林正人君の第 12 回日本学術振興会賞および第 12 回日本学士院学術奨励賞受賞を祝して

四日市大学関孝和数学研究所
上野　健爾

林正人君が「有限符号長の情報理論及び量子情報理論の研究」によって 2015 年度の第 12 回日本学術振興会賞およびを第 12 回日本学士院学術奨励賞を受賞された．日本学術振興会賞は, 優れた研究成果をあげ, 今後の活躍 が期待される若手研究者に対して与えられる賞であり，その受賞者の中から, 我が国の学術の発展に特に寄与することが期待される研究者に送られるものが日本学士院学術奨励賞である．名ばかりではあったが，元指導教官として林正人君に心からお祝いの言葉を贈りたい．

林正人君は 1994 年に京都大学理学部卒業後，同年 4 月に京都大学研究科数学専攻の修士課程に入学した．学部時代は物理学と数学の両方を主として勉強をしており，そのこともあって修士入学当初から物理学と数学の境界の分野での研究をめざしていた．しかし，どのような方向に研究を進めるかはなかなか決めることができず，試行錯誤の日が続いた．次第に量子力学と関連する話題に関心が行くようになったようである．よく知られているように量子状態は，とりうる可能性のある状態の重ね合わせ (1 次結合) として記述される．測定によって，重ね合わせ状態はある一つの状態に変わってしまうが，どの状態になるかは確率的にしか表現できない．測定によって波動関数が収縮するとよく表現されるが，その過程をどのように解釈するかにはさまざまな立場があるが，物理学ではボーアによるコペンハーゲン解釈が有力視されていた．しかし，その解釈に納得しない立場の物理学者もいて，様々な解釈がなされてきた．一方，測定結果が確率的にしか予言できないことを重視すれば，測定結果を統計的な対象として取り扱おうという立場もありうる．また，そうした立場をとれば，測定結果から，元の量子状態を推測する量子推定問題も考えられる．林正人君は研究の方向を探しているうちに，こうした統計的な手法による量子力学へのアプローチに興味を持ち，それと深く関係した量子情報理論の研究を目標とすることにした．研究目標を決める際に，量子情報理論の研究者であった A. V. Holevo との出会いが重要な役割をしたと聞いている．

「量子力学が統計的側面を持っている以上, 量子力学の本質的理解のためには, 数理統計学と量子力学を融合させた理論体系の構築が不可欠である．また同時に, 光通信システムを始めとする 量子力学に従うシステムから得られる情報の限界を追究するにも このような理論体系は必須である.」と林正人君は学位論文の概要に記している．後述するように，量子情報理論に関してこうした理論体系を構築することに林正人君は成功したといってよいと思われる．

ところで，1994 年は Peter Shor が量子計算による素因数分解の高速アルゴリズムを発見した年でもある．この発見によって，量子コンピュータが登場すれば，現在使われている RSA 暗号は簡単に破られてしまうために，一部の研究者の注目を引いていた．しかし，量子情報理論の研究者はそれほど多くはなく，理論もポピュラーではなかった当時，理論の重要さ，面白さを自ら見出した林正人君のセンスに敬意を表したい．量子力学を研究するために情報科学の考え方を持ち込むことは，現在では物理学者の間でも徐々に支持されてきているが，当時は殆ど関心を持たれなかった．林正人君は数学のサイドから量子力学へのアプローチを考えたことによって，新しい風景を見ることができたのであろう．

量子情報理論のもととなる研究は 1935 年に Einstein, B. Podolsky, N. Rosen によって発表されたエンタグルメントした粒子に関する思考実験に始まる．たとえば，スピン 0 の素粒子が崩壊して，二つの電子になる場合を考えると，二つの電子は互いに異なる方向に飛んでいき，時間が経つと空間的に離れた状態になる．二つの電子が十分に離れた状態で一方の電子のスピンを測定して，たとえば上向きのスピンであることが分かると，角運動量保存則より遠く離れたもう一方の電子のスピンは下向きでなければならない．どのように遠く離れていても，一方での測定の結果は他方の測定結果を決めてしまう．測定するまで電子のスピンの向きは分からないから，一方の電子のスピンの測定結果が遠く離れた他方の電子に瞬間的に影響を及ぼすように見える，一見不思議な現象の指摘であった．このことをもって，Einstein 達は量子力学の記述は不完全であり，隠れた変数を持つ正しい理論が存在すべきだと主張した．しかし，ボーアの反論によって (今日から見ると，ボーアの反論は全く反論になっていなかったが)，ほとんどの物理学者は関心を持たなくなった．また，隠れた変数の理論は実験によってほぼ否定された．しかし，情報科学の研究者は Einstein 達の思考実験で指摘された事実を積極的に利用して，量子情報理論へ応用し，たとえば，量子鍵配送によって絶対に安全な秘密通信が可能であることを明らかにした．林正人君の研究の重要な成果のいくつかはこの量子鍵配送に関するものである．

量子鍵配送は暗号を解読するための鍵 (乱数) を，暗号の送付者と暗号の受け取り者との間で，鍵情報を担った量子状態を (通常は位相がほぼ揃った光，コヒーレントな光を使う) 絶対に安全であるように送信する手段である．送られている鍵情報は量子状態であるので，第三者が傍受したとすると量子状態が変わり，そのことから盗聴があったことが分かる．量子状態はコピーできないので，盗聴者は盗聴する前と同じ量子状態をこっそり送り直すことができないからである．量子鍵配送に関して，林君はコヒーレンスの破壊度合いを調べることのできる位相測定を行ったときに測定値のエラーから情報漏洩の量を推測する方法を確立した．これによって，鍵情報を担った同じ量子状態を複数回送付し，送られてきたもののなかからランダムに位相測定を行うことによって，測定値のエラーの状況から情報が漏洩したか否かを判断することができる．ただし，これは送られてきたデータのすべての位相測定をしたわけでないので，全体のエラー率の推測でしかない．そこで，

林君は統計学を使って，推測誤差の見積もりを与えて，理論を完全なものとした．

しかし，実際には，量子的な通信路を用いて量子状態を送るときにノイズが発生し，完全なコヒーレンスの状態を保つことはできず，ノイズの中に盗聴が隠されてしまう危険がある．そこで，部分的に盗聴者に漏洩してしまった鍵情報を考え，そこから情報漏洩がない鍵を取り出す必要がある (これを秘匿性増強という)．そのためには，鍵のビット数を減らして新しい鍵を作り，漏洩した情報と無関係にすることができることが知られている．ただ，どれだけのビット数を減らせばよいかが重要になる．この問題に関して，林君は必要最小限とするビットの量を確定し，問題を解決した．ところで，秘匿性増強のためには，一括して処理するビット数を長くするとよいが，そのためには処理に時間がかかる．ここでも，林君は有限体を使って，一括して処理するビット数が長くても計算効率が上がる方法を見出している．こうした結果を得るために，林君は群の表現論を駆使して，問題を表現論的な観点で書き直すことによって，理論全体の数学的な構造を明確にすることによって問題を解決した．このように，林君は暗号通信に関してその理論的な基礎付けを行っただけではなく，量子情報理論の数学的な枠組みを明確にし，それを活用して多くの重要な問題を解決している．

以上その一部を見たように，林正人君の研究は数学，数理統計学を駆使した量子情報理論の構築であり，数学の見事な応用と言える．それだけでなく，これらの研究結果は量子情報理論から量子力学に新しい光を投げかけるものである．こうした研究が，数学の大学院出身者から誕生したことは誠に喜ばしいことである．しかしながら，研究者をめざす過程で，林正人君に対して日本の数学界は暖かくはなかったどころか，きわめて冷淡であった．新しいことに挑戦する若手研究者を励ます風土は日本の数学界には皆無と言ってよい．功なり遂げなければ自分たちの世界に招き入れないようでは，数学研究の世界は拡がらない．林正人君はこれまでにいくつかの賞を受賞しているが，数学関係の賞は皆無である．

私は建部賢弘賞の発案者の一人であるが，この賞が今日どれだけ有効に機能しているのであろうか．確立した分野での優秀な若手を顕彰することはもちろん意味あることではあるが，新しい分野に挑戦している若手研究者を励ますことはさらに重要なことである．そのために，日本数学会はどれだけの努力をしてきたのであろうか？

林正人君の今回の受賞は日本の数学界と日本数学会に，若手研究者の育成に対して重大な警鐘を鳴らしていることを力説しておきたい．