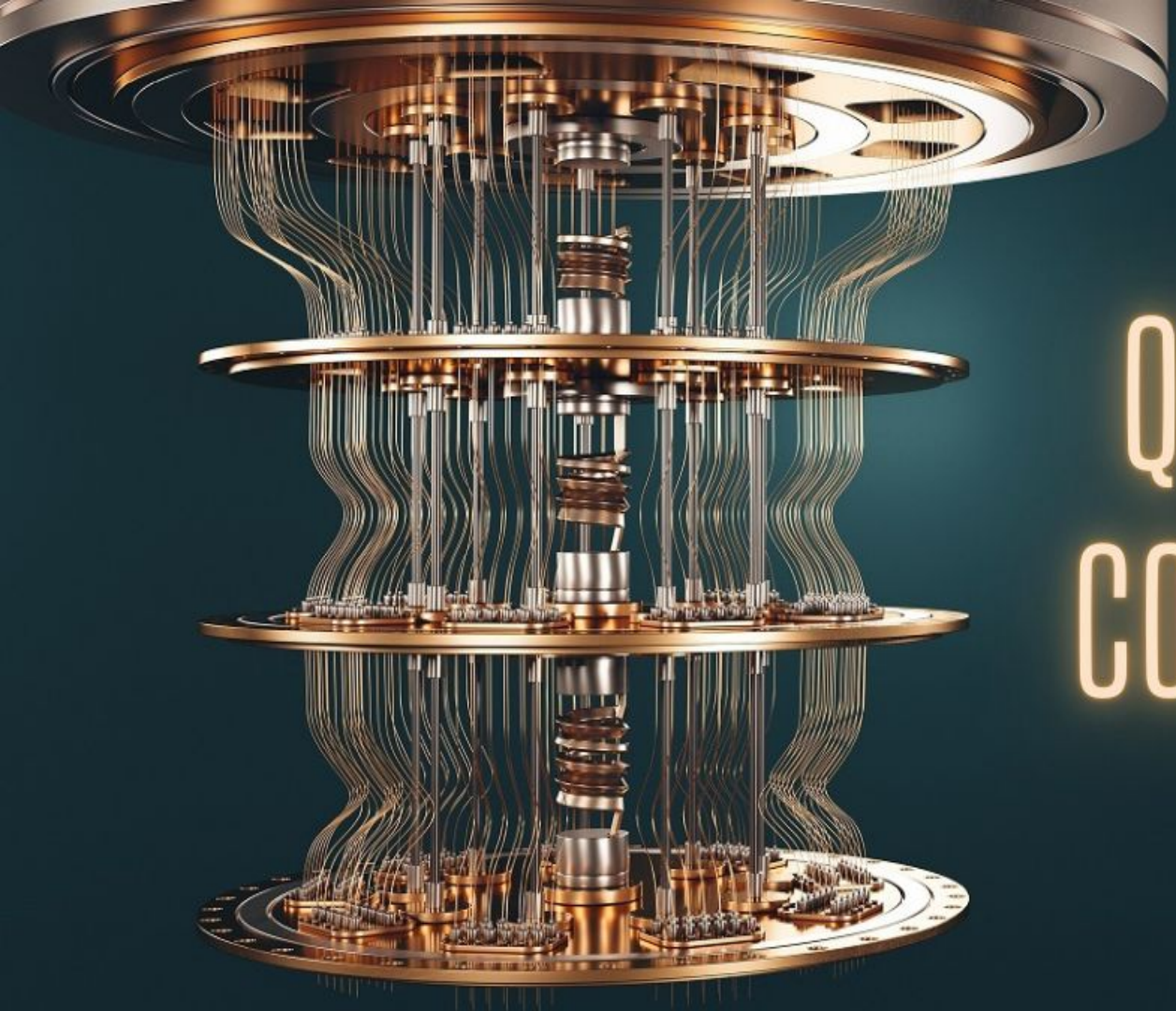
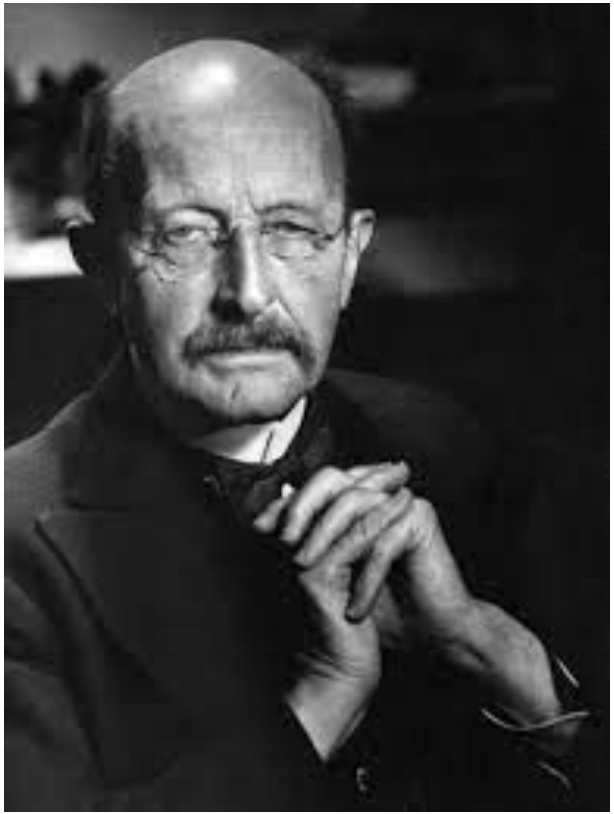


QUANTUM COMPUTING

Κυπραίος Ηλίας
ΑΛΜΑ 2023-2024

Ιστορική Αναδρομή

Max Planck – **Πατέρας της Κβαντικής Θεωρίας** (1900)



Ιστορική Αναδρομή

- Το 1969 ο Αμερικάνος φυσικός Steven Wiesner πρότεινε την αξιοποίηση της κβαντικής πληροφορίας ως ένα μέσο για την καλύτερη εκτέλεση κρυπτολογικών πρωτοκόλλων.
- Τη δεκαετία του 1970 έχουμε τις τέσσερις πρώτες δημοσιευμένες εργασίες πάνω στην κβαντική πληροφορία.
- Το 1980 ο Αμερικάνος φυσικός Paul Benioff δημοσίευσε μία εργασία του περιγράφει τη δυνατότητα της κβαντικής υπολογιστικής και το πως θα μπορούσε να λειτουργήσει ένας υπολογιστής με τους νόμους της Κβαντομηχανικής.

Ιστορική Αναδρομή

- Το 1982 ο Αμερικάνος φυσικός Richard Feymann στην ομιλία του με τίτλο ”Simulating Physics with computers”, περιγράφει τον πρώτο Καθολικό Κβαντικό Υπολογιστή και ισχυρίζεται ότι όπως η παγκόσμια μηχανή Turing μπορεί να προσομοιώσει αποτελεσματικά οποιαδήποτε άλλη μηχανή Turing, έτσι και ο Καθολικός Κβαντικός υπολογιστής έχει τη δυνατότητα να προσομοιώνει φυσικά φαινόμενα και οποιοδήποτε άλλο κβαντικό υπολογιστή, με δυνατότητες που δεν έχει ένας κλασικός υπολογιστής.
- Το 1985 ο Βρετανός φυσικός David Deutch, πρότεινε την πρώτη καθολική κβαντική μηχανή Turing και άνοιξε το δρόμο για το μοντέλο ενός κβαντικού κυκλώματος, και τον πρώτο(όχι τόσο εντυπωσιακό) κβαντικό αλγόριθμο.

Ιστορική Αναδρομή

- Στις αρχές της δεκαετίας του 1990 η εξέλιξη στον τομέα της Κβαντικής Υπολογιστικής είναι ραγδαία και το 1992 όπου παρουσιάζεται από τους David Deutch και Richard Jozsa ο πρώτος (ουσιαστικός) κβαντικός αλγόριθμος.
- Μετά από το παραπάνω γεγονός, πλήθος κβαντικών αλγορίθμων έχουν πλέον δημιουργηθεί.

Ιστορική Αναδρομή

- Από θεωρητικής άποψης τα πράγματα είναι ευχάριστα. Από τεχνικής άποψης, υπάρχουν σήμερα κβαντικοί υπολογιστές από μεγάλες εταιρείες (π.χ. Google, IBM) οι οποίοι βρίσκονται σε πρώιμο πειραματικό στάδιο. Ωστόσο, επενδύονται τεράστια ποσά για την ανάπτυξή τους.
- Παρόλα αυτά, υπάρχουν βιβλιοθήκες στην python και σε άλλες γλώσσες προγραμματισμού που προσομοιώνουν την συμπεριφορά ενός κβαντικού υπολογιστή και δίνεται η δυνατότητα προγραμματισμού του.

Qubit έναντι Bit

- Bit: είτε 0 είτε 1
- Qubit: 0 και 1 με πιθανότητα

Περιγραφή του qubit μέσω διανύσματος κατάστασης(πλάτος πιθανοτήτων)

Δύο βασικές καταστάσεις |0> και |1>

$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Αλλά και ενδιάμεσες καταστάσεις: $|x\rangle = x_1|0\rangle + x_2|1\rangle = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$

Κβαντικός Καταχωρητής

- Το μέσο αποθήκευσης των qubits
- Η κβαντική του κατάσταση υπολογίζεται από το τανυστικό γινόμενο όλων των qubits του

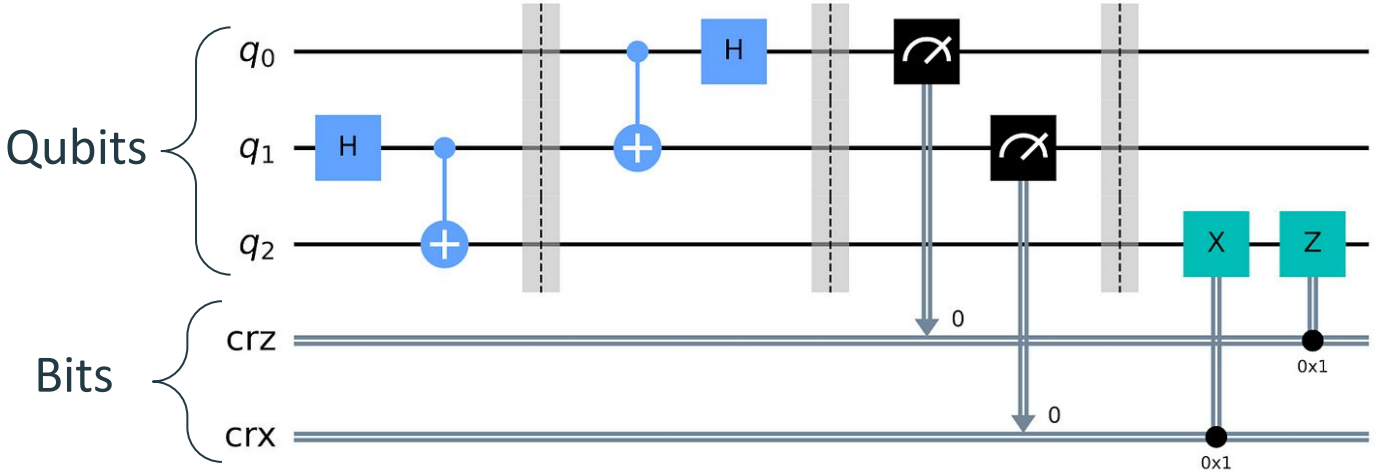
Κβαντικές Πύλες

- Ίδιος σκοπός με τις λογικές πύλες στον κλασικό υπολογιστή
- Η μαθηματική τους μορφή είναι πίνακες

Μερικές Πύλες:

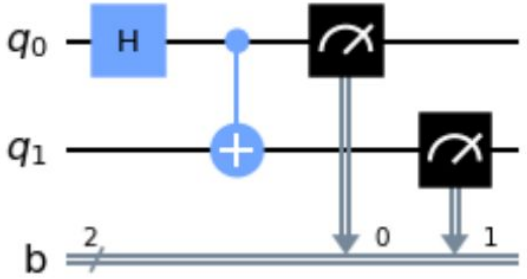
1. Αδράνειας “I”
2. Άρνησης “X”
3. Υπέρθεσης “H”
4. Ελεγχόμενης άρνησης “cX”

Κβαντικό Κύκλωμα

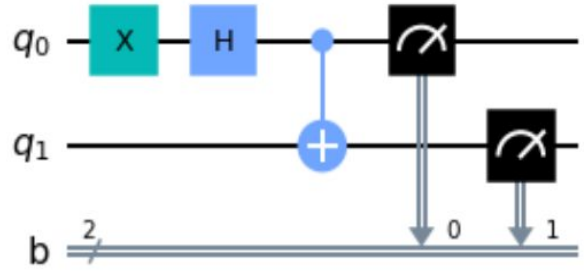


Κβαντική Διεμπλοκή

- $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



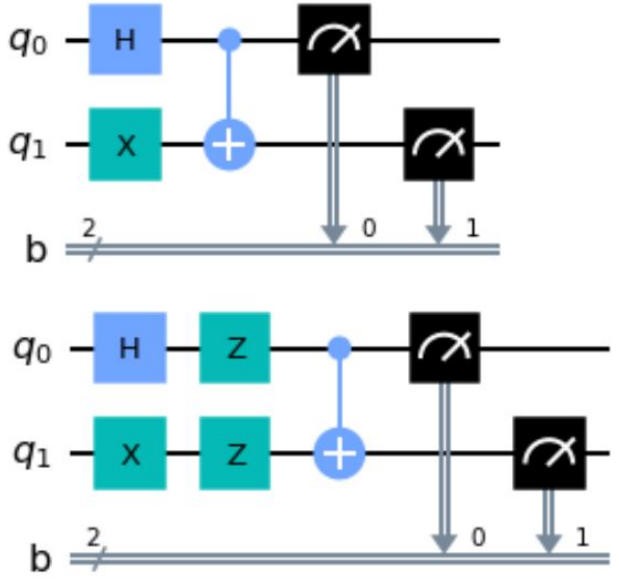
- $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$



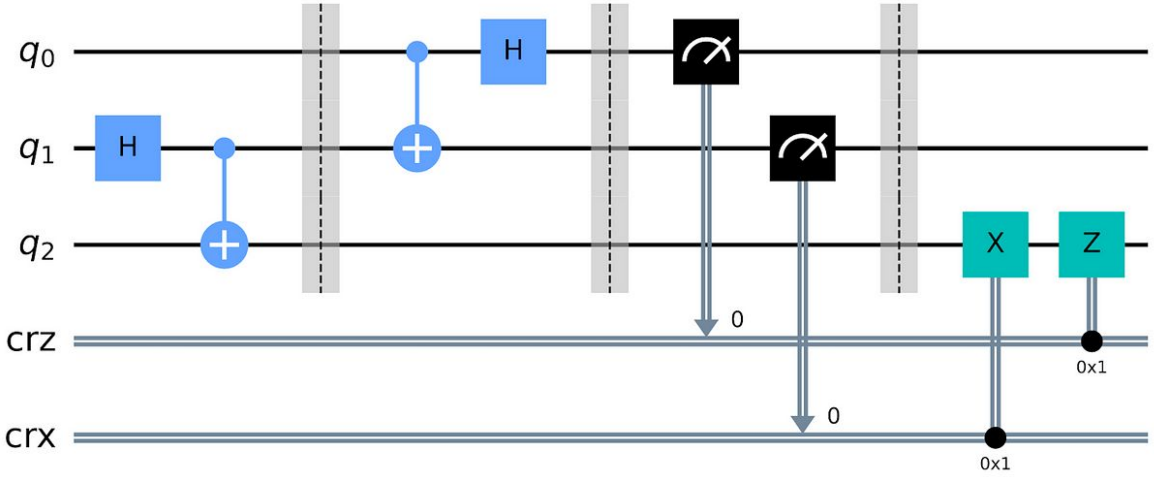
Κβαντική Διεμπλοκή

- $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$

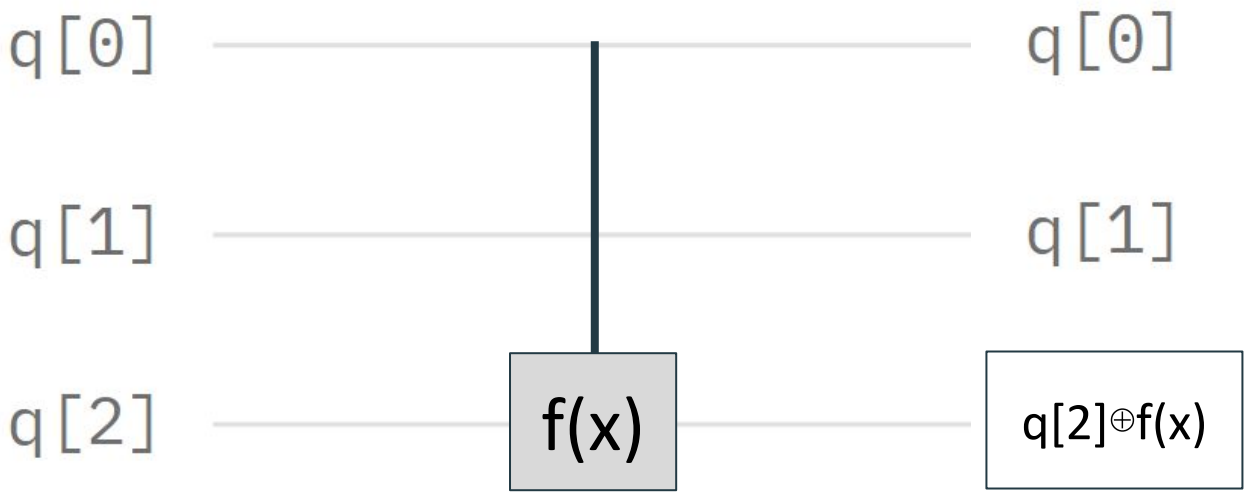
- $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$



Κβαντική Τηλεμεταφορά



Εφαρμογή συνάρτησης σε qubits



Παράδοξα στην Υπέρθεση

Πρόβλημα Deutsch

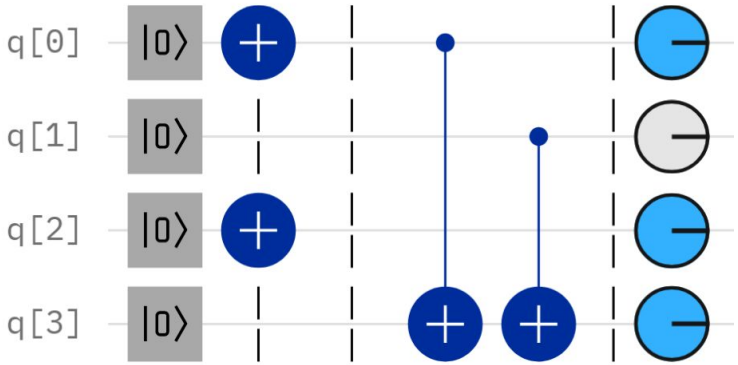
Έστω μία συνάρτηση $f:\{0,1\}\rightarrow\{0,1\}$ η οποία είναι είτε σταθερή είτε ισορροπημένη. Πόσες κλήσεις της f χρειάζεται να κάνω για να διαπιστώσω τι είναι;

Εφαρμογή συνάρτησης σε qubits

$$f(x) = (x \cdot s) \bmod 2$$

Παράδειγμα κυκλώματος για:

$x = [1\,0\,1]$ $\quad$ $s = [1\,1\,0]$



Το αποτέλεσμα της συνάρτησης βρίσκεται στο q[3]

Πρόβλημα Bernstein-Vazirani

Δοσμένης μίας συνάρτησης $f : \{0,1\}^n \longrightarrow \{0,1\}$ όπου η f υλοποιεί το εσωτερικό γινόμενο μεταξύ του x και ενός μυστικού διανύσματος $s \in \{0,1\}^n modulo 2$, δηλαδή $f(x) = x \cdot s = x_1 s_1 \oplus x_2 s_2 \oplus ... \oplus x_n s_n$, βρες το s.

$$f(x) = (x \cdot s) \bmod 2$$

Πρόβλημα Bernstein-Vazirani

- Κλασικός υπολογιστής: ο καλύτερος αλγόριθμος που υπάρχει χρειάζεται να καλέσει το μαντείο n φορές
- Κβαντικός υπολογιστής: ο αλγόριθμος Bernstein-Vazirani καλεί το μαντείο μόνο μία φορά για να ανακαλύψει το μυστικό διάνυσμα

Πρόβλημα Deutsch–Jozsa

Στο πρόβλημα $Deutsch - Jozsa$ δίνεται ένας χβαντικός υπολογιστής ως "μαύρο κουτί", ο οποίος υλοποιεί μία συνάρτηση $f : \{0,1\}^n \longrightarrow \{0,1\}$. Η συνάρτηση αυτή είτε είναι σταθερή, επιστρέφει μόνο 0 ή μόνο 1, είτε είναι ισορροπημένη, δηλαδή επιστρέφει στις μισές εισόδους 0 και στις υπόλοιπες 1. Το ερώτημα είναι αν η f είναι σταθερή ή ισορροπημένη.

Πρόβλημα Deutsch–Jozsa

- Κλασικός υπολογιστής: ο καλύτερος αλγόριθμος που υπάρχει είναι το εξαντλητικό κάλεσμα της συνάρτησης $2^{n-1}+1$ φορές στην χειρότερη περίπτωση
- Κβαντικός υπολογιστής: αρκεί να καλέσει μία φορά την συνάρτηση ώστε να διαπιστώσει αν είναι σταθερή ή όχι

Αλγόριθμος Shor

- Κβαντικός αλγόριθμος παραγοντοποίησης ενός αριθμού.
- Πολυωνυμικού χρόνου έναντι του καλύτερου αλγορίθμου κλασικού υπολογιστή ο οποίος είναι εκθετικός.
- Απειλή για τα σημερινά συστήματα κρυπτογραφίας, τα οποία βασίζονται στην δυσκολία της παραγοντοποίησης ενός αριθμού.
- Ωστόσο, χρειάζεται μερικά δεκάδες χιλιάδες qubits για να λειτουργήσει ενώ ο σημερινός κβαντικός υπολογιστής με τα περισσότερα qubits έχει μόλις περίπου 1000.

Ευχαριστώ πολύ για την προσοχή σας!

Βιβλιογραφία:

1. David Deutsch (1985). "Quantum Theory, the Church-Turing Principle and the Universal Quantum Computer". *Proceedings of the Royal Society of London A*. **400** (1818): 97–117. Bibcode:1985RSPSA.400...97D. CiteSeerX 10.1.1.41.2382. doi:10.1098/rspa.1985.0070. S2CID 1438116.
2. Johansson, N.; Larsson, JÅ. (2017). "Efficient classical simulation of the Deutsch–Jozsa and Simon's algorithms". *Quantum Inf Process (2017)*. **16** (9): 233. arXiv:1508.05027. Bibcode:2017QuIP...16..233J. doi:10.1007/s11128-017-1679-7. S2CID 28670540.
3. Simon, Daniel (November 1994). "On the power of quantum computation". *Proceedings 35th Annual Symposium on Foundations of Computer Science*. pp. 116–123. doi:10.1109/SFCS.1994.365701. ISBN 0-8186-6580-7. S2CID 7457814.
4. Ethan Bernstein and Umesh Vazirani (1997). "Quantum Complexity Theory". *SIAM Journal on Computing*. **26** (5): 1411–1473. doi:10.1137/S0097539796300921.
5. David Deutsch & Richard Jozsa (1992). "Rapid solutions of problems by quantum computation". *Proceedings of the Royal Society of London A*. **439** (1907): 553–558. Bibcode:1992RSPSA.439..553D. CiteSeerX 10.1.1.655.5997. doi:10.1098/rspa.1992.0167. S2CID 121702767.