"NP ≠ NP ∩ coNP = P"

a nostalgic talk to celebrate the mathematical

Alan J. Hoffman.

At an Alan Hoffman Fest,
Rutgers University, September 19-20, 2014.

by Jack Edmonds
<jack.n2m2m6@gmail.com>
with help from Dominik Scheder,
Laura Sanita, Vlad Gurvich,
Bernhard von Stengel,
Kathie Cameron, and Xiaotie Deng.

I am deeply honored to be able speak here of the many ways in which Alan's influence and friendship have been important to me.

1) Alan is the founder of "polyhedral combinatorics",
   my favorite subject.
2) His linear programming understandings of discrete math were,
   along with the TSP work of Dantzig, Fulkerson, and Johnson,
   the main inspiration for my own math research.
3) Alan set the tone of math research at the National Institutes of
   Science and Technology which enabled my work there.
4) In my mathematical epiphany in 1961 at the RAND Corporation,
   Alan was my main mentor and supporter.
5) Alan has been a gracious rival. He became my kite-flying friend.

6) We share old memories.

I tried to get rich so I could be a student forever.

As a student I was an investigative reporter, wrote and directed plays, studied arts and sciences, very little math. I ran errands and proofed tv schedules at the Washington Post newspaper.

I was too slow to become a journalist, and so in 1958, I chose grad school in math, the easiest subject with the longest turn-around time.

I loved math but was a poor student, and disliked the ways of academia.

Dropped out in 1960 to support a wife and kids.

I was born 1934, Washington, D.C., the perfect time and place,

into a family who had always worked with stone and wood.

Looking for work in 1960,

I lucked on to Alan Hoffman's footsteps at **NBS**, now **NIST**.

Reading Hoffman, Berge, plus some negatively inspiring 'algorithms',

I discovered P, NP, and conjectured the thrilling "**NP ∩ coNP = P"** .

I presumed that **"NP ≠ NP ∩ coNP"** was easy and at that time

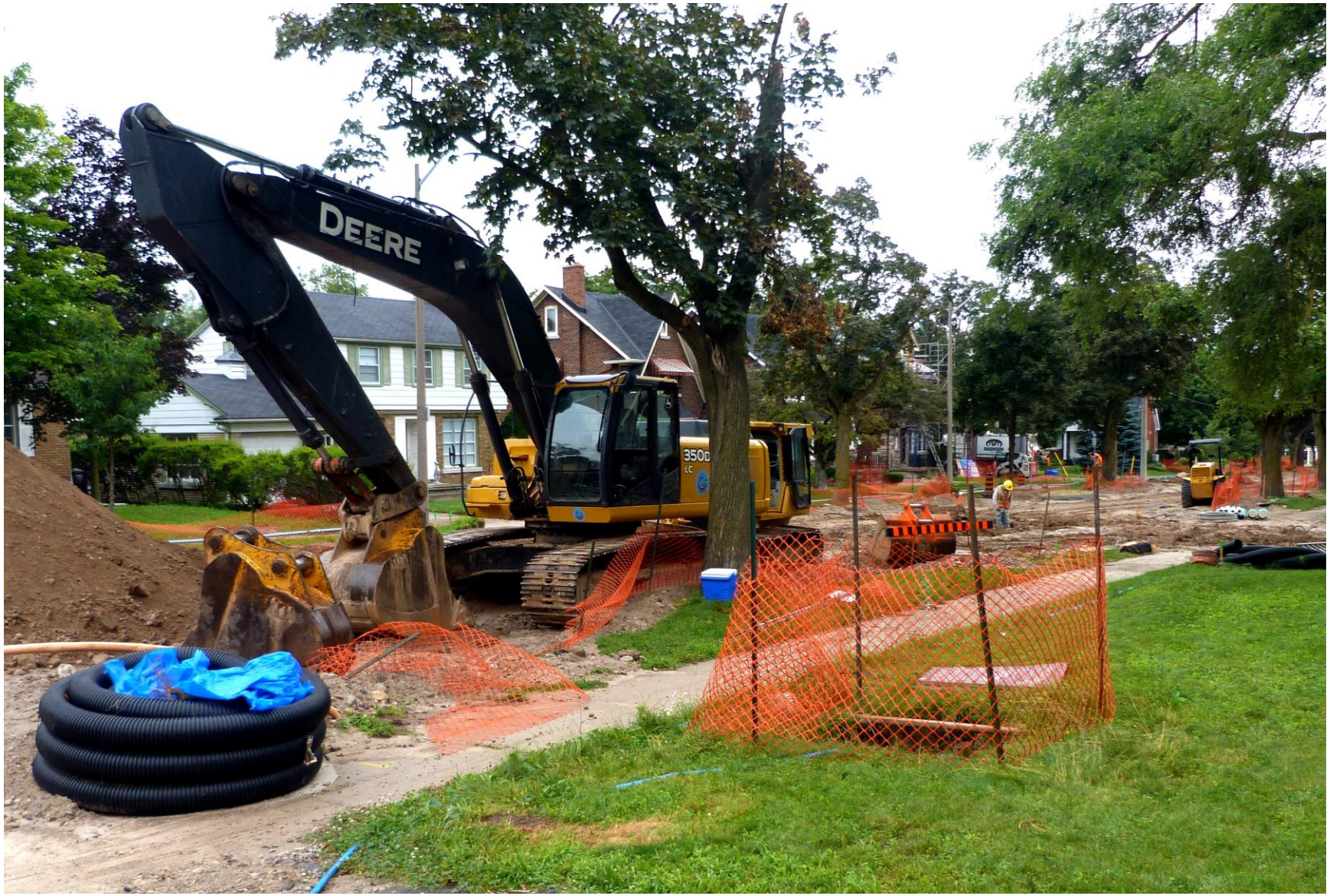
not thrilling to anyone. I had a silly theorem which generalized Berge's

matching augmenting paths to independent-vertex-set augmenting trees.

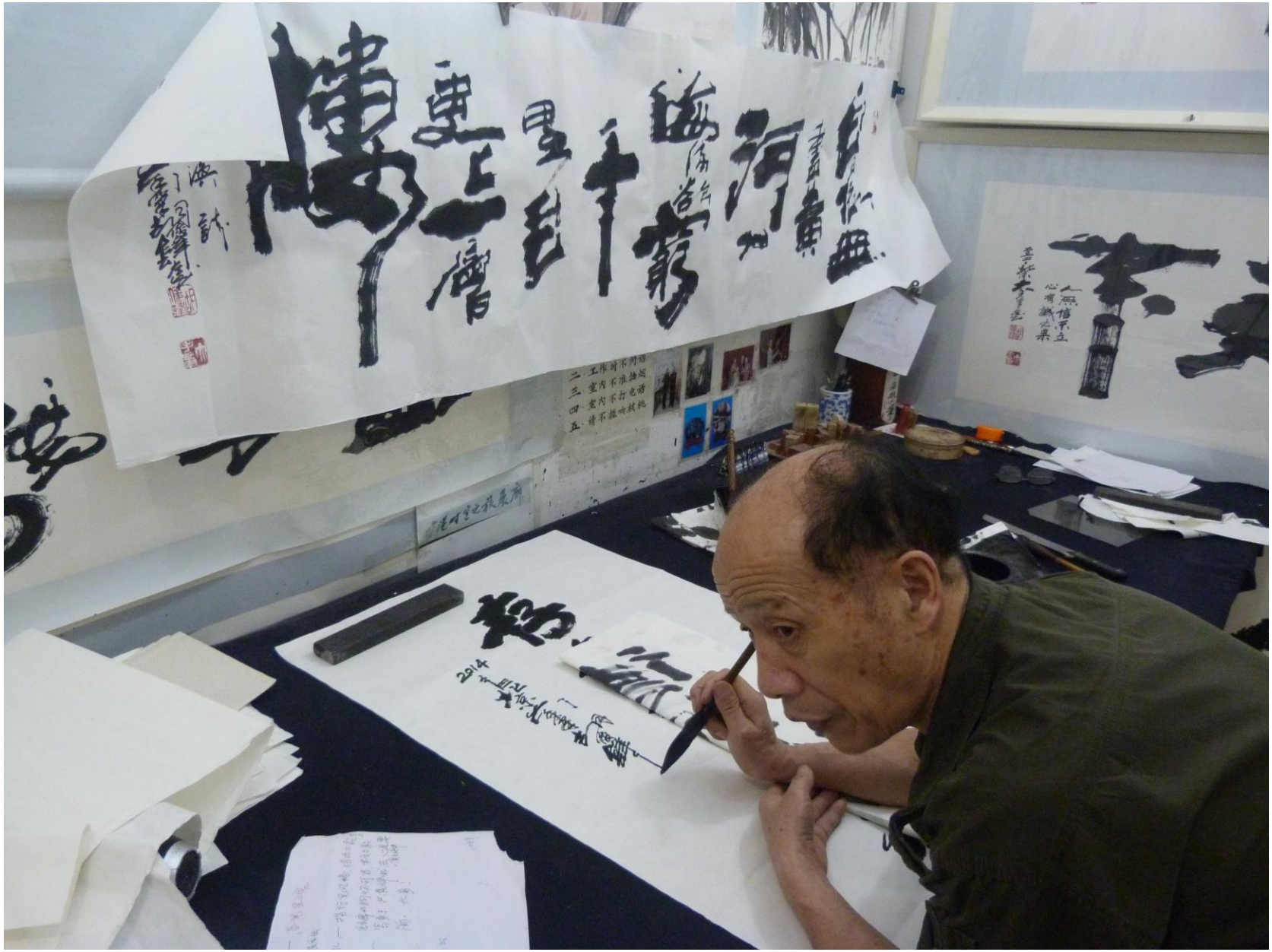
Jiao Tong University, Shanghai

O


NP≠NP∩coNP=P


DEERE
350D
LC


NP≠NP∩coNP=P




售書法教材


U.S. ARMY

Before reading Alan Hoffman on the subject
I was mystified by treatments like Halmos and Vaughn of the
The Marriage Theorem:
Given a set of girls, a set of boys,
and the set of pairs, (i, j), such that boy, i, loves girl, j.

The traditional way to say the marriage theorem is:
The girls can all marry distinct boys who love them
If and only if, for every subset S of the girls,
the size of S ≤ the number of boys who love someone in S.

Are we to see if the girls can all marry by looking at every subset of the girls?
The Halmos-Vaughn proof seems to confirm that the question is exponentially difficult.

The NP∩coNP way to say the theorem begs us to prove it by a polytime algorithm:

Either there is a way for all the girls
to marry distinct boys who love them,
or else there is a subset S of the girls which is bigger than
the subset of boys who love someone in S. (Not both).

In fact, a simple algorithm proves the more general “Konig Formula”,

Max size of a matching in a bipartite graph G

= Min size of a set of the nodes which ‘cover’ all the edges of G.

At the general step of the algorithm you have some matching M in G.

If some node v isn’t hit by M you grow from v an ‘alternating tree’ T.

That leads to either an M augmenting path

or else a covering by the ‘inner nodes’ of T

of all the edges which hit any node in T.

This does not work unless G is bipartite.

Hoffman’s writings (1956) taught me the idea of representing a set of

‘combinatorially interesting substructures’ by a set V of 0,1 vectors, and

then using a set L of linear inequalities such that x(L), the solution set of L, is conv(V), the convex hull of V. Together with the linear programming duality theory, this gives combinatorial optimization and feasibility results.

Using total unimodularity, Alan studied structures where L can be explicitly listed.

Dantzig, Fulkerson, and Johnson (1956) solved an instance of the traveling salesman problem by regarding V as the set of possible tours in a graph and by taking L to be $\mathbf{0} \leq x \leq \mathbf{1}$ and

subtour elimination inequalities: For every proper subset S of nodes (i.e., cities), the sum of the variables indexed by edges leaving S is ≥ 2.

In general, this L describes a polytope whose vertex-set includes the tours, but also includes fractional vertices.

The then new idea: if a set V of points has a nice (i.e., NP) description and a set L of linear inequalities has a nice (i.e., NP) description, and the solution-set x(L) of L is the convex hull, conv(V), of V, then using the lp duality theorem, for any linear objective, cx, we have a **"good (i.e., NP ∩ coNP) characterization"** of existence and optimality.

It seems reasonable that if V is NP then there ought to be an L that is NP and describes the hull of V. If we can discover such an L we ought to be able to prove it by a polytime algorithm. I became obsessed without knowing any interesting examples. I hoped that V as the set of TSP tours would be an example, thus solving the Traveling Salesman Problem.

I would like to stress that NP∩coNP theorems – that is, good characterizations, and more generally Existentially Polytime (EP) theorems, are in themselves more important to mathematics than P is. They are not merely of interest as evidence for the existence of polytime algorithms. In fact I believe that EP is a formalization of what mathematicians most often informally regard as beautiful.

My chief, Alan Goldman, persuaded his PhD chief, Prof. Al Tucker at Princeton, to invite me to be a novice participant in a summer-long workshop on combinatorics at the RAND Corporation in Santa Monica, 1961.

Every combinatorial big shot was there.

The day before it was my turn to lecture, I still didn't have an example of my NP∩coNP philosophy though I had settled on the "b-matchings" in a graph as V and, as the L, hopefully inequalities (1) $x \geq 0$;

(2) for every node, u, [the sum of x indexed by edges hitting u] ≤ b_u ; and

(3) for every subset S of nodes such that $\sum(b_u : u \text{ in } S)$ is odd,

$\sum[x_j : \text{edge } j \text{ has both ends in } S] \leq [-1 + \sum(b_u : u \text{ in } S)] / 2$.

All I actually had was the inadequate "augmenting tree theorem" and a speech about **NP∩coNP**. Suddenly my officemates, Balinski and Witzgall, heard me shout something like **"Eureka! You shrink!".**

With b = all 1s, and the linear objective function cx with c = all 1s,

and with “total dual integrality”, lp duality applied to these inequalities gives a

“Konig-type min-max formula”

for the max cardinality of a matching in a non-bipartite graph, G,

which is much more transparent then the one already given by Berge.

Say that a single node ‘covers with weight 1’ all the edges which hit it, and that

any set S of nodes of size 2k+1 ‘covers with weight k’ edges with both ends in S.

Then Max size of a matching in G = Min weight of a covering of all edges of G.

“Eureka! You Shrink!” meant that I had just figured out

‘the blossom algorithm’ which proves that formula, and so presumably

the preceding L does give the convex hull of the b-matchings. (It does.)

My talk next morning to the high priests was a sensation. There was heckling. Alan Hoffman defended me. Some question prompted me to say “Perhaps only Prof.Tutte and God know”. Alan said “Could one of the cited authorities comment?”

I accepted Professor Tucker’s invitation to be a Research Associate at Princeton and take charge of the Combinatorics and Games Seminar. And so I was on the slippery slope of academia. I at least declined his urging to get a PhD. (Recall that the 1960s was the beginning of great liberation movements. I was trying to liberate academia, mathematics, and computing theory.)

Thirty years later while I was teaching courses on *Oriented Matroids* and *Submodular Functions* at Stanford, pregnant Kathie and I noticed that the lovely Secretary was in love with Alan. When we invited him to bring her to dinner he brought CS Professor Gene Golub instead.

I feel simply extraordinarily lucky to be cited for introducing P. The book *Complexity Theory* by Arora and Barak even gives a long quote of my proselytizing in *Paths, Trees, and Flowers*, 1965. Here are some parts of it.

I am claiming, as a mathematical result, the existence of a *good* algorithm for finding a maximum cardinality matching in a graph.

There is an obvious finite algorithm, but that algorithm increases in difficulty exponentially with the size of the graph. It is by no means obvious whether *or not* there exists an algorithm whose difficulty increases only algebraically with the size of the graph.

we may use something like Church's thesis in logic. Then, it is possible to ask: Does there or does there not exist an algorithm of given order of difficulty for a given class of problems?

One can find many classes of problems, besides maximum matching and its generalizations, which have algorithms of exponential order but seemingly none better. An example known to organic chemists is that of deciding whether two given graphs are isomorphic. For practical purposes the difference between algebraic and exponential order is often more crucial than the difference between finite and non-finite.

There is an extensive combinatorial-linear theory related on the one hand to matchings in bipartite graphs and on the other hand to linear programming. It is surveyed, from different viewpoints, by Ford and Fulkerson in **(5)** and by A. J. Hoffman in **(6)**. They mention the problem of extending this relationship to non-bipartite graphs. Section 5 does this, or at least begins to do it. There, the König theorem is generalized to a matching-duality theorem for arbitrary graphs. This theorem immediately suggests a polyhedron which in a subsequent paper **(4)** is shown to be the convex hull of the vectors associated with the matchings in a graph.

Maximum matching in non-bipartite graphs is at present unusual among combinatorial extremum problems in that it is very tractable and yet not of the "unimodular" type described in **(5** and **6)**.

In paper **(4)**, the algorithm is extended from maximizing the cardinality of a matching to maximizing for matchings the sum of weights attached to the edges. At another time, the algorithm will be extended from a capacity of one edge at each vertex to a capacity of d_i edges at vertex v_i.

This paper is based on investigations begun with G. B. Dantzig while at the RAND Combinatorial Symposium during the summer of 1961. I am indebted to many people, at the Symposium and at the National Bureau of Standards, who have taken an interest in the matching problem. There has been much animated discussion on possible versions of an algorithm.

My proselytizing about NP ∩ coNP is more interesting:

We seek a good characterization of the minimum number of independent sets into which the columns of a matrix of Π can be partitioned. As the criterion of "good" for the characterization we apply the "principle of the absolute supervisor." The good characterization will describe certain information about the matrix which the supervisor can require his assistant to search out along with a minimum partition and which the supervisor can then use "with ease" to verify with mathematical certainty that the partition is indeed minimum. Having a good characterization does not mean necessarily that there is a good algorithm. The assistant might have to kill himself with work to find the information and the partition.

Theorem 1 on partitioning matroids provides the good characterization in the case of matrices of Π. The proof of the theorem provides a good algorithm in the case of matrices of Π. (We will not elaborate on how.) The theorem and the algorithm apply as well to all matroids via the matroid axioms. However, the "goodness" depends on having a good algorithm for recognizing independence.

From *Minimum Partition of a Matroid into Independent Sets, J. Res. NBS, 1965.*

Let us mean by a ***good polyhedron characterization*** **(GP):**
an NP∩coNP characterization which is based on lp duality
applied to an NP set V of points and an NP set L of linear inequalities
such that all of V satisfies L and 'the vertices' of L are all in V. (Long ago
I tried to convince Vasek that this should be the meaning of 'Edmonds polyhedron'.)
After the RAND debut I did manage to find some more nice classes of GPs,
in particular based on matroids and submodularity. However in a serious search
for a GP where V is the set of vectors of tours (Hamiltonian cycles) in a graph, I failed.
E.g., adding to subtour elimination, 0,1 b-matching inequalities, or tree inequalities,
still produces fractional vertices. In frustration I conjectured P ≠ NP,
in an obviously equivalent form which anyone can more easily appreciate:

I conjecture that there is no good algorithm for the traveling salesman problem.
My reasons are the same as for any mathematical conjecture:
(1) It is a legitimate mathematical possibility, and (2) I do not know.
(Optimum Branchings, J.Res.NBS, 1967)

I hope that discovery of classes of GP has not been completely buried by
NP completeness. Surely there are more GPs out there.

In 1970, nine years after my RAND epiphany I'm afraid I didn't resist leaving NBS in Washington, D.C., to start as a full professor with tenure without PhD at the Canadian University of Waterloo. It has a Faculty of Math with 5 departments including the then innovative Dept.of C&O first led by a visionary Gerry Berman who is now totally forgotten by UW, like me and other less than model teachers.

I had great students including Peyton Young, Bill Pulleyblank, Vasek Chvatel, Bill Cook, Gilberto Calvillo, Rick Giles, Komei Fukuda, Anna Lubiw, Kathie Cameron, Arnaldo Mandel, and many others. The stupid Department declined to hire my guest, Haken, who then promptly proved the 4 color conjecture, and also declined to hire my post-doc, Paul Seymour, who then went to Ohio State to do the Graph Minor Project.

There are many theorems giving coNP descriptions of Alan's totally unimodular matrices (regular matroids), besides the definition. My favorite problem was to get an NP description. I was thrilled when post-doc Paul Seymour did that.

We loved the rock music of the day. Laci Lovasz didn't. We had great fun.

In 1982 I taught courses in combinatorial optimization at Cornell
where Jon Lee and Walter Morris were among my star pupils.

I went directly from there to Beijing and Shanghai where I gave courses to
the first grad students after the cultural revolution.

Everyone in China wore a dark blue Mao jacket, drove a black bicycle,
and was part of a one-room family. Except for my full-time driver,
there were almost no cars. The pollution then was from the coal heating.
Jazz and rock were forbidden – I explained how they were even better than matroids.
The students were using my slowness to improve their English.
Almost all of them then studied abroad – several at U. of Waterloo.
I encouraged my favorite, Xiaotie Deng, to move on to study with Christos.

.In the 70s at U. of Waterloo, I didn't learn of NP completeness until Knuth conducted a poll to name it, and even then I didn't make sense of ***non-deterministic*** Turing machines.

I was heartbroken not to be included in *Complexity of Computer Computations*, 1972.

Eventually I saw that the Cook-Levin NP completeness is easy to prove

by using (1) the definition I knew of an NP predicate, g(x),

as g(x) = **[** there exists a polysize y such that f(x,y)] where f is in P;

(2) that a Turing machine for fixed size input (x,y) is a polynomial size Boolean circuit;

and (3) that Boolean circuit satisfiability reduces to cnf satisfiability.

B reduces to A means there is way to get a polytime algorithm for B by using a polytime algorithm for A. We can also then say that A is B hard. Of course many problems are solved by reductions. The Chinese Postman problem can be reduced to the shortest problem and the 1-matching problem. The b-matching problem is polytime solved by reducing it to the optimum flow problem and the 1-matching problem.

There has been great success in using the conjecture NP∩coNP = P as a template for special cases. The conjecture prompted my GP math, as well as famous successes like linear programming and PRIME (deciding whether a number is prime). Still there are some NP ∩ coNP theorems for which good deterministic algorithms are not known.

Anne Condon wrote in 1992: "Although many number theoretic problems not known to be in P lie in the class NP∩coNP, combinatorial problems that lie between P and NP∩coNP are rare." Then she goes on to describe a good candidate: Simple Stochastic Games.

[AM09] Daniel Andersson and Peter Bro Miltersen. The complexity of solving stochastic games on graphs. In Yingfei Dong, Ding-Zhu Du, and Oscar H. Ibarra, editors, Algorithms and Computation, 20th International Symposium, ISAAC 2009, Honolulu, Hawaii, USA, December 16-18, 2009. Proceedings, volume 5878 of Lecture Notes in Computer Science.

[Con92] Anne Condon. The complexity of stochastic games. Information and Computation, 96:203{224, 1992.

PRIME being in P, which Condon did not know, puts Integer Factorization into NP ∩ coNP.

Cryptographers would hate Integer Factorization being in P,
even though it already is with quantum computing.

The simplest example of a problem in NP∩coNP conjectured not to be in P might be Integer Factorization.
To be concrete, let us define the following decision version of factorization:

Given two natural numbers n and k,
decide whether there is a prime factor p of n with $p \leq k$.

If this task was in P, then one could use binary search
to find the smallest prime factor of n efficiently;
thus factoring n in polynomial time.

On the other hand, the above problem is in NP∩coNP:
The witness for both Yes-instances and No-instances
is just the integer factorization of n itself.

Indeed, given numbers $p_1,\ldots,p_t$, it is easy to check that

(i) Their product is n, and
(ii) They are all prime, since Primes is in P.
(iii) Finally, one can check whether $\min \{ p_1,\ldots,p_t \} \leq k$.

So the above problem is in NP∩coNP.

By the same token, if a computational task always has a unique solution and a solution is efficiently verifiable, then one can cook up a NP∩coNP problem by simply asking for the k^{th} bit of the solution.
In this way, every bijective one-way function
would give a decision problem in (NP∩coNP) – P.

Maybe I should hedge my bet by
weakening the conjecture NP∩coNP = P to
"GP, i.e., good polyhedral characterization, is in P",
since these have been my only successes
(and we don't want to threaten national security).

Could we show that NP∩coNP reduces to GP?
Might we more modestly show that Integer Factorization reduces to GP?
That would be a lovely GP, regardless of whether it is in P.

An existentially polytime (EP) theorem means a theorem of the form
"For any x, there is a polynomial size y such that f(x,y)",
where f(x,y) is in P,
Most of the revered theorems of combinatorics are EP.

Example. Dirac's Thm: In any graph G, there is a Hamilton cycle in G
or a node joined to fewer than half the other nodes.

Of course NP∩coNP theorems are EP.
Most EP theorems seem to have polytime algorithms for finding a y,
such as "derandomization" for EP theorems
which are proved by inequality-type counting.

However Papadimitriou has famously identified 2 classes of beautiful EP
theorems based on parity which have beautiful algorithmic proofs
(that there is a y) but seem not to have polytime algorithms:
PPA theorems and PPAD theorems.

Chen and Deng have famously shown that 2NASH,
i.e., finding a 2-person Nash equilibrium, is PPAD complete.

By reducing from 2NASH, Vlad Gurvich and I have shown that
Polytopal Sperner is PPAD complete.

"Manifold Sperner" Theorem. For any simplicial (pseudo) d-manifold M,
and any coloring of the vertices of M with d+1 colors,
and any chosen one of the colors,
there is a natural pairing of the rainbow rooms.

A simplicial (pseudo) d-manifold M means a finite set V of vertices
and a set R of size d+1 subsets of V, called the rooms,
such that each size d subset of a room, called a wall, is a wall of exactly 2 rooms.
A room is rainbow means that it has one vertex of each color.

The associated search problem is to find the brother of a given rainbow room.

Polytopal Sperner is where the d-manifold M is the simplicial polytope boundary
of the convex hull of a set V of points in general position in d+1 space.

There many beautiful, and apparently algorithmically exponential, PPA theorems, but currently no known PPA search problem which does not use abstract Boolean circuits.

Zeying Xu, Xiaotie Deng, and I, are working on showing a non-oriented geometrical Sperner to be PPA complete.

Here is another nice EP theorem:
Any graph G has either
an induced odd hole, an induced odd anti-hole,
or a clique and a proper node-coloring the same size.

An odd hole is a simple polygon with no chords and
the number of its nodes odd and greater than 3.
An odd anti-hole is the complementary graph of an odd hole.

There should be a good direct algorithm which proves the theorem
by finding in any graph an instance of what is said to exist.

Many years ago, with any NP obstruction to perfection
possibly substituting for odd holes and anti-holes,
I called this The SIAM Perfect Graph Problem.

The problem has at least a very long indirect solution
by putting together three different long works.

Thank you for listening.