John Forbes Nash Jr. (1928–2015)

Camillo De Lellis, Coordinating Editor

John Forbes Nash Jr. was born in Bluefield, West Virginia, on June 13, 1928 and was named after his father, who was an electrical engineer. His mother, Margaret Virginia (née Martin), was a school teacher before her marriage, teaching English and sometimes Latin. After attending the standard schools in Bluefield, Nash entered the Carnegie Institute of Technology in Pittsburgh (now Carnegie Mellon University) with a George Westinghouse Scholarship. He spent one semester as a student of chemical engineering, switched momentarily to chemistry and finally decided to major in mathematics. After graduating in 1948 with a BS and a MS at the same time, Nash was offered a scholarship to enter as a graduate student at either Harvard or Princeton. He decided for Princeton, where in 1950 he earned a PhD degree with his celebrated work on noncooperative games, which won him the Nobel Prize in Economics thirty-four years later.

Courtesy of Martha Nash Legg and John D. Stier.

A picture of Nash taken the day of his graduation in Princeton.

In the summer of 1950 he worked at the RAND (Research and Development) Corporation, and although he went back to Princeton during the autumn of the same year, he remained a consultant and occasionally worked at RAND for the subsequent four years, as a leading expert on the Cold War conflict. He was fired from RAND in 1954 after being arrested for indecent exposure in Santa Monica, although the charges were dropped.

In 1951 he joined the mathematics faculty of MIT as a C.L.E. Moore Instructor, where he remained until his resignation in the spring of 1959. In 1951 he wrote his groundbreaking paper "Real algebraic manifolds", cf. [39], much of which was indeed conceived at the end of his graduate studies: According to his autobiographical notes, cf. [44], Nash was prepared for the possibility that the game theory work would not be regarded as acceptable as a thesis at the Princeton mathematics department. Around this time Nash met Eleanor Stier, with whom he had his first son, John David Stier, in 1953.

Courtesy of John D. Stier.

John and Alicia Nash on the day of their wedding.

After his work on real algebraic manifolds he began his deep studies on the existence of isometric embeddings of Riemannian manifolds, a fundamental and classical open problem, which Nash solved completely in his two subsequent revolutionary papers [40] and [41]. During the academic year 1956–1957 he received an Alfred P. Sloan grant and decided to spend the year as a temporary member of the Institute for Advanced Study in Princeton. It is during this period that he got interested in another classical question, the continuity of solutions to uniformly elliptic and parabolic second order equations, which would have lead to a solution of the 19th Hilbert problem. Nash published his solution [42] and learned slightly after that a different independent proof, in the case of elliptic equations, had just been given by De Giorgi [14].

During his academica sabbatical at the Institute for Advanced Study Nash married Alicia Lopez-Harrison de

Camillo De Lellis is professor of mathematics at Universität Zürich. His email address is camillo.delellis@math.uzh.ch.

For permission to reprint this article, please contact: reprint-permission@ams.org.

DOI: http://dx.doi.org/10.1090/noti1366

Lardé and shortly after, in 1958, he earned a tenured position at MIT. In the last months of 1958 and the early months of 1959 the first signs of mental disorder had become evident, while his wife was pregnant with their child, John Charles. This was the start of a long miserable period of mental illness, during which Nash still managed to produce some remarkable pieces of mathematics, such as [45], [43], [46] (published a couple of decades later) and the idea of the "Nash blow-up."

Nash and de Lardé divorced in 1962. However, after his final hospital discharge in 1970, Nash lived in the house of his former wife and the couple eventually remarried in 2003. After a long period Nash gradually recovered from his paranoid delusions, was allowed by Princeton to audit classes and finally to teach again.

After he received the Nobel Memorial Prize in Economic Sciences in 1994, jointly with John Harsanyi and Reinhard Selten, Nash's dramatic life attracted the attention of the media and was the subject of Sylvia Nasar's bestseller *A Beautiful Mind*, which inspired the 2001 movie with the same title. During this period Nash became an icon of genius in popular culture.

In 1978 he was awarded the John von Neumann Theory Prize for his discovery of the Nash Equilibria. In 1999 he received a Leroy P. Steele Prize for Seminal Contribution to Research from the American Mathematical Society and finally in 2015 he was one of the two recipients of the Abel Prize, the other one being Louis Nirenberg. On May 23, 2015, on their way back home after spending one week in Oslo on the occasion of the Abel prize ceremony, John and Alicia Nash were killed in a taxi accident on the New Jersey Turnpike.

John Milnor

About John Nash

John Forbes Nash was an amazing person, highly original, and determined to make a name for himself by attacking the most difficult and important mathematical problems.

His most widely influential work is surely the 1950 Princeton Thesis, in which he introduced what we now call a ***Nash equilibrium***. I have heard that this was described by von Neumann as "just another fixed point theorem". Whether or not this is a true quotation, this evaluation is certainly valid from the point of view of pure mathematics. However, when mathematics is applied to the real world, the important question is not whether it represents the most cutting edge mathematical techniques, but whether it tells us something meaningful about reality. The theory of two-person zero-sum games had been firmly established by the work of Zermelo, von Neumann and Morgenstern; but before Nash's work the theory of any more general form of conflict between two or more parties was a wasteland of complicated mathematics with no apparent relation to reality. Nash's ideas transformed the subject, and over the years, they have become basic and central in fields as diverse as economic theory and evolutionary biology. (See the exposition by Nachbar and Weinstein below.)

In 1952, Nash created a relation between differential and algebraic manifolds by showing that every smooth compact manifold is diffeomorphic to an essentially isolated smooth subset of some real algebraic variety. (See the exposition by Henry King below. One important application was given by Michael Artin and Barry Mazur [4] thirteen years later: For any smooth compact manifold M, they used Nash's result in proving that any smooth mapping from M to itself can be smoothly approximated by one for which the number of isolated periodic points of period n grows at most exponentially with n. For related results by V. Kaloshin, see [27].)

Nash had not forgotten about application of mathematical ideas to real world problems. A 1954 RAND Corporation memorandum described his ideas for the architecture and programing of a parallel processing computer. This was well before any such machine existed. In 1955, he wrote a letter to the National Security Agency which proposed an encypherment procedure, and explained his ideas about computational complexity and cryptography. Long before such ideas were generally known, he realized that a key criterion for secure cryptography is that the computation time for determining the key, given other information about the system, should increase exponentially with the key length. He conjectured that this criterion should be satisfied, but very hard to prove, for many possible encryption schemes. (This is perhaps an early relative of the P versus NP problem, which was posed by Stephen Cook sixteen year later, see [12].) More explicitly, Nash stated that "I cannot prove [this conjecture], nor do I expect it to be proven." His message was filed and presumably forgotten by the NSA, but declassified and released in 2012.

An amazing person, highly original, and determined to make a name for himself.

Returning to the study of smooth manifolds, the following classical statement could easily have been proved by Gauss, if he had considered such questions: *A compact surface which is smoothly embedded in 3-dimensional Euclidean space must have points of positive Gaussian curvature.* More precisely, the proof requires that the embedding should be twice continuously differentiable. A reasonable person would assume that C^2-differentiability is just a technicality, but Nash was never a reasonable person. His 1954 paper, as sharpened one year later by Nicholaas Kuiper, shows in particular that *every* compact surface with a smooth Riemannian metric can be C^1-isometrically embedded in Euclidean 3-space. Such exotic C^1-embeddings are very hard to visualize, and it is only in the last year or so that a determined French team

John Milnor is professor of mathematics at the Stony Brook University. His email address is `jack@math.stonybrook.edu`.

Courtesy of John D. Stier.

Nash and his first son John David Stier in a picture taken at Princeton in the mid-1970s.

has managed to provide computer visualizations, and even 3-D printed models, for a flat torus C^1-isometrically embedded in 3-space (see [7]).

For $k > 1$, the problem of C^k-isometric embedding of a smooth manifold in a suitable Euclidean space is less dramatic, but far more important for most applications. Its effective solution by Nash in 1956 required the invention of new and important methods in the study of partial differential equations. One step in the proof was extracted by Jürgen Moser ten years later [32], [33] and used to study periodic orbits in celestial mechanics. The resulting Nash-Moser Inverse Function Theorem is a basic tool; but is not easy to explain. (Richard Hamilton in 1982 took more than 150 pages to explain it, see [23].)

A reasonable person would assume that C^2-differentiability is just a technicality, but Nash was never a reasonable person.

Further information on Nash's Embedding Theory can be found in the article by De Lellis and Székelyhidi below. This was just the beginning of Nash's work in partial differential equations. For his 1957–1958 study of parabolic and elliptic equations, see the article by Villani below. It is hard for a nonspecialist to understand the details of this work, but it is surely notable for its originality and depth.

During these years, Nash was bouncing back and forth between the Courant Institute in New York and the Institute for Advanced Study in Princeton. He was full of ideas on every subject. At Courant he was talking about partial differential equations and fluid mechanics, for example, with Louis Nirenberg and Peter Lax. In Princeton he was talking with number theorists such as Atle Selberg about ideas towards the Riemann Hypothesis, and arguing with physicists such as Robert Oppenheimer about the foundations of quantum mechanics.

Nash's work was drastically interrupted by a breakdown in early 1959. (Many years later, he blamed his collapse on efforts to resolve the contradictions in quantum mechanics.) Whatever the cause, the next thirty years were quite miserable for Nash and for his friends, although he did manage to write a few more papers. It was a wonderful relief when he began to recover in the early 1990s. It was also wonderful that he lived to see his life's work validated, both by a Nobel Prize in Economics in 1994, and by an Abel Prize in Mathematics this May, just a few days before his untimely death.

Comments and Further References

One convenient source is *The Essential John Nash*, edited by Harold Kuhn and Sylvia Nasar, Princeton University Press, 2002. This includes biographical and autobiographical material, as well as the complete texts of a number of papers, including the following:

Real Algebraic Manifolds [39].
Parallel Control [an otherwise unpublished RAND Corporation memorandum from 1954].
The Imbedding Problem for Riemannian Manifolds [41], plus an erratum.
Continuity of Solutions of Parabolic and Elliptic Equations [42].

For Nash's letter to the NSA, see `https://www.nsa.gov/public_info/_files/nash_letters/nash_letters1.pdf`. For a discussion of Nash's cryptosystem by Ron Rivest and Adi Shamir, see `www.iacr.org/conferences/eurocrypt2012/Rump/nash.pdf`.

For video illustrating a flat torus in 3-space, see `hevea.imag.fr/Site/Hevea_images-eng.html`.

John Nachbar and Jonathan Weinstein

Nash Equilibrium

Game theory is a mathematical framework for analyzing conflict and cooperation. It was originally motivated by recreational games and gambling, but has subsequently seen application to a wide range of disciplines, including the social sciences, computer science, and evolutionary

John Nachbar is professor in economics at the Washington University in St. Louis. His email address is `nachbar@wustl.edu`.

Jonathan Weinstein is professor in economics at the Washington University in St. Louis. His email address is `j.weinstein@wustl.edu`.

For permission to reprint this article, please contact: `reprint-permission@ams.org`.

biology. Within game theory, the single most important tool has proven to be Nash equilibrium. Our objective here is to explain why John Nash's introduction of Nash equilibrium (Nash called it an "equilibrium point") in [37] and [38] caused a radical shift in game theory's research program.

We start with some terminology. A *finite strategic-form game* (henceforth simply *game*), is a triple $G = (N, S, u)$ where $N = \{1, \dots, n\}$ is a finite set of players, $S = \prod_{i \in N} S_i$, where S_i denotes the finite set of strategies available to player i, and $u = (u_1, \dots, u_n)$ where $u_i : S \to \mathbb{R}$ describes the utility achieved by player i at each *strategy profile* $s \in S$. A *mixed strategy* σ_i is a probability distribution over S_i. Players attempt to maximize their utilities, or, if facing randomness, the expected value of their utilities; we extend our notation by letting $u_i(\sigma_1, \dots, \sigma_n)$ be the expectation of u_i with respect to the independent distribution over strategy profiles induced by $(\sigma_1, \dots, \sigma_n)$.

Two-player *zero-sum* games (two-player games for which $u_1(s) + u_2(s) = 0$ for all $s \in S$) are games of pure conflict. The central result for such games was first established by von Neumann ([55]):

Theorem 1 (Minimax Theorem)**.** *For every two-player zero-sum game, there is a number V such that:*

$$V = \max_{\sigma_1} \min_{\sigma_2} u_1(\sigma_1, \sigma_2) = \min_{\sigma_2} \max_{\sigma_1} u_1(\sigma_1, \sigma_2).$$

Player 1 can thus guarantee an average utility of at least V, called the *security value* of the game, while Player 2 can guarantee that Player 1 achieves at most V, or equivalently (since the game is zero-sum) that Player 2 achieves at least $-V$. This provides a strong basis for the prediction that players will achieve average utilities of V and $-V$. Any other outcome involves some player achieving less than he or she could have guaranteed. In standard formalizations of Rock-Paper-Scissors, for example, $V = 0$, which players can guarantee by randomizing equally over "rock", "paper", and "scissors".

In game theory, the single most important tool has proven to be Nash equilibrium.

Courtesy of John D. Stier.

Nash and his second son John Charles.

At the time Nash began working on game theory, the *de facto* bible in the discipline was [56] by von Neumann and Morgenstern (hereafter VN-M). VN-M made the following proposal for how to extend the Minimax Theorem to general games, games that may combine elements of both cooperation and conflict. Given a general n-player game, construct an $(n+1)$-player zero-sum game by adding a dummy player. For each *coalition* (nonempty set of players), construct a two-player zero-sum game in which the two players are the coalition and its complement; implicitly, each coalition is assumed to cooperate perfectly within itself. The *value* of the coalition is the value V from the Minimax Theorem in the induced two-player zero-sum game. VN-M thus converted a general n-player game in strategic form into an $(n+1)$-player game in *coalition form*. For games in coalition form, VN-M proposed a solution concept now called a *stable set*, consisting of a set of payoff profiles with certain properties. Finally, VN-M proposed that for a general n-player game in strategic form, the *solution* is the set of utility profiles that correspond to elements of the stable set for the associated $(n+1)$-player game in coalition form, with the additional restriction that the solution maximize the total utility to the nondummy players.

The VN-M solution is difficult to compute for games of four or more players. When there are only two players, however, the VN-M solution is simply the set of all utility profiles such that (1) each player gets at least his security value (which is defined even in a nonzero-sum game) and (2) the sum of player utilities is maximal. We refer to such utility profiles as *efficient*.

Consider, in particular, a game of the Prisoner's Dilemma form.

	C	D
C	$4, 4$	$0, 5$
D	$5, 0$	$1, 1$

Here, player 1 is the row player and player 2 is column. If they play the strategy profile (C, D), for example, then player 1 gets 0 and player 2 gets 5. The VN-M solution for this game is the set of utility profiles such that the utilities sum to 8 and each player gets at least 1.

As an alternative to the VN-M solution, Nash ([37]) proposed what is now called a *Nash equilibrium* (NE): a NE is a strategy profile (possibly involving mixed strategies) such that each player maximizes his or her own expected utility given the profile of (mixed) strategies of the other players. The focus of NE is thus on individual, rather than collective, optimization.

The zero-sum game Rock-Paper-Scissors has a unique NE in which each player randomizes equally over "rock", "paper", and "scissors". This NE yields an expected utility profile of (0,0), which is the VN-M solution.

On the other hand, in the Prisoner's Dilemma, the unique NE is (D, D). The induced utility profile $(1, 1)$ is inefficient, hence is not an element of the VN-M solution. The Prisoner's Dilemma is the canonical example of a game in which individual incentives lead players away from collective optimality. The VN-M solution, in contrast, assumes this inefficiency away.

Nash proved:

Theorem 2 (Existence of Nash Equilibrium)**.** *For every finite game, there is a Nash Equilibrium profile* $(\sigma_1^*, \dots, \sigma_n^*)$.

As noted in [37], Theorem 2 is an almost immediate consequence of [26], which extended Brouwer's fixed point theorem to correspondences for the express purpose of aiding proofs in economics and game theory. ([38] provided an alternate proof directly from Brouwer.) In contrast, it was unknown at that time whether every finite game had a VN-M solution; [30] later provided an example of a game with no VN-M solution.

That Theorem 2 is a generalization of the Minimax Theorem can be seen by noting that Theorem 1 is equivalent to:

Theorem 3 (Minimax Theorem, Equilibrium Version)**.** *For every two-player zero-sum game, there is a pair* (σ_1^*, σ_2^*) *such that*

$$u_1(\sigma_1^*, \sigma_2^*) = \max_{\sigma_1} u_1(\sigma_1, \sigma_2^*)$$

and

$$u_2(\sigma_1^*, \sigma_2^*) = \max_{\sigma_2} u_2(\sigma_1^*, \sigma_2).$$

Thus, both the VN-M solution and NE generalize the Minimax Theorem, but along very different paths. To characterize the difference between the approaches, Nash ([38]) coined the terms *cooperative* game theory (for games in coalition form, solved by concepts such as the stable set) and *noncooperative* game theory (for games in strategic form, solved by NE and related concepts). This choice of language can be deceptive. In particular, noncooperative game theory does not rule out cooperation.

For example, a standard explanation for cooperation in the Prisoner's Dilemma is that the players interact repeatedly. But if this is the case, then the actual game isn't the Prisoner's Dilemma as written above but a more complicated game called a repeated game. If, in this repeated game, players are sufficiently patient, then there are NE that are cooperative: the players play (C, C) in every period, and this cooperation is enforced by the threat of retaliation in future periods if either player ever deviates and plays D.

As this example illustrates, noncooperative game theory requires that the analyst specify the strategic options for the players correctly: if the game is played repeatedly, or if players can negotiate, form coalitions, or make binding agreements, then all of that should be represented in the strategic form. By highlighting both individual optimization and the importance of the fine details of the strategic environment, non-cooperative game theory allows us to investigate when, or to what degree, cooperation can be sustained. Such questions could not even be posed within the research program advocated by VN-M.

Photo credit: Princeton University.

A press conference in Princeton on occasion of Nash winning the 1994 Nobel Prize. At left facing the camera is Princeton mathematician and game theorist Harold Kuhn.

Noncooperative game theory has become the dominant branch of game theory, and research on noncooperative game theory began with Nash's formulation of NE, [37] and [38]. It was appropriate, therefore, that the 1994 Sveriges Riksbank Prize in Economic Science in Memory of Alfred Nobel (the Nobel Prize in Economics), which Nash shared with two other prominent game theorists, cited Nash not only for Nash equilibrium, but also for launching noncooperative game theory as a whole.

Additional Reading

For more on game theory generally, see [17] and [48]. For motivation for, and interpretation of, NE, see [8] (introspective reasoning), [36] (learning), and [49] (evolution). For a gloss on whether NE is predictively accurate, and why testing this is not straightforward, see [29]. For connections between cooperative and noncooperative game theory (often called the Nash program), see [52]. Finally, see [35] for a more thorough history of NE. In particular, [35] discusses at length an issue that we omitted: the relationship between Nash's work and that of Cournot ([13]).

Henry C. King

Nash's Work on Algebraic Structures

I first learned of Nash's work on algebraic structures from Dick Palais who shaped my understanding of the subject. I never met Nash, but am grateful to him for the many enjoyable mathematical excursions his work made possible.

Henry C. King is professor emeritus of mathematics at the University of Maryland. His email address is hking@math.umd.edu.

For permission to reprint this article, please contact: reprint-permission@ams.org.

An m-dimensional differentiable submanifold M of $\mathbb{R}^n$ is locally given as the zeroes of $n - m$ differentiable functions f_i with linearly independent gradients. By asking that each f_i be polynomial (or a generalization now called a Nash function[1]) we get an algebraic structure on M. In [39], Nash showed that any compact differentiable manifold M has a unique algebraic structure. The meat of this result is showing existence, in particular that M has a representation as a submanifold V_0 of $\mathbb{R}^n$ locally given by polynomials f_i as above. This is what Nash calls a proper representation: There is a real algebraic set $V \subset \mathbb{R}^n$; i.e., V is the set of solutions of a collection of polynomial equations in n variables, and V_0 is a union of connected components of V. If $V = V_0$ it is called a pure representation. There is also a plain old representation (where the f_i are Nash functions), an example being the image of a polynomial embedding of a proper representation.

Here are some examples if M is the circle. The algebraic set X in $\mathbb{R}^2$ given by $x^2 + y^2 = 1$ is a pure representation of the circle. Let Y be the cubic $y^2 = x^3 - x$. The portion Y_0 of Y with $-1 \leq x \leq 0$ is a proper representation of the circle[2]. The cubic Y contains other points Y_1 with $x \geq 1$ but these are in a different connected component of Y. Now consider the image $p(Y)$ under the map

$$p(x, y) = (x - x^2(x + 1)^2/2, y).$$

Elimination theory tells us that this image is an algebraic set Z, as long as we include any real images of complex solutions[3] of $y^2 = x^3 - x$. Then $p(Y_0)$ is a representation of the circle but is not proper since $p(Y_1)$ intersects $p(Y_0)$ at $(-1, 0) = p(1, 0) = p(-1, 0)$.

Nash finds an algebraic representation of M by writing $M \subset \mathbb{R}^n$ as the zeroes of some differentiable functions, approximating these functions by polynomials, and concluding that the zeroes of the polynomials have connected components which are a slightly perturbed copy of M. Unfortunately, to make this work Nash must add some auxiliary variables and the proper representation ends up in $\mathbb{R}^{n+m}$.

Let $y(x)$ denote the closest point in M to x; then M is the zeroes of $x - y(x)$. Approximate $x - y(x)$ (and its derivatives) near M by some polynomial $u(x)$. We would not expect the zeroes of u to approximate M; after all, $u(x) = 0$ is n equations in n unknowns so we expect its solutions to have dimension 0. Let $K(x)$ be the matrix of orthogonal projection to the $n - m$ plane normal to M at $y(x)$. If we could approximate $K(x)$ by a polynomial $P(x)$ so that $P(x)$ had rank $n - m$ near M we would be in business; $\{x \mid P(x)u(x) = 0\}$ would have connected components which are a perturbed copy of M. To see this, restrict to the plane normal to M at a point p, $K(p)P(x)u(x)$ approximates the identity and thus has a unique zero near p. But $K(p)P(x)u(x) = 0$ implies $P(x)u(x) = 0$ near p, so we have a one-to-one correspondence between M and the components of $\{x \mid P(x)u(x) = 0\}$ near M. If we approximate $K(x)$ by a polynomial $L(x)$ we would not expect L to have rank $n - m$. But let $\alpha(t) = t^m + \delta_1 t^{m-1} + \cdots + \delta_m = (t - r_1)(t - r_2)\cdots(t - r_m)$ where the r_i are the eigenvalues of $L(x)$ close to 0. Then $P(x) = \alpha(L(x))$ has rank $n - m$ and $P(x) \approx K^m(x) = K(x)$. The coefficients δ_i are polynomially related to x, set to 0 the remainder of the quotient of the characteristic polynomial of $L(x)$ by α. So at the expense of adding the auxiliary variables δ_i, we can perturb M to a proper algebraic representation.

Nash's paper mentions the following questions, among others.

(1) Can every compact differentiable submanifold M of $\mathbb{R}^n$ be approximated by a proper algebraic representation in $\mathbb{R}^n$? He tried proving this without success.

(2) Can every compact differentiable submanifold M of $\mathbb{R}^n$ be approximated by a pure algebraic representation in $\mathbb{R}^n$? He speculated that this is plausible.

(3) Does every compact differentiable manifold M have a pure algebraic representation in some $\mathbb{R}^n$? He thought this was probably true.

In [57], Wallace claimed to prove conjecture 1. Unfortunately, there was a serious error (he neglected to include the real images of complex solutions in his projections). However he did prove conjecture 3 in the case where M is the boundary of a compact differentiable manifold W. Glue two copies of W together along M. By Nash, we may assume this is a component V_0 of an algebraic subset V of some $\mathbb{R}^n$. Let f be a differentiable function which is positive on one copy of W, negative on the other copy of W, zero on M, and positive on $V - V_0$. Approximate f by a polynomial p and then $V \cap p^{-1}(0)$ is a pure representation of M.

In [53], Tognoli proved conjecture 3 by greatly improving on this idea of Wallace. By work of Thom and Milnor, we know that any compact differentiable manifold M is cobordant to a nonsingular real algebraic set S; i.e., there is a compact differentiable manifold W whose boundary is $M \cup S$ where S is a pure representation of some manifold. Glue two copies of W together along their boundaries. Tognoli then does a careful version of Nash to make the result a component V_0 of a real algebraic set V so that $S \subset V$ is still a nonsingular algebraic set. Let f be a differentiable function which is positive on one copy of W, negative on the other copy of W, zero on M and S, and positive on $V - V_0$. Approximate f by a polynomial p, being careful to ensure that p still vanishes on S, and then $V \cap p^{-1}(0) = M' \cup S$ is an algebraic set with M' diffeomorphic to M. It turns out that M' is by itself an algebraic set and the conjecture is proven.

This method of Tognoli ends up being very useful and gives us a general rule of thumb: If a differentiable situation is cobordant to a real algebraic situation, then it can be perturbed to be real algebraic.

[1] *Nash functions are only needed for uniqueness; we shall ignore them here.*

[2] *The map* $(x, y) \mapsto (2x + 1,\ 2y/\sqrt{1 - x})$ *gives a Nash diffeomorphism from* Y_0 *to* X.

[3] *We'll have to include* $(2 - 2\sqrt{3}, \pm\sqrt[4]{12}) = p((-\sqrt{3} \pm \sqrt{-5})/2, \pm\sqrt[4]{12})$.

In [54], Tognoli claimed to prove conjecture 2 but the proof had serious errors detailed in [2]. This inspired Akbulut and me to prove Conjecture 1 [2] and to use the above rule of thumb [1] to reduce conjecture 2 to a cobordism statement: A compact differentiable submanifold M of $\mathbb{R}^n$ can be approximated by a pure representation if and only if there is a compact differentiable submanifold W of $\mathbb{R}^n \times [0,1]$ whose boundary is $M \times 0 \cup S \times 1$ where $S \subset \mathbb{R}^n$ is a pure representation of some manifold. The proof in [2] consists of being careful with the images of complex solutions. Nash's proof gives a nonsingular component V_0 of a real algebraic set V and a polynomial embedding $p\colon V_0 \to \mathbb{R}^n$ so that $p(V_0)$ is a perturbation of M. We alter one coordinate of p to make sure that $p(V - V_0)$ is far from $p(V_0)$ and also any real images of nonreal solutions of the polynomial equations of V lie far from $p(V_0)$. Then $p(V_0)$ is a proper representation approximating M.

Photo credit: Robert P. Matthews, Princeton University.

Camillo De Lellis and László Székelyhidi Jr.

Nash's Work on Isometric Embeddings

Nash wrote three papers on isometric embeddings of Riemannian manifolds in Euclidean space, which are landmark papers not only for the mathematical problem they solved, but more importantly because of the impact they had on other fields, encompassing applications that go well beyond differential geometry. In these papers Nash studied the following problem:

> Given a smooth compact n-dimensional Riemannian manifold M with metric g, can we find an embedding of M into some Euclidean space $\mathbb{R}^N$ which preserves the metric structure?

This was a fundamental issue, aimed at linking the notion of submanifolds of $\mathbb{R}^N$, and hence of classical surfaces, to the abstract concept arising from the pioneering work of Riemann and his contemporaries.

In the statement of the problem there are two complementary requirements on the map $u : M \to \mathbb{R}^N$:

(i) it should be a topological embedding, that is, continuous and injective;

(ii) it should be continuously differentiable and preserve the length of curves; in other words the length of any rectifiable curve $\gamma \subset M$ should agree with the length of its image $u(\gamma) \subset \mathbb{R}^N$:

$$\ell(u \circ \gamma) = \ell(\gamma) \quad \text{for all rectifiable } \gamma \subset M. \tag{1}$$

László Székelyhidi Jr. is professor of Mathematics at the Universität Leipzig. His email address is laszlo.szekelyhidi@math.uni-leipzig.de*.*

For permission to reprint this article, please contact: reprint-permission@ams.org.

In local coordinates the condition (ii) amounts to the following system of partial differential equations

$$\sum_{k=1}^{N} \partial_i u_k \partial_j u_k = g_{ij}, \quad i, j = 1 \dots n \tag{2}$$

consisting of $s_n := n(n+1)/2$ equations in N unknowns.

An important relaxation of the concept above is that of *short embedding*. A C^1 embedding $u : M \to \mathbb{R}^N$ is called *short* if it reduces (rather than preserving) the length of all curves, i.e. if (1) holds with $\leq$ replacing the equality sign. In coordinates this means that $(\partial_i u \cdot \partial_j u) \leq (g_{ij})$ in the sense of quadratic forms.

Nash realized that given a smooth embedding $u : M \to \mathbb{R}^N$, which is not necessarily isometric but it is short, one may try to solve (2) via *local perturbations* which are small in C^0, because being an embedding is a stable property with respect to a large class of such perturbations (since (2) alone guarantees that the differential of u has maximal rank, i.e. that u is an immersion). Let us assume for simplicity that $g \in C^\infty$. The three main theorems concerning the solvability of the system of partial differential equations (2) are the following:

(A) If $N \geq n+1$, then any short C^1 embedding can be uniformly approximated by isometric embeddings of class C^1 (Nash [40] proved the statement for $N \geq n+2$, Kuiper [28] extended it to $N = n+1$) .

(B) If $N \geq s_n + \max\{2n, 5\}$, then any short C^1 embedding can be uniformly approximated by isometric embeddings of class C^∞ (Nash [41] proved the *existence of isometric embeddings* for $N \geq 3s_n + 4n$; the approximation statement above was first shown by Gromov and Rokhlin for $N \geq s_n + 4n + 5$ [20]; subsequently the threshold was lowered by Gromov [19] to $N \geq s_n + 2n + 3$ and by Günther [21] to $N \geq s_n + \max\{2n, 5\}$, see also [22]).

(C) If g is real analytic and $N \geq s_n + 2n + 3$, then any short C^1 embedding can be uniformly approximated by analytic isometric embeddings (Nash [43] extended his C^∞ existence theorem to the analytic case, whereas the approximation statement was shown first by Gromov for $N \geq s_n + 3n + 5$ [18] and lowered to the threshold above [19]).

Corresponding theorems can also be proved for noncompact manifolds M, but they are more subtle (for instance the noncompact case of (C) was left in [43] as an open problem; we refer the reader to [18], [19] for more details).

Nash's papers on isometric embeddings of Riemannian manifolds in Euclidean space are landmark papers.

For M compact, any C^1 embedding of M into $\mathbb{R}^N$ can be made short after multiplying it by a sufficiently small

Photo: Berit Roald, NTB scanpix.

The award ceremony of the Abel prize, with King Harald V of Norway and Louis Nirenberg. Courtesy of The Norwegian Academy of Science and Letters.

constant. Thus, (A), (B) and (C) are not merely existence theorems: they show that the set of solutions is huge (essentially C^0-dense). Naively, this type of flexibility could be expected for high codimension as in (B) and (C), since then there are many more unknowns than equations in (2). Statement (A) on the other hand is rather striking, not just because the problem is formally over-determined in dimension $n \geq 3$, but also when compared to the classical rigidity result concerning the Weyl problem: if (S^2, g) is a compact Riemannian surface with positive Gauss curvature and $u \in C^2$ is an isometric immersion into $\mathbb{R}^3$, then u is uniquely determined up to a rigid motion [11, 24]. Notice on the other hand that if u is required merely to be Lipschitz, then condition (ii) still makes sense in the form (1) and it is not difficult to construct a large class of non-equivalent isometric embeddings of any (orientable) surface in $\mathbb{R}^3$: just think of crumpling paper!

The results (A) and (B)-(C) rely on two, rather different, iterative constructions, devised by Nash to solve the underlying set of equations (2). In order to explain the basic idea, let us write (2) in short-hand notation as

$$du \cdot du = g. \tag{3}$$

Assuming that we have an approximation u_k, i.e. such that $\varepsilon_k := \|du_k \cdot du_k - g\|_{C^0}$ is small, we wish to add a perturbation w_k so that $u_{k+1} := u_k + w_k$ is a better approximation. The quadratic structure of the problem yields the following equation for w_k:

$$[dw_k \cdot du_k + du_k \cdot dw_k] + dw_k \cdot dw_k = g - du_k \cdot du_k.$$

A basic geometric insight in both constructions is that, assuming u_k is a short embedding, the perturbation w_k should *increase* lengths and thus it makes sense to choose w_k normal to the image $u_k(M)$. This amounts to the differential condition $du_k \cdot w_k = 0$, from which one easily deduces $du_k \cdot dw_k = -d^2 u_k \cdot w_k$.

For the construction in (B)-(C) the idea is now to follow the Newton scheme: assuming that w_k and dw_k are comparable and small, $dw_k \cdot dw_k$ is much smaller than the linear term $[dw_k \cdot du_k + du_k \cdot dw_k]$, hence a good approximation can be obtained by solving for w_k the *linearization*

$$[dw_k \cdot du_k + du_k \cdot dw_k] = g - du_k \cdot du_k.$$

This can be reduced to an algebraic system for w_k by using $du_k \cdot w_k = 0$ and $du_k \cdot dw_k = -d^2 u_k \cdot w_k$. The central analytic difficulty in carrying out the iteration is that, by solving the corresponding algebraic system, estimates on w_k will depend on estimates of $d^2 u_k$ - the mathematical literature refers to this phenomenon as *loss of derivative* and Nash dealt with this by introducing an additional regularization step.

The latter obviously perturbs the estimates on how small $u_{k+1} - u_k$ is. However, Nash's key realization is that Newton-type iterations converge so fast that such loss in the regularization step does not prevent the convergence of the scheme. Regularizations are obviously easier in the C^∞ category, where for instance standard convolutions with compactly supported mollifiers are available. It is thus not surprising that the real analytic case requires a subtler argument and this is the reason why Nash dealt with it much later in the subsequent paper [43].

Nash's scheme has numerous applications in a wide range of problems in partial differential equations where a purely functional-analytic implicit function theorem fails. The first author to put Nash's ideas in the framework of an abstract implicit function theorem was J. Schwartz, cf. [51]. However the method became known as the Nash-Moser iteration shortly after Moser succeeded in developing a general framework going beyond an implicit function theorem, which he applied to a variety of problems in his fundamental papers [32], [33], in particular to the celebrated KAM theory. Several subsequent authors generalized these ideas and a thorough mathematical theory has been developed by Hamilton [23], who defined the categories of "tame Fréchet spaces" and "tame nonlinear maps."

It is rather interesting to notice that in fact neither the results in (B) nor those in (C) ultimately really needthe Nash-Moser hard implicit function theorem. In fact in case (B) Günther has shown that the perturbation w_k can be generated inverting a suitable elliptic operator and thus appealing to standard contraction arguments in Banach spaces. Case (C) can instead be reduced to the local solvability of (2) in the real analytic case (already known in the thirties, cf. [25], [9]); such reduction uses another idea of Nash on approximate decompositions of the metric g (compare to the decomposition in primitive metrics explained below).

Contrary to the iteration outlined above to handle the results in (B) and (C), in the construction used for (A) w_k and dw_k have different orders of magnitude. More precisely, if w_k is a highly oscillatory perturbation of the type

$$w_k(x) \sim \operatorname{Re}\left(\frac{a_k(x)}{\lambda_k} e^{i\lambda_k x\cdot\xi_k}\right), \tag{4}$$

then the linear term is $O(\lambda_k^{-1})$ whereas the quadratic term is $O(1)$. For the sake of our discussion, assume for the moment the following:

(*) w_k can be chosen with oscillatory structure (4) in such a way that $dw_k \cdot dw_k \sim g - du_k \cdot du_k$.

Then the amplitude of the perturbation will be $\|a_k\|_{C^0} \sim \|g - du_k \cdot du_k\|_{C^0}^{1/2}$ whereas the new error will be $\varepsilon_{k+1} = O(\lambda_k^{-1})$. Since

$$\|du_{k+1} - du_k\|_{C^0} = \|dw_k\|_{C^0} \sim \|a_k\|_{C^0},$$

the C^1 convergence of the sequence u_k is guaranteed when $\sum_k \sqrt{\varepsilon_k} < \infty$, which is easily achieved by choosing a sequence λ_k which blows up sufficiently rapidly. Furthermore, $\|u_{k+1} - u_k\|_{C^0} = O(\lambda_k^{-1})$, so that topological properties of the map u_k (e.g. being an embedding) will be easily preserved. On the other hand it is equally clear that in this way $\|u_k\|_{C^2} \to \infty$, so that the final embedding will be C^1 but not C^2.

It should be added that in fact it is not possible to achieve (*) as stated above: it is easy to check that a single oscillatory perturbation of the type (4) adds a rank-1 tensor to $du_k \cdot du_k$, modulo terms of order $O(\lambda_k^{-1})$. Nash overcame this difficulty by decomposing $g - du_k \cdot du_k$ as a sum of finitely many (symmetric and positive semidefinite) rank-1 tensors, which nowadays are called *primitive metrics*: the actual iterative step from u_k to u_{k+1} consists then in the (serial) addition of finitely many oscillatory perturbations of type (4).

Nirenberg did not hesitate to use the word 'genius'.

Nash's iteration served as a prototype for a technique developed by Gromov, called convex integration, which unraveled the connection between the Nash-Kuiper theorem and several other counterintuitive constructions in geometry, cf. [19]. In recent decades this technique has been applied to show similar phenomena (called *h*-principle statements) in many other geometric contexts. More recently, Müller and Šverak [34] discovered that a suitable modification of Gromov's ideas provides a further link between the geometric instances of the *h*-principle and several theorems with the same flavor proved in the 1980s and in the 1990s in partial differential equations. This point of view can be used to explain the existence of solutions to the Euler equations that do not preserve the kinetic energy, cf. [15]. Although the latter phenomenon was discovered only rather recently in the mathematical literature by Scheffer [50], in the theory of turbulence it was predicted already in 1949 by a famous paper of Onsager, cf. [47]. Mil

Even nowadays the Nash-Kuiper theorem defies the intuition of most scholars. In spite of the fact that Nash's iteration is constructive and indeed rather explicit, its numerical implementation has been attempted only in the last few years. After overcoming several hard computational problems, a team of French mathematicians have been able to produce its first computer-generated illustrations, cf. [7].

Photo: Eirik Furu Baardsen.

Nash at the Abel Lectures. Courtesy of the University of Oslo.

Cedric Villani

On Nash's Regularity Theory for Parabolic Equations in Divergence Form

In the fall of 1958 the *American Journal of Mathematics* published what may possibly be, to this date, the most famous article in its long history: *Continuity of solutions of elliptic and parabolic equations*, by John Nash. At twenty-four pages, this is a quite short paper by modern standards in partial differential equations; but it was solving a major open problem in the field, and was immediately considered by experts (Carleson, Nirenberg, Hörmander, to name just a few) as an extraordinary achievement. Nirenberg did not hesitate to use the word "genius" to comment on the paper; as for me, let me say that I remember very well the emotion and marvel which I felt at studying it, nearly forty years after its writing.

Here is one form of the main result in Nash's manuscript.

Theorem 4. *Let $a_{ij} = a_{ij}(x,t)$ be a $n \times n$ symmetric matrix depending on $x \in \mathbb{R}^n$ and $t \in \mathbb{R}_+$. Assume that (a_{ij}) is uniformly elliptic, that is*

$$\forall \xi \in \mathbb{R}^n, \qquad \lambda |\xi|^2 \le \sum_{ij} a_{ij}\,\xi_i\,\xi_j \le \Lambda |\xi|^2, \tag{1}$$

for some positive constants λ and Λ. Let $f = f(x,t) \ge 0$ solve the divergence form linear parabolic equation

$$\frac{\partial f}{\partial t} = \sum_j \frac{\partial}{\partial x_i}\left(a_{ij}\,\frac{\partial f}{\partial x_j}\right)$$

Cedric Villani is director of the Institute Henry Poincaré and professor of mathematics at the Université Claude Bernard Lyon 1. His email address is villani@ihp.fr.

For permission to reprint this article, please contact: reprint-permission@ams.org.

in $\mathbb{R}^n \times \mathbb{R}_+$. Then f is automatically continuous, and even C^α (Hölder-continuous) for some exponent $\alpha > 0$, when $t > 0$. The exponent α, as well as a bound on the C^α norm, can be made explicit in terms of λ, Λ, n and the (time-independent) $L^1(\mathbb{R}^n)$ norm of f.

The two key features in the assumptions of this theorem are that

(a) *no regularity assumption* of any kind is made on the diffusion matrix: the coefficients a_{ij} should just be measurable, and this is in contrast with the older classical regularity theories for parabolic equations, which required at least Hölder continuity of the coefficients;

(b) Equation (1) is in divergence form; actually, equations in nondivergence form would later be the object of a quite different theory pioneered by Krylov and Safonov.

The fact that the equation is of parabolic nature, on the other hand, is not so rigid: elliptic equations can be considered just the same, as a particular, stationary, case. Also, this theorem can be localized by classical means and considered in the geometric setting of a Riemannian manifold.

The absence of regularity assumptions on the diffusion matrix makes it possible to use this theorem to study nonlinear diffusion equations with a nonlinear dependence between the diffusion matrix and the solution itself. In this spirit, Nash hoped that these new estimates would be useful in fluid mechanics. Still, the first notable use of this theorem was the solution of Hilbert's nineteenth problem on the analyticity of minimizers of functionals with analytic integrand. Namely, consider a nonnegative minimizer for $\int L(\nabla v(x))\,dx$, with a uniformly convex analytic L: is v analytic too? Classical calculus of variations shows that $C^{1,\alpha}$ solutions are analytic; then Nash's estimate completes the proof by establishing the Hölder-continuity of ∇v. Indeed, if v is a minimizer, then for any index k, $u = \partial_k v$ solves the divergence form linear elliptic Euler–Lagrange equation $\sum_{ij} \partial_i(a_{ij}\partial_j u) = 0$, where $a_{ij} = \partial^2_{ij} L(\nabla v)$ is uniformly elliptic (this requires a few clever manipulations of mixed derivatives). Note that in this case, when we apply the theorem, absolutely nothing is known on the regularity of a_{ij}, which directly depends on the unknown function v.

Still, it is not only its contents, and this foray into Hilbert's problem, that would make this paper unique, but also the amazing set of circumstances and human passion surrounding it.

First, although a complete outsider in the field, Nash had managed to solve in just a few months the problem, which had been submitted to him by Nirenberg.

Then it was discovered by accident that De Giorgi—future icon, but completely unknown at the time—had just published an alternative solution [14], in the form of an even shorter article in a journal that was obscure (at least in comparison with the AJM). For decades to come, the coincidence of the solutions of Nash and De Giorgi would be regarded by all analysts as the example *par excellence* of simultaneous discovery.

As for his own paper, Nash, amazingly, withdrew it immediately upon its acceptance by *Acta Mathematica*, where the referee was none other than Hörmander; and he resubmitted it to the AJM, in an unsuccessful hope of winning the 1959 Bôcher Prize. Just a few months later, Nash's health would deteriorate to a point that would (among other much more tragical consequences) stop his scientific career for many years, leaving him only a couple of later opportunities for additional contributions.

In spite of all this, when I read the detailed account by Nasar [44, Chapters 30–31] or when I had the opportunity to discuss with a prime witness like Nirenberg, what most fascinated me was the genesis of the paper. (How I would have loved that the movie *A Beautiful Mind* pay proper tribute to this truly inspiring adventure, rather than choosing to forget the science and focus on the illness with such heavy pathos.)

In order to get to his goal, Nash had not developed his own tools, but rather orchestrated fragmented efforts from his best fellow analysts, combining his own intuition with the skills of specialists. A typical example is Nash's interpolation inequality

$$\int_{\mathbb{R}^n} f^2\,dx \le C(n)\left(\int_{\mathbb{R}^n} |\nabla_x f|^2\,dx\right)^{1-\theta}\left(\int_{\mathbb{R}^n} f\,dx\right)^{2\theta}, \qquad \theta = \frac{2}{n+2}. \tag{2}$$

As Nash acknowledged in the manuscript, this inequality was actually proven, on his request, by Stein; but it was Nash who understood the crucial role that it could play in the regularity theory of diffusion processes, and which has been later explored in great generality.

Another example is the jaw-dropping use of Boltzmann's entropy, $S = -\int f \log f$, completely out of context. Entropy became famous as a notion of disorder or information, mainly in statistical physics; but it certainly had nothing to do with a regularity issue. Still, Nash brilliantly used the entropy to measure the spreading of a distribution, and related this spreading to the smoothing. Again, the tool was borrowed from somebody else: I learnt from Carleson that it was him who initiated Nash to the notion of entropy. This was the start of a long tradition of using nonlinear integral functionals of the solution as an approach to regularity bounds.

One should praise Nash's informal style, intended to convey not only the proof, but also the ideas underlying it.

The next thing that one should praise is Nash's informal style, all intended to convey not only the proof, but also the ideas underlying it – or "powerful."

But then, it is also the construction of the proof which is a work of art. Nash uses a rather visual strategy, inspired by physics: think of the solution as the spreading of some quantity of heat, But then, it is also the construction of the proof which

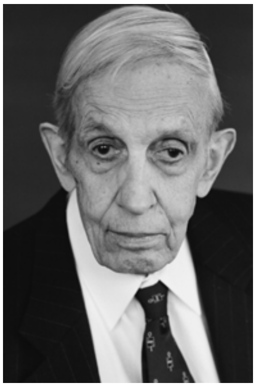


Photo: Peter Badge/Typos1—all rights reserved 2015.

and be interested in the contribution of an initial point source of heat; displacement of "sources of heat" will imply strict positivity, which in turn will imply overlapping of nearby contributions, which in turn will imply the continuity. He also uses fine tactics, in particular to find dynamical relations between appropriate "summary" quantities. As a typical start: Nash shows how the L^2 norm of the solution has to decrease immediately, which implies an unconditional bound on the maximum temperature, which in turn implies a lower bound on the entropy. Then he shows that entropy goes with spreading (high entropy implies spreading; but through diffusion, spreading increases entropy). These ideas have been quite influential, and can be found again, for instance, in the beautiful work [10] by Carlen and Loss on the 2-dimensional incompressible Navier–Stokes equation.

Various authors rewrote, simplified and pushed further the De Giorgi–Nash theory. The two most important contributors were Moser [31] and Aronson [3]. Moser introduced the versatile Moser iteration, based on the study of the time-evolution of successive powers, which simplifies the proof and avoids the explicit use of the entropy. (Entropy is a way to consider the regime $p \to 1$ in the L^p norm; a dual approach is to consider the regime $p \to \infty$ as Moser.) Moser further proved what can be called the Moser–Harnack inequality: positive solutions of an elliptic divergence equation satisfy an estimate of the form

$$\sup_{B(x,r)} f \le C \inf_{B(x,2r)} f,$$

where C only depends on r, n and the ellipticity bounds. As for Aronson, he established a Gaussian-type bound on the associated heat kernel: $p_t(x,y)$ is bounded from above and below by functions of the form

$$\frac{K}{t^{n/2}}\, e^{-B|x-y|^2/t}.$$

These three results—the Hölder continuity, the Moser–Harnack inequality, and the Gaussian type bounds—are all connected and in some sense equivalent. Fine expositions of this can be found in Bass [5] (Chapter 7), [6], and Fabes & Stroock [16]. They have also been extended to nonsmooth geometries. Actually, these techniques have been so successful that some elements of proof now look so familiar even when we are not aware of it!

To conclude this exposition, following Fabes & Stroock, here is a brief sketch of the proof of Aronson's upper bound, using Nash's original strategy. By density, we may pretend that f is smooth, so it is really about an a priori estimate. First fix $q \in (1,\infty)$ and consider the time-evolution of the power q of the solution: the divergence assumption leads to a neat dissipation formula,

$$\begin{aligned}\frac{d}{dt}\int f^q &= -q(q-1)\int \langle a\nabla f, \nabla f\rangle f^{q-2}\\ &\le -Kq(q-1)\int |\nabla f|^2 f^{q-2}.\end{aligned}$$

Using the chain-rule, we deduce

$$\frac{d}{dt}\int f^q \le -K\left(\frac{q-1}{q}\right)\int |\nabla f^{q/2}|^2.$$

Now, the Nash inequality (2) tells us that the integral on the right-hand side controls a higher power of the integral on the left-hand side: more precisely, if, say, $q \ge 2$,

$$\frac{d}{dt}\int f^q \le -K\frac{(\int f^q)^{1+\beta}}{\int f^{q/2}},$$

for some $\beta = \beta(n) > 0$. This relates the evolution of the L^q norm and the evolution of the $L^{q/2}$ norm; it implies a bound for $\|f\|_{L^q}$ in terms of t and $\|f\|_{L^{q/2}}$, which can be made explicit after some work. Iterating this bound up to infinity, we may obtain an estimate on $\|f\|_{L^p}$ as $p \to \infty$, and eventually to $\|f\|_{L^\infty}$: writing $f_0 = f(0,\cdot)$ we have

$$\|f\|_{L^\infty} \le \frac{C}{t^{n/4}}\|f_0\|_{L^2}.$$

Combining this with the dual inequality

$$\|f\|_{L^2} \le \frac{C}{t^{n/4}}\|f_0\|_{L^1}$$

(which can also be proven from Nash's inequality), we obtain

$$\|f\|_{L^\infty} \le \frac{C}{t^{n/2}}\|f_0\|_{L^1}.$$

This is the sharp L^∞ estimate in short time. Now do all the analysis again with f replaced by $f\,e^{-\alpha\cdot x}$, for some $\alpha \in \mathbb{R}^n$. Error terms will arise in the differential equations, leading to

$$\frac{d}{dt}\|f\|_{L^q} \le -\frac{K}{q}\|f\|_{L^q}^{1+\beta q/2}\|f\|_{L^{q/2}}^{-\beta q/2} + \frac{|\alpha|^2 q}{2\lambda}\|f\|_{L^q}.$$

Iteration and the study of these ordinary differential inequalities will lead to a similar bound on $f\,e^{-\alpha\cdot x}$ as on f; after some optimization this will imply the Gaussian bound.

As can be seen, the method is elementary, but beautifully arranged, and obviously flexible. Whether in the original version, or in the modern rewritings, Nash's proof is a gem; or, to use the expression of Newton, a beautiful pebble.

References

1. S. Akbulut and H. King, *Algebraicity of immersions in* $\mathbf{R}^n$, Topology **31** (1992), no. 4, 701–712. MR 1191374 (94d:57055)
2. ———, *On approximating submanifolds by algebraic sets and a solution to the Nash conjecture*, Invent. Math. **107** (1992), no. 1, 87–98. MR 1135465 (93d:57051)
3. D. G. Aronson, *Bounds for the fundamental solution of a parabolic equation*, Bull. Amer. Math. Soc. **73** (1967), 890–896. MR 0217444 (36 #534)
4. M. Artin and B. Mazur, *On periodic points*, Ann. of Math. (2) **81** (1965), 82–99. MR 0176482 (31 #754)

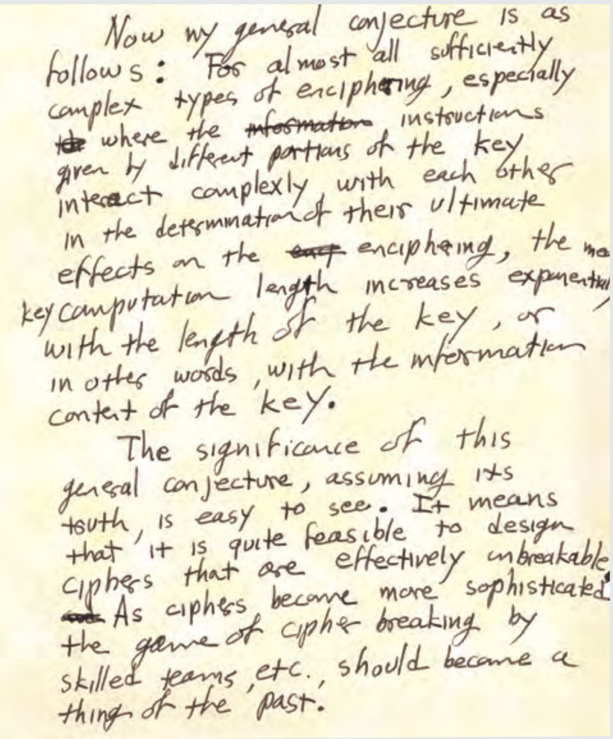
5. R. F. Bass, *Diffusions and elliptic operators*, Probability and its Applications (New York), Springer-Verlag, New York, 1998. MR 1483890 (99h:60136)
6. ———, *On Aronson's upper bounds for heat kernels*, Bull. London Math. Soc. **34** (2002), no. 4, 415–419. MR 1897420 (2003c:35054)
7. V. Borrelli, S. Jabrane, F. Lazarus, and B. Thibert, *Flat tori in three-dimensional space and convex integration*, Proc. Natl. Acad. Sci. USA **109** (2012), no. 19, 7218–7223. MR 2935570
8. A. Brandenburger, *Epistemic game theory: An overview*, The New Palgrave Dictionary of Economics, ed. Steven N. Durlauf & Lawrence E. Blume. Second Edition., Palgrave Mcmillan, 2008.
9. C. Burstin, *Ein Beitrag zum Problem der Einbettung der Riemannschen Räume in euklidischen Räumen*, Rec. Math. Moscou **38** (1931), no. 3-4, 74–85 (German).
10. E. A. Carlen and M. Loss, *Optimal smoothing and decay estimates for viscously damped conservation laws, with applications to the 2-D Navier-Stokes equation*, Duke Math. J. **81** (1995), no. 1, 135–157 (1996), A celebration of John F. Nash, Jr. MR 1381974 (96m:35199)
11. S. Cohn-Vossen, *Zwei Sätze über die Starrheit der Eiflächen*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. **1927** (1927), 125–134 (German).
12. S. A. Cook, *The complexity of theorem-proving procedures*, Proceedings of the Third Annual ACM Symposium on Theory of Computing (New York, NY, USA), STOC '71, ACM, 1971, pp. 151–158.
13. A. Cournot, *Researches into the mathematical principles of the theory of wealth*, Kelley, 1838, Translation from the French by Nathaniel T. Bacon. Translation publication date: 1960.
14. E. De Giorgi, *Sulla differenziabilità e l'analiticità delle estremali degli integrali multipli regolari*, Mem. Accad. Sci. Torino. Cl. Sci. Fis. Mat. Nat. (3) **3** (1957), 25–43. MR 0093649 (20 #172)
15. C. De Lellis and L. Székelyhidi, Jr., *Dissipative continuous Euler flows*, Invent. Math. **193** (2013), no. 2, 377–407. MR 3090182
16. E. B. Fabes and D. W. Stroock, *A new proof of Moser's parabolic Harnack inequality using the old ideas of Nash*, Arch. Rational Mech. Anal. **96** (1986), no. 4, 327–338. MR 855753 (88b:35037)
17. D. Fudenberg and J. Tirole, *Game theory*, MIT Press, Cambridge, MA, 1991. MR 1124618 (92m:90001)
18. M. L. Gromov, *Isometric imbeddings and immersions*, Dokl. Akad. Nauk SSSR **192** (1970), 1206–1209. MR 0275456 (43 #1212)
19. ———, *Partial differential relations*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 9, Springer-Verlag, Berlin, 1986. MR 864505 (90a:58201)
20. M. L. Gromov and V. A. Rohlin, *Imbeddings and immersions in Riemannian geometry*, Uspehi Mat. Nauk **25** (1970), no. 5 (155), 3–62. MR 0290390 (44 #7571)
21. M. Günther, *Zum Einbettungssatz von J. Nash*, Math. Nachr. **144** (1989), 165–187. MR 1037168 (91m:58014)
22. ———, *Isometric embeddings of Riemannian manifolds*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, pp. 1137–1143. MR 1159298 (93b:53049)
23. R. S. Hamilton, *The inverse function theorem of Nash and Moser*, Bull. Amer. Math. Soc. (N.S.) **7** (1982), no. 1, 65–222. MR 656198 (83j:58014)
24. G. Herglotz, *Über die Starrheit der Eiflächen*, Abh. Math. Sem. Univ. Hamburg **15** (1943), no. 1, 127–129. MR 3069737
25. M. Janet, *Sur la possibilité de plonger un espace riemannien donné à n dimensions dans un espace euclidien à* $\frac{n(+1)}{2}$ *dimensions.*, C. R. Acad. Sci., Paris **183** (1926), 942–943 (French).
26. S. Kakutani, *A generalization of Brouwer's fixed point theorem*, Duke Math. J. **8** (1941), 457–459. MR 0004776 (3,60c)
27. V. Yu. Kaloshin, *Generic diffeomorphisms with superexponential growth of number of periodic orbits*, Comm. Math. Phys. **211** (2000), no. 1, 253–271. MR 1757015 (2001e:37035)
28. N. H. Kuiper, *On C^1-isometric imbeddings. I, II*, Nederl. Akad. Wetensch. Proc. Ser. A. **58** (Indag. Math.) **17** (1955), 545–556, 683–689. MR 0075640 (17,782c)
29. D. Levine and J. Zheng, *The relationship of economic theory to experiments*, The Methods of Modern Experimental Economics, ed. Guillame Frechette & Andrew Schotter, Oxford University Press, 2010.
30. W. F. Lucas, *A game with no solution*, Bull. Amer. Math. Soc. **74** (1968), 237–239. MR 0220522 (36 #3581)
31. J. Moser, *On Harnack's theorem for elliptic differential equations*, Comm. Pure Appl. Math. **14** (1961), 577–591. MR 0159138 (28 #2356)
32. ———, *A rapidly convergent iteration method and non-linear differential equations. II*, Ann. Scuola Norm. Sup. Pisa (3) **20** (1966), 499–535. MR 0206461 (34 #6280)
33. ———, *A rapidly convergent iteration method and non-linear partial differential equations. I*, Ann. Scuola Norm. Sup. Pisa (3) **20** (1966), 265–315. MR 0199523 (33 #7667)
34. S. Müller and V. Šverák, *Convex integration for Lipschitz mappings and counterexamples to regularity*, Ann. of Math. (2) **157** (2003), no. 3, 715–742. MR 1983780 (2005i:35028)
35. R. Myerson, *Nash equilibrium and the history of economic theory*, Journal of Economic Literature **37** (1999), 1067–1082.
36. J. Nachbar, *Learning and evolution in games: Belief learning*, The New Palgrave Dictionary of Economics, ed. Steven N. Durlauf & Lawrence E. Blume. Second Edition, Palgrave Mcmillan, 2008.
37. J. F. Nash, Jr., *Equilibrium points in n-person games*, Proc. Nat. Acad. Sci. U. S. A. **36** (1950), 48–49. MR 0031701 (11,192c)
38. ———, *Non-cooperative games*, Ann. of Math. (2) **54** (1951), 286–295. MR 0043432 (13,261g)
39. ———, *Real algebraic manifolds*, Ann. of Math. (2) **56** (1952), 405–421. MR 0050928 (14,403b)
40. ———, *C^1 isometric imbeddings*, Ann. of Math. (2) **60** (1954), 383–396. MR 0065993 (16,515e)
41. ———, *The imbedding problem for Riemannian manifolds*, Ann. of Math. (2) **63** (1956), 20–63. MR 0075639 (17,782b)
42. ———, *Continuity of solutions of parabolic and elliptic equations*, Amer. J. Math. **80** (1958), 931–954. MR 0100158 (20 #6592)
43. ———, *Analyticity of the solutions of implicit function problems with analytic data*, Ann. of Math. (2) **84** (1966), 345–355. MR 0205266 (34 #5099)
44. ———, *The essential John Nash*, Princeton University Press, Princeton, NJ, 2002, Edited by Harold W. Kuhn and Sylvia Nasar. MR 1888522 (2002k:01044)
45. J. F. Nash, Jr., *Le problème de Cauchy pour les équations différentielles d'un fluide général*, Bull. Soc. Math. France **90** (1962), 487–497. MR 0149094 (26 #6590)
46. J. F. Nash, Jr., *Arc structure of singularities*, Duke Math. J. **81** (1995), no. 1, 31–38 (1996), A celebration of John F. Nash, Jr. MR 1381967 (98f:14011)
47. L. Onsager, *Statistical hydrodynamics*, Nuovo Cimento (9) **6** (1949), no. Supplemento, 2 (Convegno Internazionale di Meccanica Statistica), 279–287. MR 0036116 (12,60f)

48. M. J. Osborne and A. Rubinstein, *A course in game theory*, MIT Press, Cambridge, MA, 1994. MR 1301776 (95k:90002)
49. W. Sandholm, *Learning and evolution in games: An overview*, The New Palgrave Dictionary of Economics, ed. Steven N. Durlauf & Lawrence E. Blume. Second Edition., Palgrave Mcmillan, 2008.
50. V. Scheffer, *An inviscid flow with compact support in space-time*, J. Geom. Anal. **3** (1993), no. 4, 343–401. MR 1231007 (94h:35215)
51. J. Schwartz, *On Nash's implicit functional theorem*, Comm. Pure Appl. Math. **13** (1960), 509–530. MR 0114144 (22 #4971)
52. R. Serrano, *Nash program*, The New Palgrave Dictionary of Economics, ed. Steven N. Durlauf & Lawrence E. Blume. Second Edition, Palgrave Mcmillan, 2008.
53. A. Tognoli, *Su una congettura di Nash*, Ann. Scuola Norm. Sup. Pisa (3) **27** (1973), 167–185. MR 0396571 (53 #434)
54. ______, *Any compact differentiable submanifold of* $\mathbf{R}^n$ *has an algebraic approximation in* $\mathbf{R}^n$, Topology **27** (1988), no. 2, 205–210. MR 948183 (89i:14016)
55. J. v. Neumann, *Zur Theorie der Gesellschaftsspiele*, Math. Ann. **100** (1928), no. 1, 295–320. MR 1512486
56. J. von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*, Princeton University Press, Princeton, N. J., 1947, 2d ed. MR 0021298 (9,50f)
57. A. H. Wallace, *Algebraic approximation of manifolds*, Proc. London Math. Soc. (3) **7** (1957), 196–210. MR 0087205 (19,320a)

"Perhaps the best undergraduate course, the course in which I learned the most, was the junior full year course in real analysis. The teacher was John F. Nash Jr. He was brilliant, arrogant, and eccentric. At this time he was in the midst of his spectacular work on embedding theorems, nevertheless, his course was meticulously prepared and beautifully presented. The course started with an introduction to mathematical logic and set theory and covered, with great originality, the central topics of analysis culminating in the study of differential and integral equations."

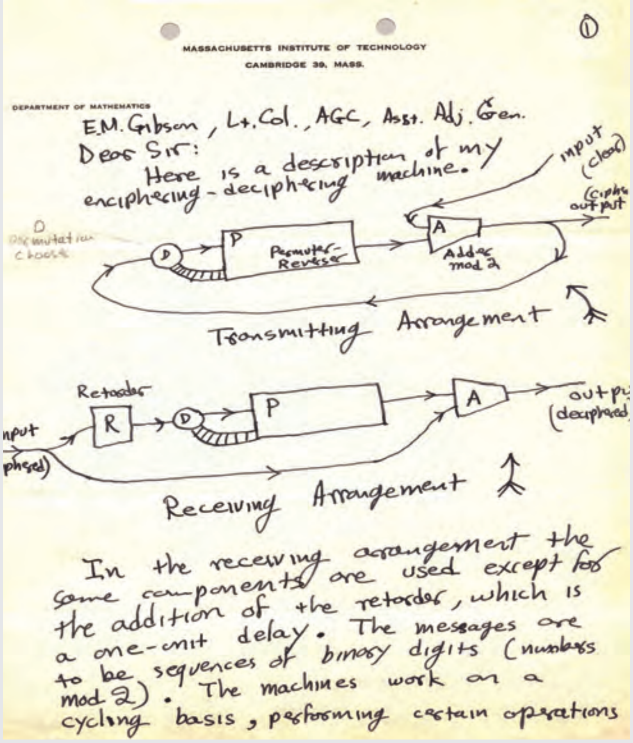
Joseph J. Kohn, "Mathematical Encounters", *All That Math*, Real Sociedad Matemática Española, 2011.

Nash and the NSA



Now my general conjecture is as follows: For almost all sufficiently complex types of enciphering, especially where the ~~information~~ instructions given by different portions of the key interact complexly with each other in the determination of their ultimate effects on the enciphering, the me key computation length increases exponentially with the length of the key, or in other words, with the information content of the key.

The significance of this general conjecture, assuming its truth, is easy to see. It means that it is quite feasible to design ciphers that are effectively unbreakable. As ciphers become more sophisticated the game of cipher breaking by skilled teams, etc., should become a thing of the past.



MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE 39, MASS.

DEPARTMENT OF MATHEMATICS

①

E.M. Gibson, Lt. Col., AGC, Asst. Adj. Gen.

Dear Sir:

Here is a description of my enciphering-deciphering machine.

input (clear)
(cipher output
D
permutation
choose
D
P
Permuter-Reverser
A
Adder mod 2
Transmitting Arrangement
Retarder
R
D
P
A
input
(ciphered)
outpu
(deciphered)
Receiving Arrangement

In the receiving arrangement the same components are used except for the addition of the retarder, which is a one-unit delay. The messages are to be sequences of binary digits (numbers mod 2). The machines work on a cycling basis, performing certain operations

At left: An excerpt from a six-page letter Nash wrote to the NSA describing a conjecture that captures the transformation to modern cryptography, which occurred two decades after he wrote this letter.
At right: Diagrams Nash drew, as part of another multi-page letter to the NSA, describing an enciphering machine he invented.
Both formerly classified letters are now available in full at `https://www.nsa.gov/public_info/_files/nash_letters/nash_letters1.pdf`.

Above are excerpts from two Nash letters that the National Security Agency (NSA) declassified and made public in 2012. In these extraordinary letters sent to the agency in 1955, Nash anticipated ideas that now pervade modern cryptography and that led to the new field of complexity theory. (In the obituary for Nash that appears in this issue of the *Notices*, page 492, John Milnor devotes a paragraph to these letters.)

Nash proposed to the NSA the idea of using computational difficulty as a basis for cryptography. He conjectured that some encryption schemes are essentially unbreakable because breaking them would be computationally too difficult. He cannot prove this conjecture, he wrote, nor does he expect it to be proved, "[but] that does not destroy its significance." As Noam Nisan wrote in a February 2012 entry in the blog Turing's Invisible Hand (`https://agtb.wordpress.com`), "[T]his is exactly the transformation to modern cryptography made two decades later by the rest of the world (at least publicly…)."

Nash also discussed in the letters the distinction between polynomial time and exponential time computations, which is the basis for complexity theory. "It is hard not to compare this letter to Gödel's famous 1956 letter to von Neumann also anticipating complexity theory (but not cryptography)," Nisan writes. "That both Nash and Gödel passed through Princeton may imply that these ideas were somehow 'in the air' there."

The handwriting and the style of Nash's letters convey a forceful personality. One can imagine that the letters might not have been taken seriously at first by the NSA. "I hope my handwriting, etc. do not give the impression that I am just a crank or a circle-squarer," Nash wrote, noting that he was an assistant professor at the Massachusetts Institute of Technology.

After receiving a reply from the NSA, Nash sent another letter describing a specific "enciphering-deciphering machine" he had developed while at the RAND Corporation. At the Eurocrypt 2012 conference, Ron Rivest and Adi Shamir presented an analysis of the actual security level of Nash's proposed machine and found it was not as strong as Nash had thought (`www.iacr.org/conferences/eurocrypt2012/Rump/nash.pdf`). Their conclusion: "John Nash foresaw in 1955 many theoretical developments which would appear in complexity theory and cryptography decades later. However, he was a much better game theorist than a cryptographer…".

—Allyn Jackson

Open Problems in Mathematics

Just before he left to collect his Abel Prize in Oslo in May 2015, Nash was working with Princeton postdoc Michael Th. Rassias to finish up the preface to an extraordinary book they edited together called *Open Problems in Mathematics*. The book will be published later this year by Springer.

The book consists of seventeen expository articles, written by outstanding researchers, on some of the central open problems in the field of mathematics today. Each article is devoted to one problem or a "constellation of related problems," the preface says. Nash and Rassias do not claim the book represents all of the most important problems in mathematics; rather, it is "a collection of beautiful mathematical questions which were chosen for a variety of reasons. Some were chosen for their undoubtable importance and applicability, others because they constitute intriguing curiosities which remain unexplained mysteries on the basis of current knowledge and techniques, and some for more emotional reasons. Additionally, the attribute of a problem having a somewhat *vintage flavor* was also influential in our decision process."

Photo Princeton University, Office of Communications, Danielle Alio (2015).

Rassias talks to 2014 Abel Laureate Yakov Sinai as 2015 Abel Laureate Nash looks on.

Here is another taste of the book, this one from the introduction, titled "John Nash: Theorems and Ideas" and written by Mikhail Gromov: "Nash was solving classical mathematical problems, difficult problems, something that nobody else was able to do, not even to imagine how to do it… But what Nash discovered in the course of his constructions of isometric embeddings is far from 'classical'—it is something that brings about a dramatic alteration of our understanding of the basic logic of analysis and differential geometry. Judging from the classical perspective, what Nash has achieved in his papers is as impossible as the story of his life… [H]is work on isometric immersions…opened a new world of mathematics that stretches in front of our eyes in yet unknown directions and still waits to be explored."

Nash and Rassias first met in September 2014 in the common room of the Princeton mathematics building, Fine Hall. Nash was eighty-six years old and probably the most famous mathematician in the world, and Rassias a twenty-seven-year-old Princeton postdoc who hails from Greece and had just finished his PhD at the ETH in Zurich. A chemistry developed between the two mathematicians and precipitated their collaboration on *Open Problems in Mathematics*. A Princeton News article that appeared on the occasion of Nash receiving the 2015 Abel Prize discussed Rassias's interactions with Nash (`www.princeton.edu/main/news/archive/S42/72/29C63/index.xml?section=topstories`). Rassias is quoted as saying: "Working with him is an astonishing experience—he thinks differently than most other mathematicians I've ever met. He's extremely brilliant and has all this experience. If you were a musician and had an opportunity to work with Beethoven and compose music with him, it'd be astonishing. It's the same thing."

Table of Contents of *Open Problems in Mathematics* edited by John F. Nash Jr. and Michael Th. Rassias