John Nash, Mathematician

26th International Game Theory Conference

Stony Brook, July 22, 2015

For correction and references see Slides 17–19.

Photo by Jay Goldman

The old Fine Hall

Photos by Lee Neuwirth


·Raffiniert·ist·der·Herr·Gott·
Aber·Boshaft·ist·Er·nicht·

Game theory in action in the old Fine Hall

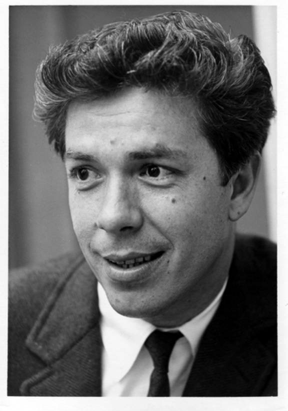
Fox, Gonshor, Milnor

Fox, Neuwirth

Photos by Jay Goldman

Game Theorists

Albert Tucker



Harold Kuhn

Although his earliest important work was in Game Theory. Nash was interested in many different kinds of mathematical problem.

He sought out the hardest problems, and was often ahead of everyone else.

In 1952, he proved that every smooth compact manifold could be given a smooth **real algebraic structure,** unique up to real analytic homeomorphism.

(Six years later, Charles Morrey published the related result that every smooth compact manifold could be given an essentially unique real analytic structure.

Hans Grauert then extended Morrey's result to paracompact manifolds.)

Parallel computation.

A 1954 RAND Corporation memorandum discusses ideas and architecture for a parallel processing computer.

This was well before any such machine existed.

1955. Letter to the National Security Agency

"...So a logical way to classify enciphering processes is by the way in which the computation length for the computation of the key increases with increasing length of the key. This is at best exponential and at worst probably at most a relatively small power of [the key length]..."

"...Now my general conjecture is as follows: for almost all sufficiently complex types of enciphering, $\cdots$ the mean key computation length increases exponentially with the length 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..."

"...The nature of this conjecture is such that I cannot prove it, even for a special type of ciphers. Nor do I expect it to be proven..."

This is an early relative of the P versus NP problem (*Stephen Cook, 1971*).

Classical Embedding Theory

If M is a Riemannian manifold, then an embedding

$$M \longrightarrow \mathbb{R}^n$$

into some Euclidean space is **isometric** if the Riemannian length of any smooth curve in M is precisely equal to the length of the image curve in $\mathbb{R}^n$.

Lemma. *Any C^2-smooth compact surface isometrically embedded in $\mathbb{R}^3$ must have at least one point with Gaussian curvature $K > 0$.*

C^1-Isometric Embedding.

Theorem (Nash 1954, Kuiper 1955). *Any distance reducing smooth embedding of a manifold into some Euclidean space can be approximated arbitrarily closely by a C^1-smooth isometric embedding.*

Example: A flat torus, obtained by identifying opposite edges of the unit square, can be C^1-isometrically embedded in 3-space.

56 years later: Borrelli, Jabrane, Lazarus, and Thibert, in Grenoble, using ideas of Misha Gromov, were able to construct concrete realizations of such embeddings.

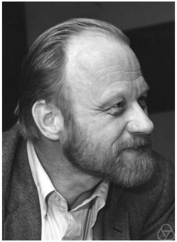
(movie-flat-torus)

C^k-Isometric Embedding.

In 1956, Nash tackled an extremely difficult problem in partial differential equations, proving that:

Any C^k-differentiable manifold with $k \geq 3$ can be C^k isometrically embedded in $\mathbb{R}^n$ for n sufficiently large.

The proof required complicated new methods, including a detailed study of calculus in Fréchet spaces, combined with carefully chosen smoothing operators. Nash noted that: "The methods used here may prove more fruitful that the results."



One step in the proof was extracted by Jürgen Moser ten years later 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 that 150 pages to explain it.)

Many Ideas ...

At this time, 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

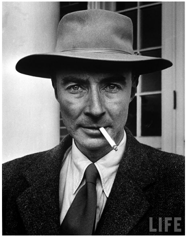
and

Peter Lax

In Princeton he was talking with number theorists about ideas towards the Riemann Hypothesis;

Atle Selberg

and arguing with physicists about the foundations of Quantum Mechanics.



Robert Oppenheimer

Collapse

It was all too much, and in early 1959 he went to pieces.

Many years later, he blamed his collapse on efforts to resolve the contradictions in Quantum Mechanics. These were:

"possibly overreaching, and psychologically destabilizing”.

Over the next few years, he managed to publish several further important papers about differential equations.

But in general the next thirty years were miserable.

It was a wonderful surprise, in the early 90’s, when he begin to recover.

Nobel Prize, 1994

Abel Prize, 2015

Further comments and references.

Nash and Morrey: In the lecture. I mistakenly stated that Morrey's result (essential uniqueness of real analytic structure on a smooth compact manifold) is an immediate corollary to Nash's result about real algebraic structure; but that is wrong. Morrey's Theorem implies that every compact real analytic manifold can be analytically embedded in some Euclidean space. (In particular, it has many globally defined real analytic functions.) But Nash considered only analytic manifolds which are already embedded in Euclidean space.

Nash and the NSA: Nash received a polite reply:

> "· · · *Although your system cannot be adopted, its presentation for appraisal and your generosity in offering it for official use are very much appreciated.* · · · "

But the NSA did file his letter, which was declassified and released in 2011. 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

`http://www.iacr.org/conferences/eurocrypt2012/Rump/nash.pdf`

Effective computation of C^1-surfaces in $\mathbb{R}^3$: The movie is available in

`http://hevea.imag.fr/Site/Hevea_images-eng.html`

For further information see:

`http://math.univ-lyon1.fr/~borrelli/Hevea/Presse/index-en.html`

`http://www.pnas.org/content/109/19/7218.full.pdf`

`http://www.emis.de/journals/em/images/pdf/em_24.pdf`

Further References

See "**The Essential John Nash**", edited by Harold Kuhn and Sylvia Nasar (Princeton U. Press 2002) for the full texts of many of Nash's papers in game theory, as well as the following:

Parallel Control

Real Algebraic Manifolds

The Imbedding Problem for Riemannian Manifolds

Continuity of Solutions of Parabolic and Elliptic Equations.

For the Nash-Moser Theorem, see R. Hamilton, *The inverse function theorem of Nash and Moser,* Bull. Amer. Math. Soc. **7** (1982), 65–222.

For my own writings about Nash, see *A Nobel Prize for John Nash*, Math. Intelligencer **17** (1995) 11–17; as well as *John Nash and "A Beautiful Mind",* Notices Amer. Math. Soc. **45** (1998) 1329–1332.

John Milnor, 7-29-2015