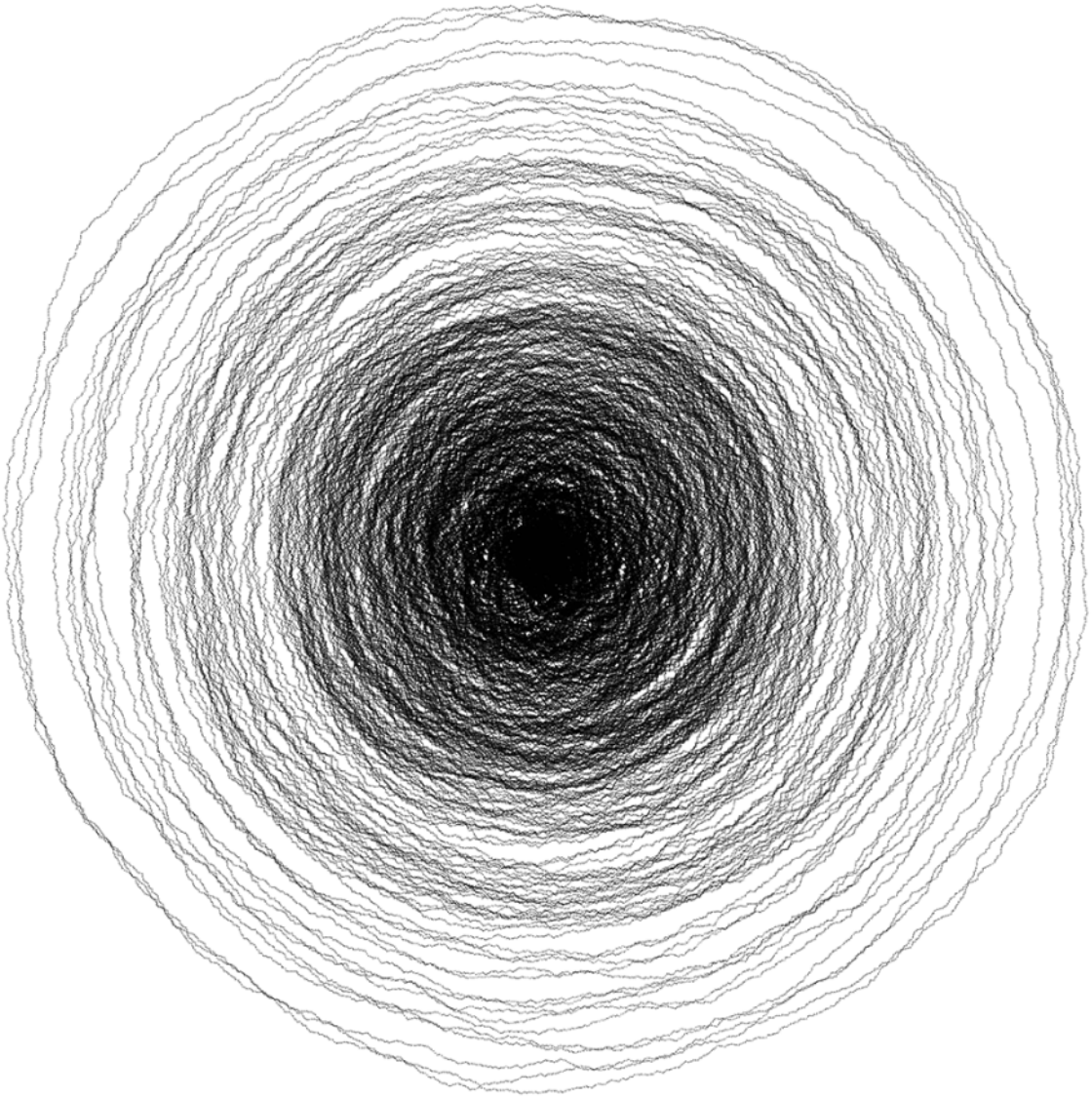

Figure 19: Graph illustrating the magnitude of meander of 2^{20} Mathematica bits from the origin point.

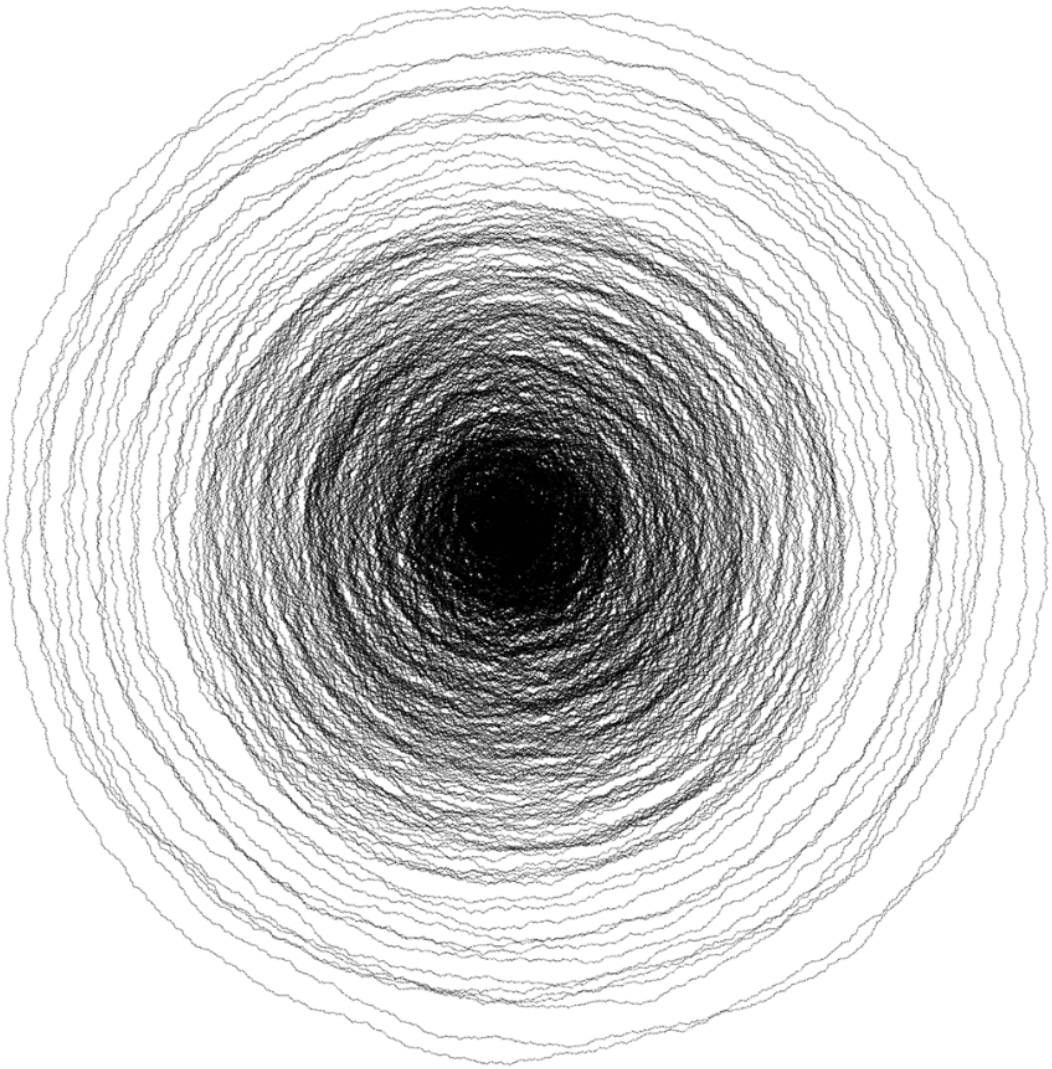

Figure 20: Graph illustrating the magnitude of meander of 2^{20} Pi bits from the origin point.

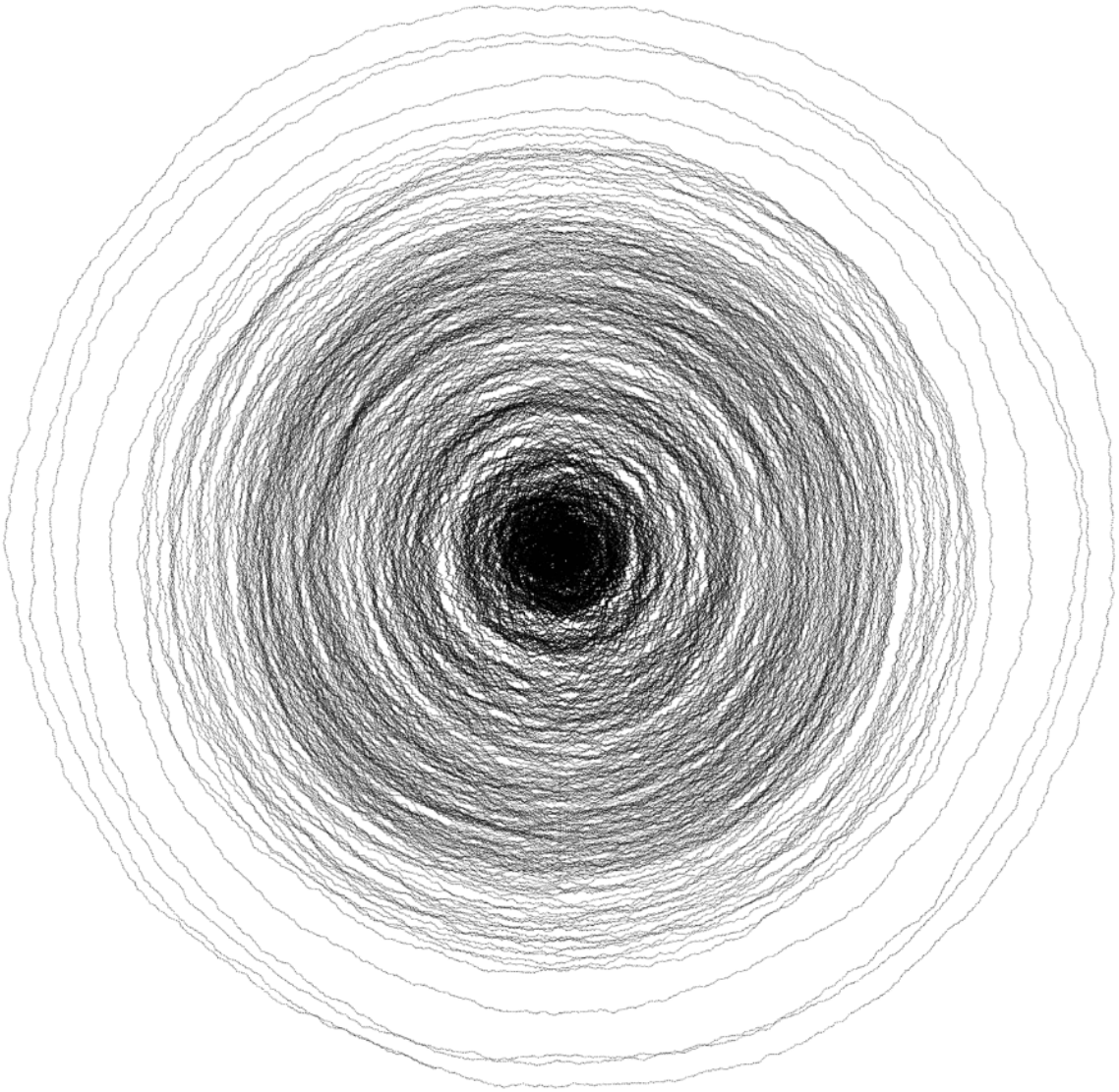

Figure 21: Graph illustrating the magnitude of meander of 2^{20} Quantis bits from the origin point.

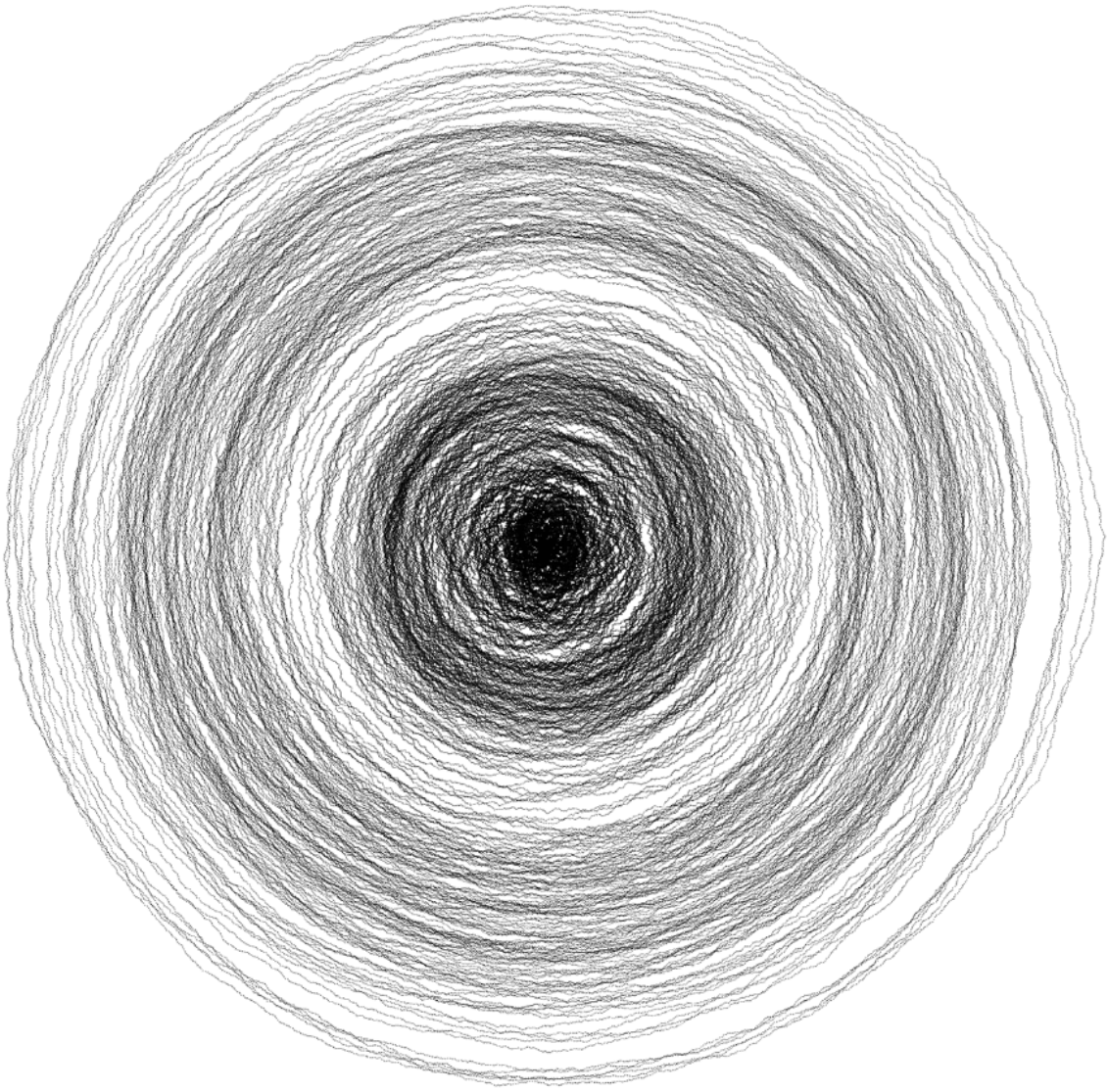

Figure 22: Graph illustrating the magnitude of meander of 2^{20} Vienna bits from the origin point.

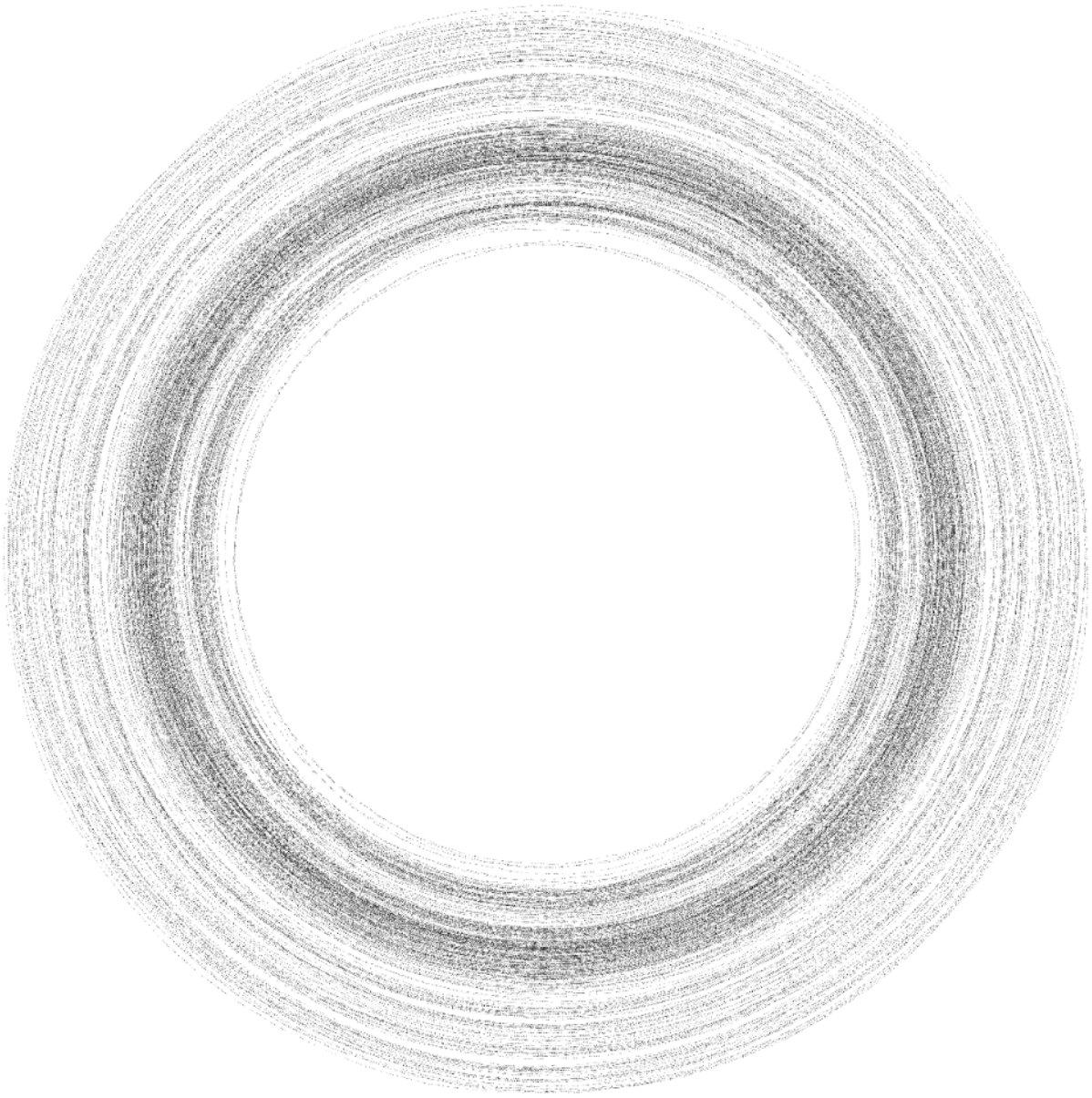

Figure 23: Graph illustrating the 2^{20} Maple bits in a random walk about a circle.

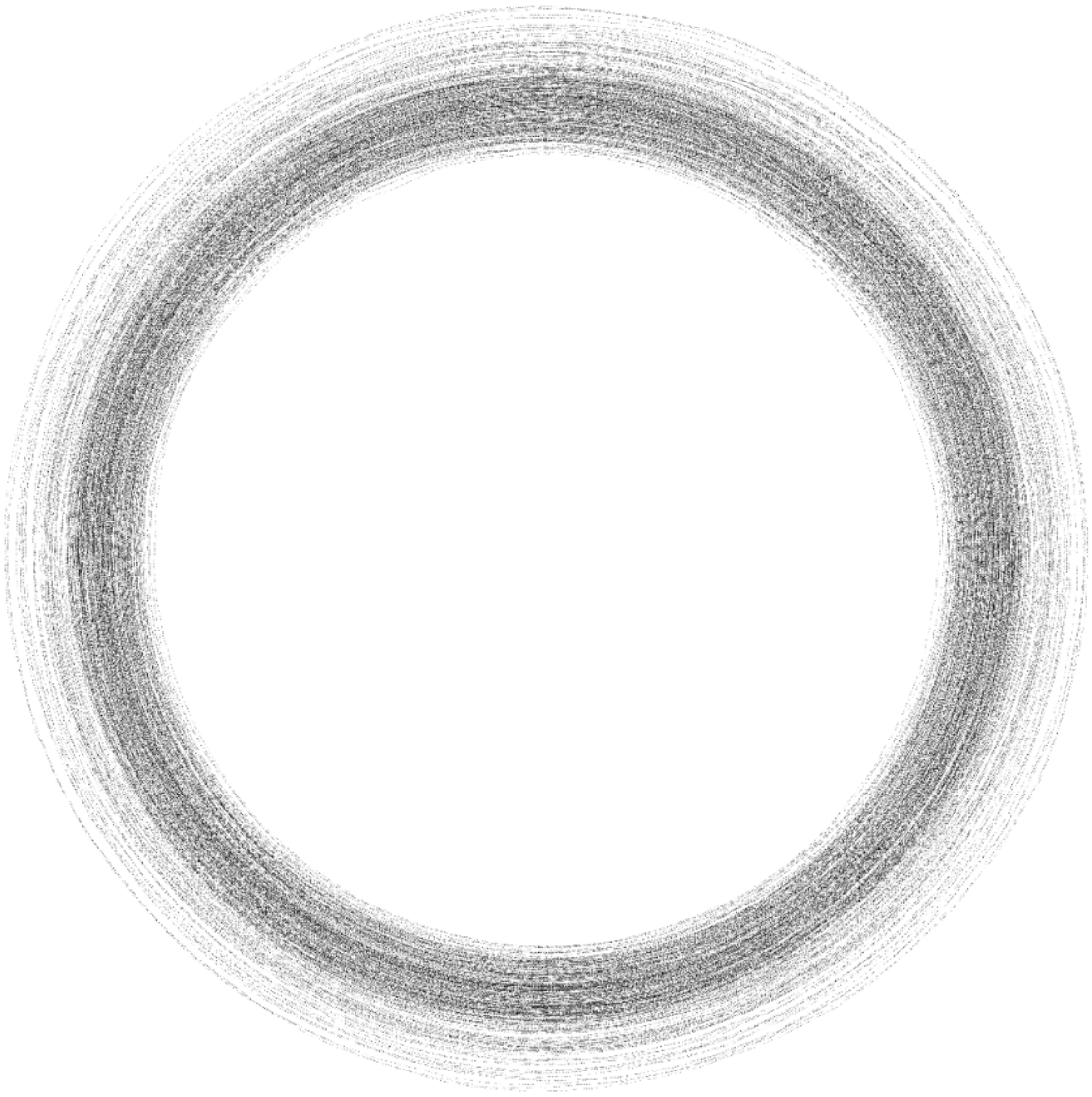

Figure 24: Graph illustrating the 2^{20} Mathematica bits in a random walk about a circle.

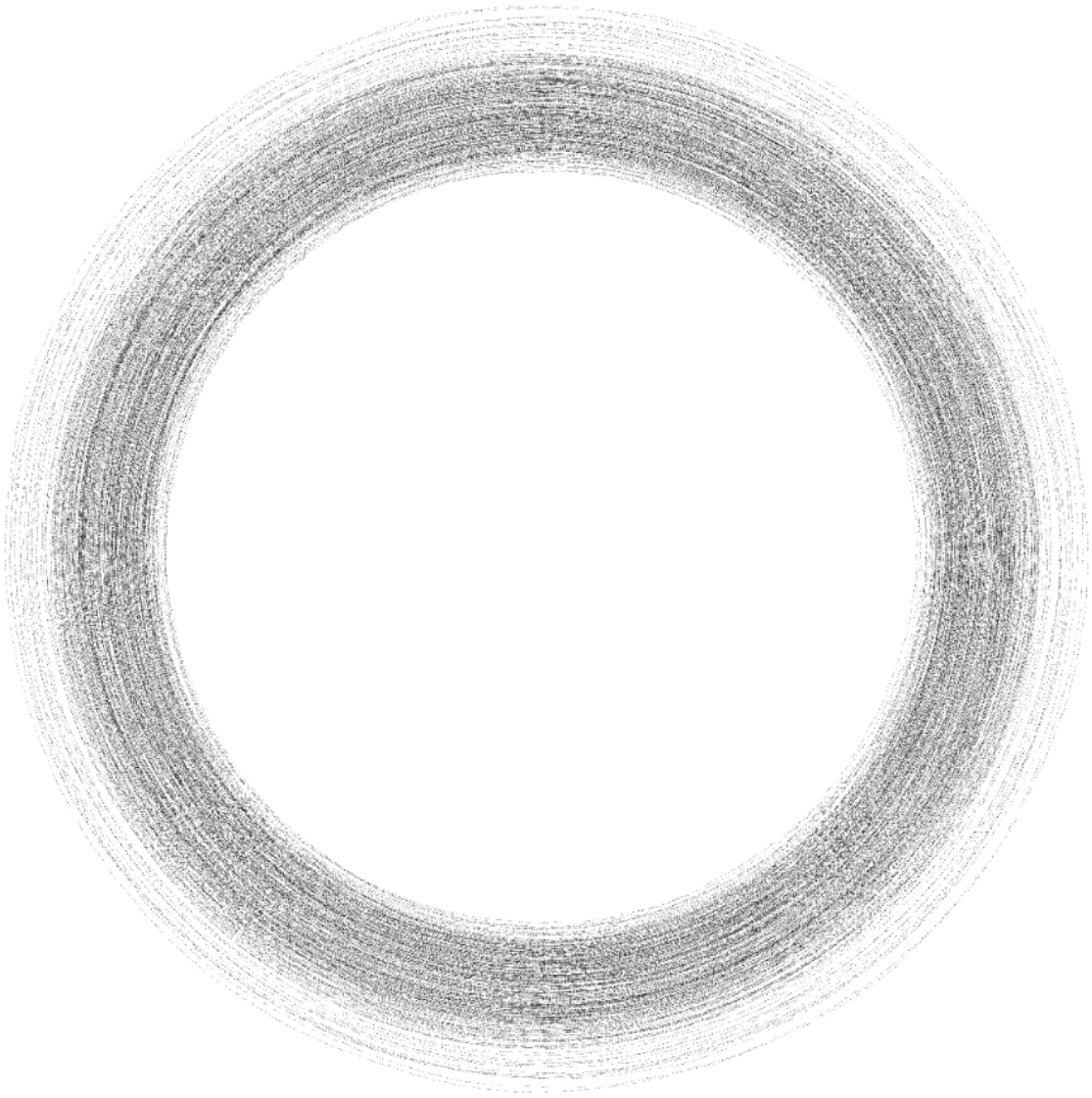

Figure 25: Graph illustrating the 2^{20} Pi bits in a random walk about a circle.

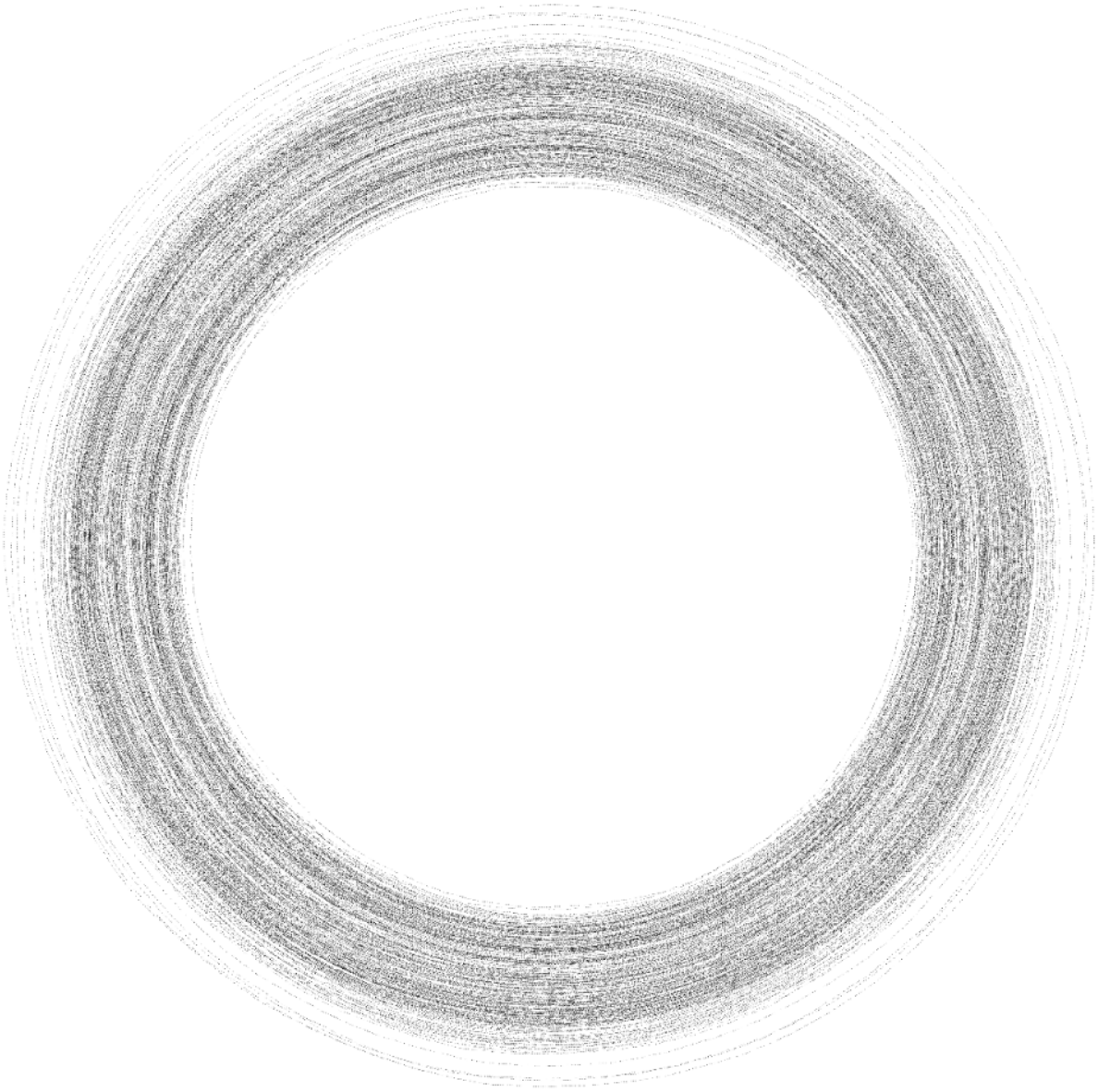

Figure 26: Graph illustrating the 2^{20} Quantis bits in a random walk about a circle.

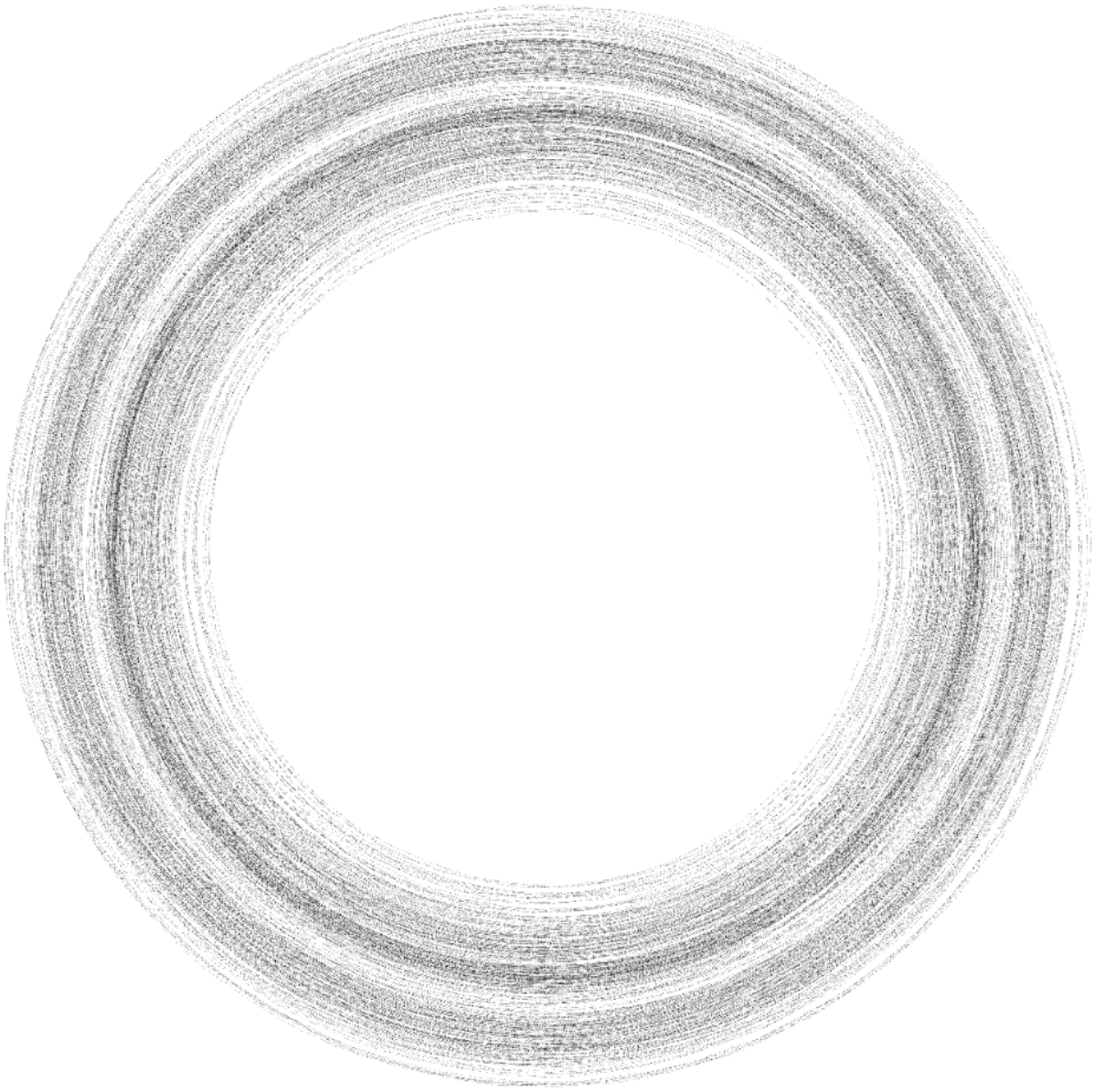

Figure 27: Graph illustrating the 2^{20} Vienna bits in a random walk about a circle.

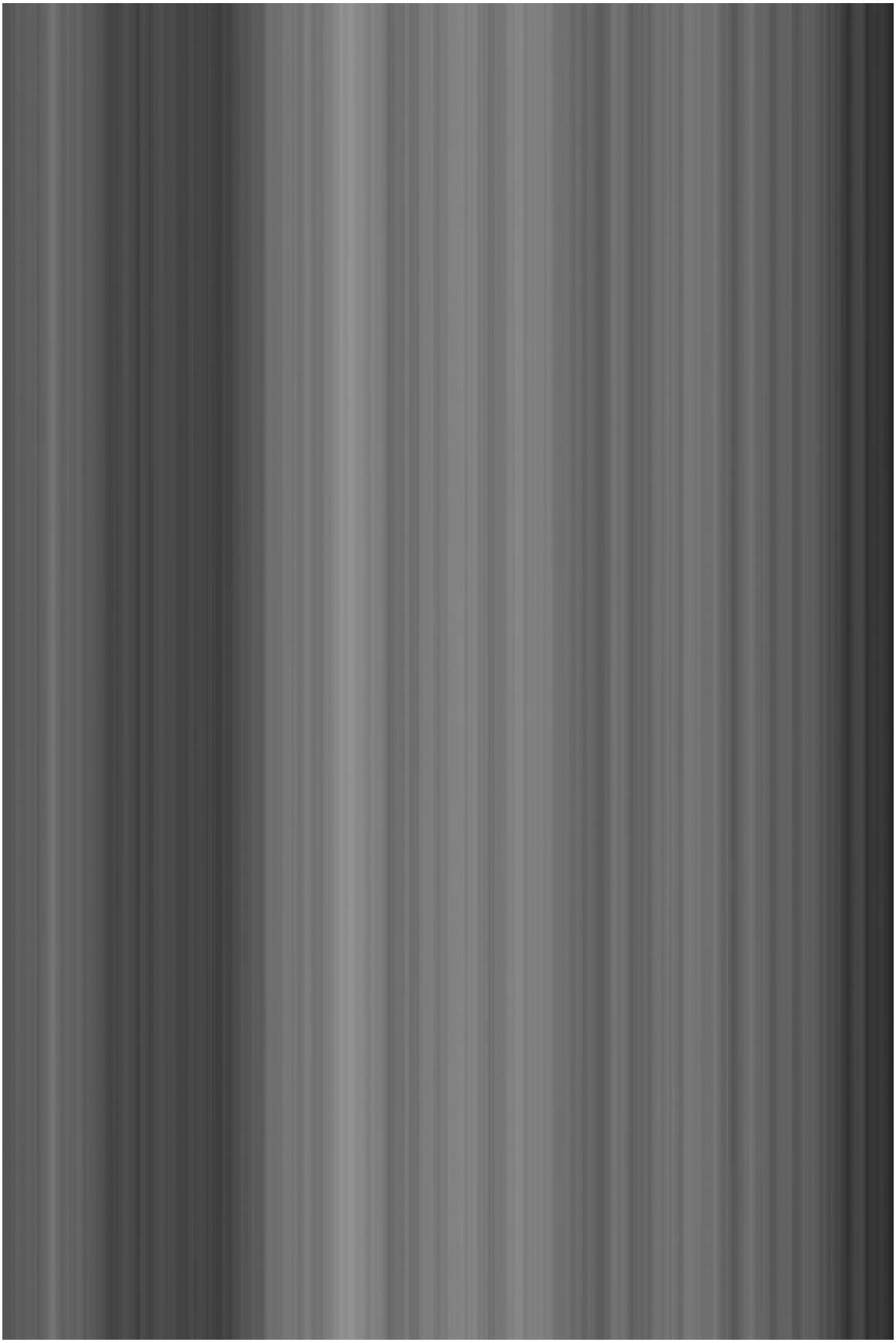

Figure 28: Greyscale random walk of 2^{24} bits of Maple with each bit associated with a single pixel at a relative greyscale value and beginning at the bottom-left and zig-zagging up/down towards the right of the page.

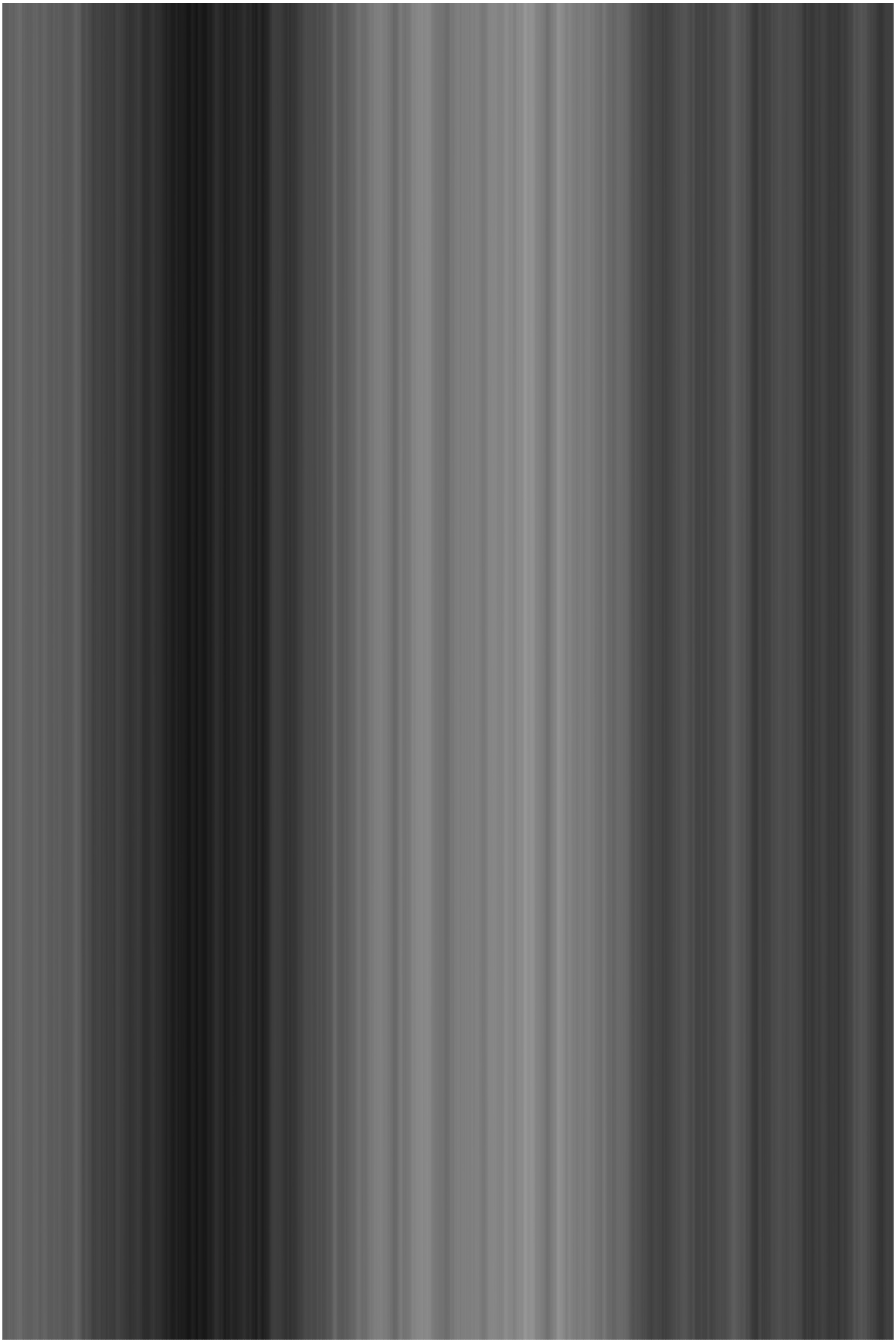

Figure 29: Greyscale random walk of 2^{24} bits of Mathematica with each bit associated with a single pixel at a relative greyscale value and beginning at the bottom-left and zig-zagging up/down towards the right of the page.

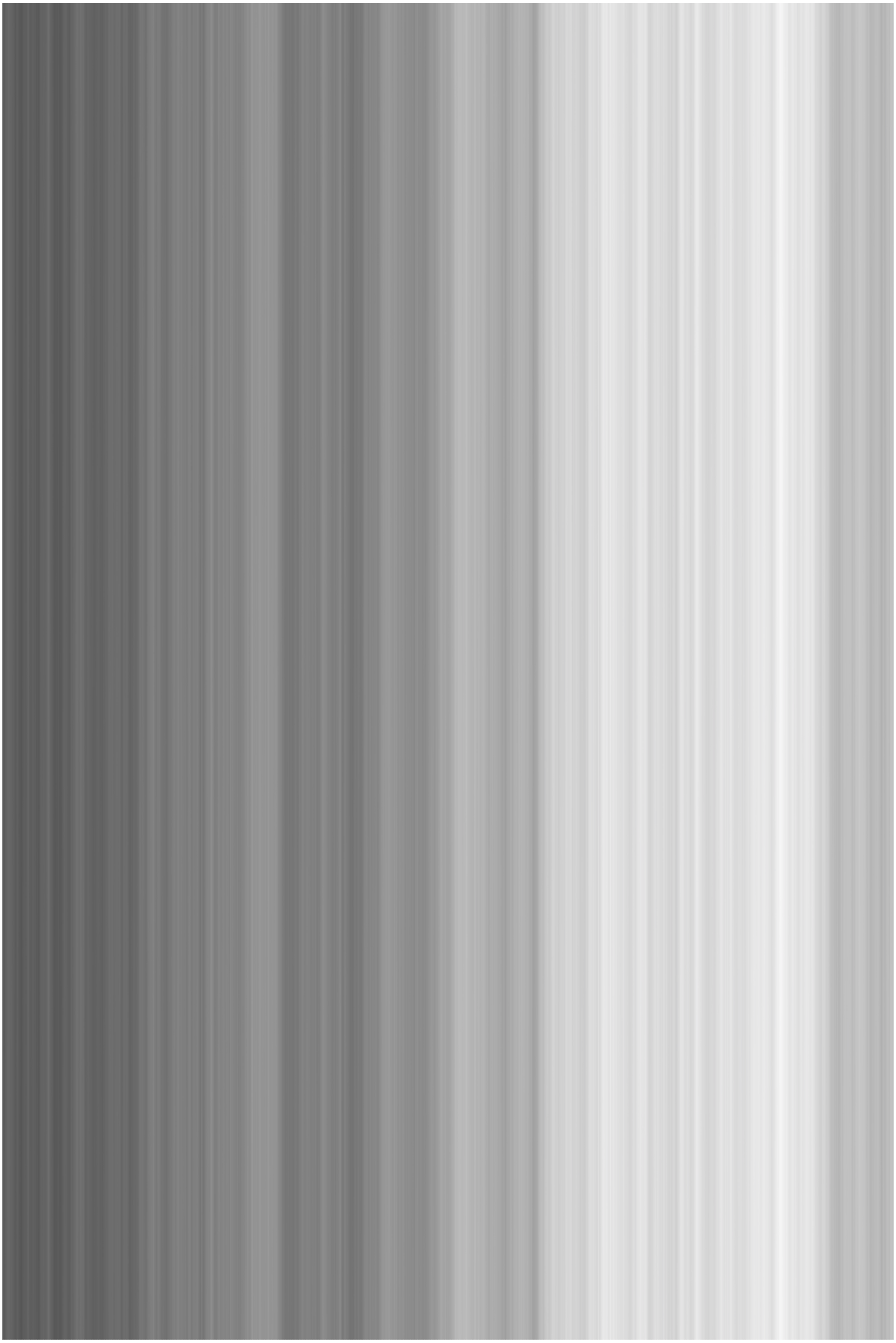

Figure 30: Greyscale random walk of 2^{24} bits of Pi with each bit associated with a single pixel at a relative greyscale value and beginning at the bottom-left and zig-zagging up/down towards the right of the page.

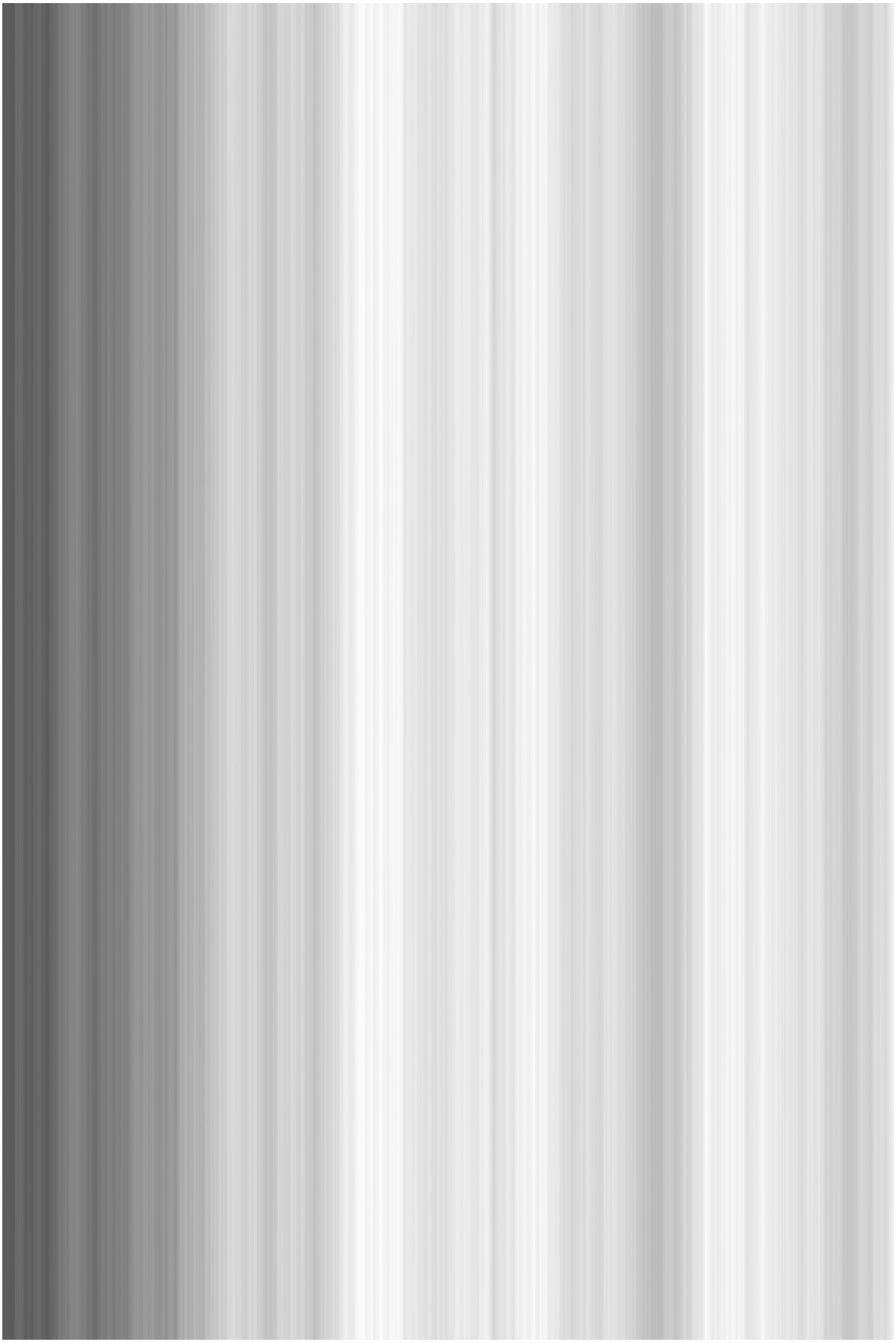

Figure 31: Greyscale random walk of 2^{24} bits of Quantis with each bit associated with a single pixel at a relative greyscale value and beginning at the bottom-left and zig-zagging up/down towards the right of the page.

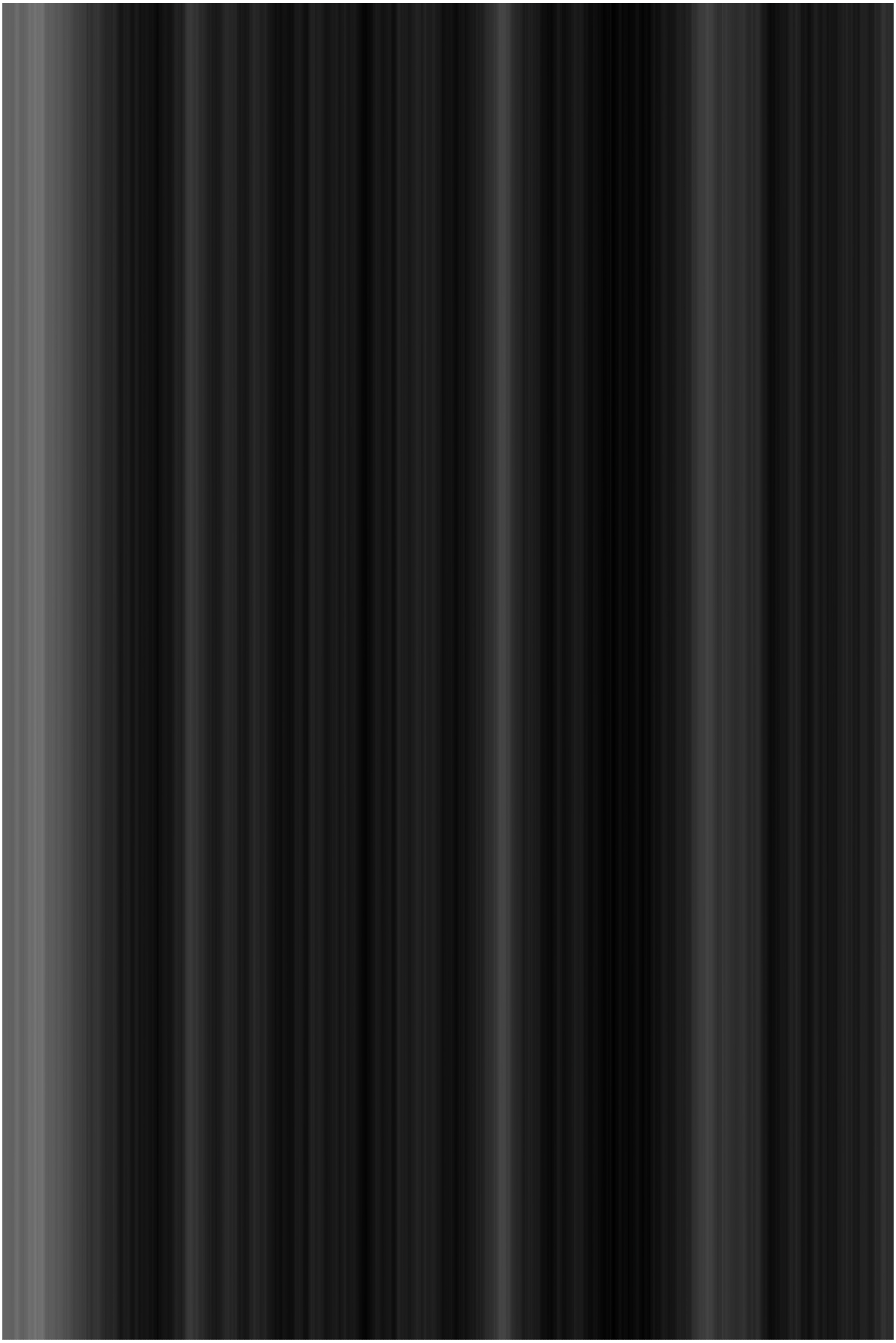

Figure 32: Greyscale random walk of 2^{24} bits of Vienna with each bit associated with a single pixel at a relative greyscale value and beginning at the bottom-left and zig-zagging up/down towards the right of the page.

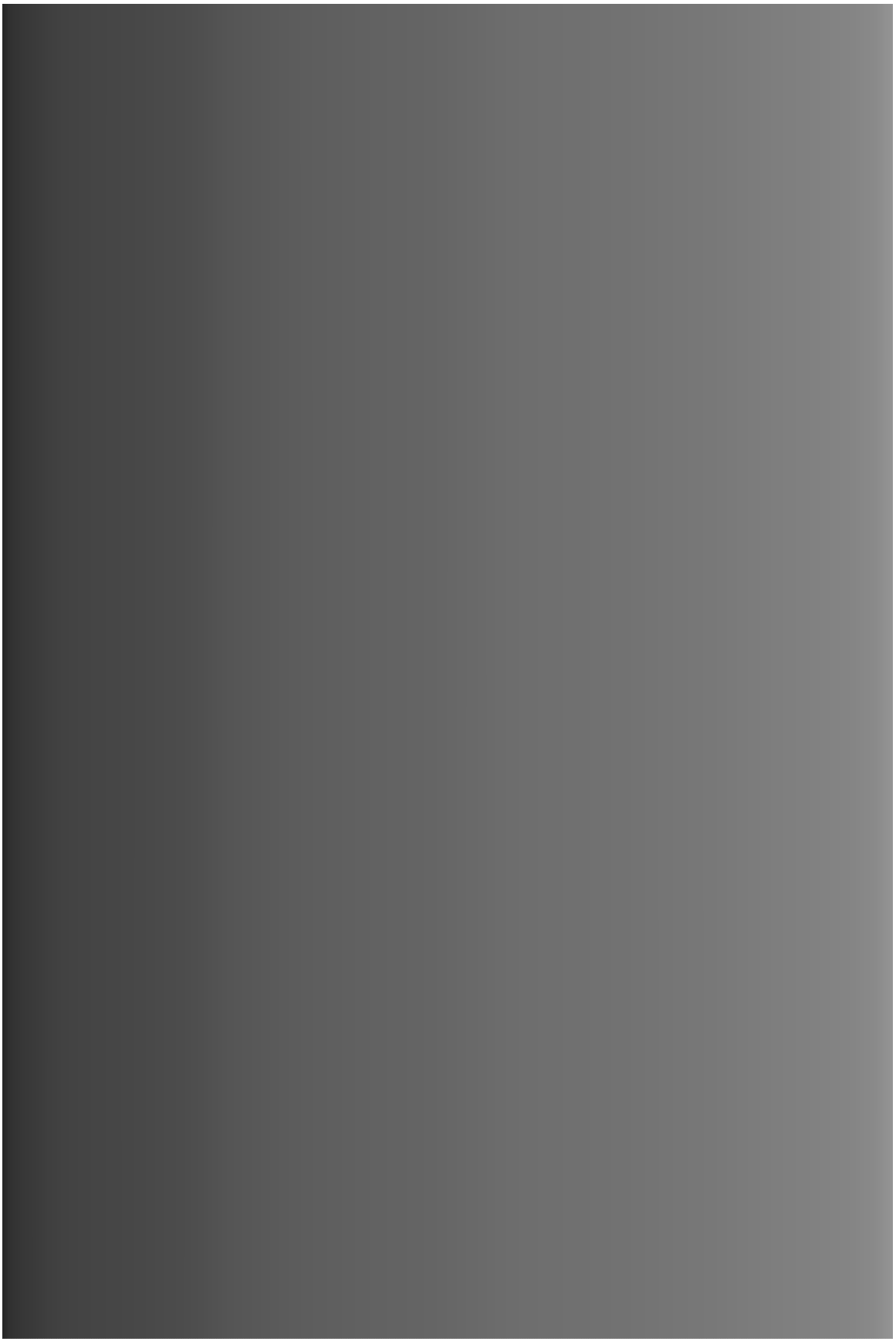

Figure 33: Sorted greyscale pixels of random walk of Figure 28 (Maple) from lowest greyscale (0, black) to highest (255, white).

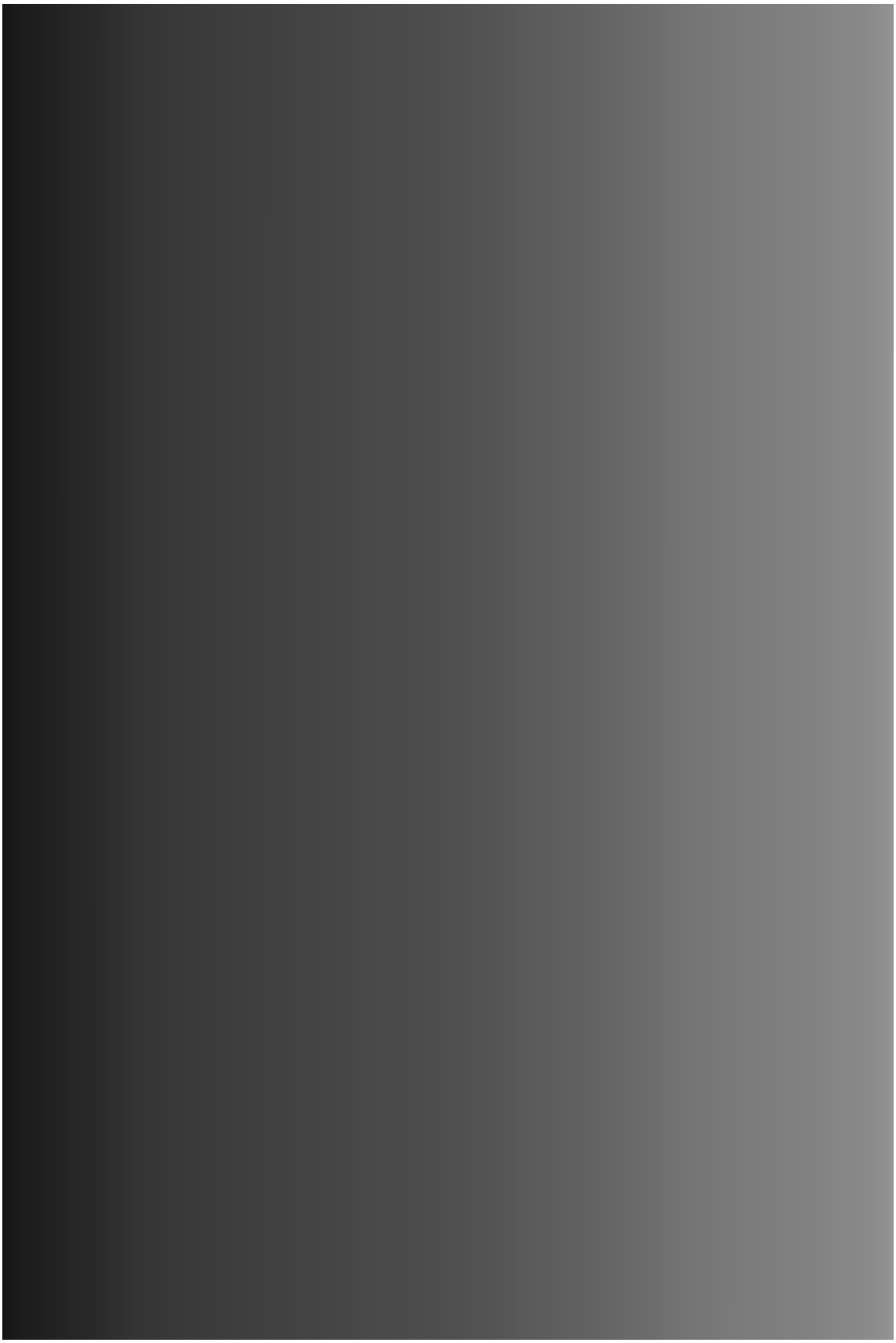

Figure 34: Sorted greyscale pixels of random walk of Figure 29 (Mathematica) from lowest greyscale (0, black) to highest (255, white).

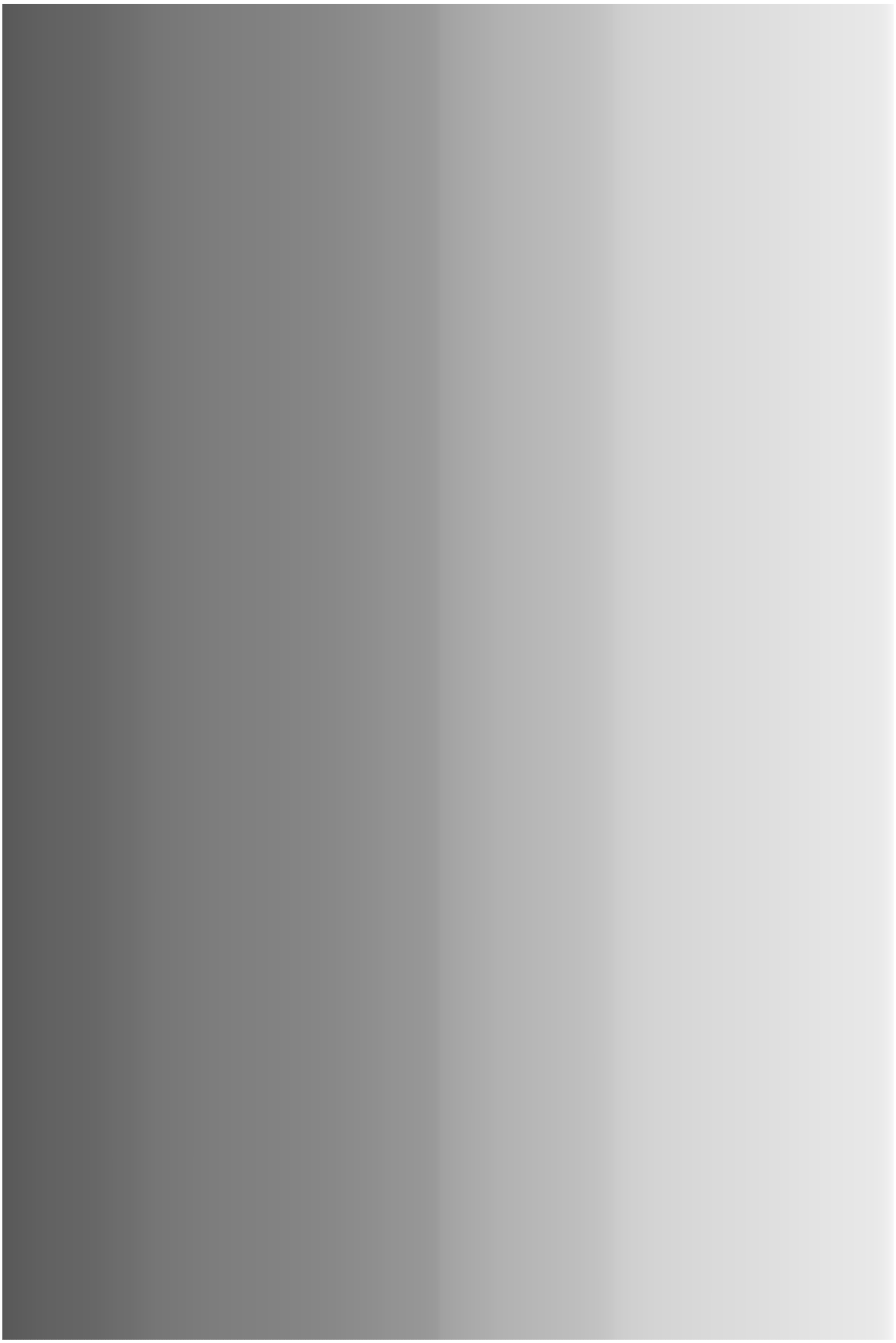

Figure 35: Sorted greyscale pixels of random walk of Figure 30 (Pi) from lowest greyscale (0, black) to highest (255, white).

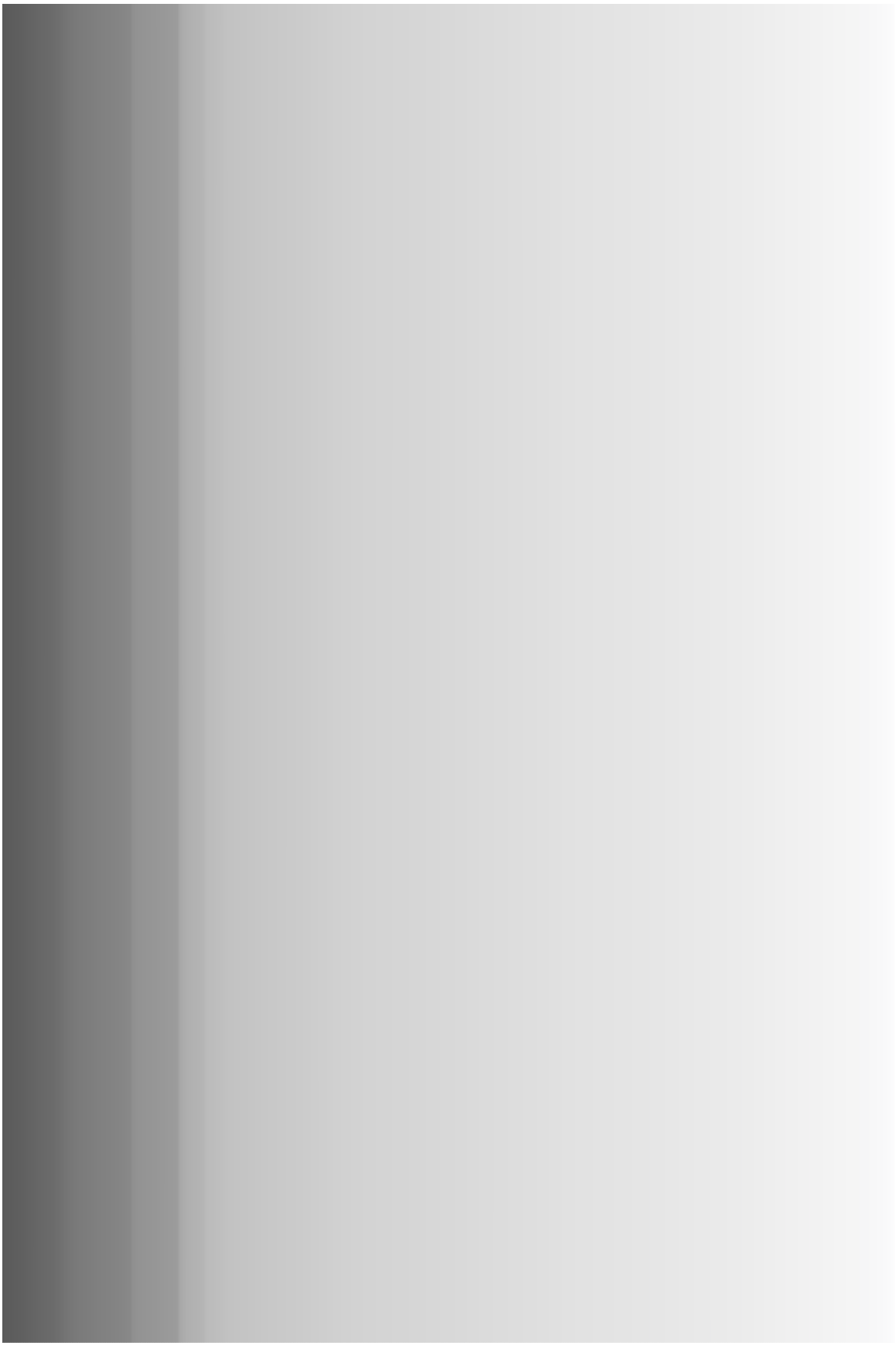

Figure 36: Sorted greyscale pixels of random walk of Figure 31 (Quantis) from lowest greyscale (0, black) to highest (255, white).

Figure 37: Sorted greyscale pixels of random walk of Figure 32 (Vienna) from lowest greyscale (0, black) to highest (255, white).

Approaching randomness through images is an endeavor with its own limitations. Initially these included the length of the string in relation to the size of the image. For example, the format in Figure 12 illustrated that significant differences could not be detected over short strings. As the size of the representable data increased, clearer differences became distinguishable, as seen in Figures 13-17. However, any meaning behind these differences remained undecipherable in these images. Figures 28–32 translated the 'magnitude' seen in the earlier, more decipherable graphic forms (Figures 1–5;7–11;18–22;23–27) to a system that registered magnitude as contrast. The random walk data shows that certain things can only be discovered about the 'workings' of quantum random numbers when each bit of a string is set in connection to the bits prior and following. These representations, though successful in many ways, held limitations of a more conceptual nature–what creates the specificity of quantum produced random strings is that each bit is not produced in 'connection' to the other bits at all. This conceptual hurdle perhaps concerns the artist more than the scientist. Figures 33–37 attempt to address this limitation not by negating it, but rather by reconfiguring it with the addition of a second system of re-ordering. This system focused on the distribution of the magnitude of the walk from the origin and displaced the relevance of the 'narrative' of the walk. This process produced information about the spread of the random walk data in relation to the origin—in the cases of pseudo randomness, smooth gradients are produced, in the cases of quantum randomness, gradients are produced with more noticeable banding.

Biographies

- C. S. Calude is a mathematician and computer scientist based at the University of Auckland working in algorithmic and quantum randomness. His webpage is `http://www.cs.auckland.ac.nz/~cristian`.
- M. J. Dinneen is a theoretical and experimental computer scientist based at the University of Auckland mainly working in combinatorial and graph algorithms. His webpage is `http://www.cs.auckland.ac.nz/~mjd`.
- A. M. Gardner is an Auckland based artist. In the past, her work has commented upon anxieties of contemporary living, mapped connections of chance, coincidence and happenstance and contested traditional relationships between performer and audience. Her practice encompasses live/performance art, photography, writing, video and here, for the first time, quantum physics, mathematics and computer science.