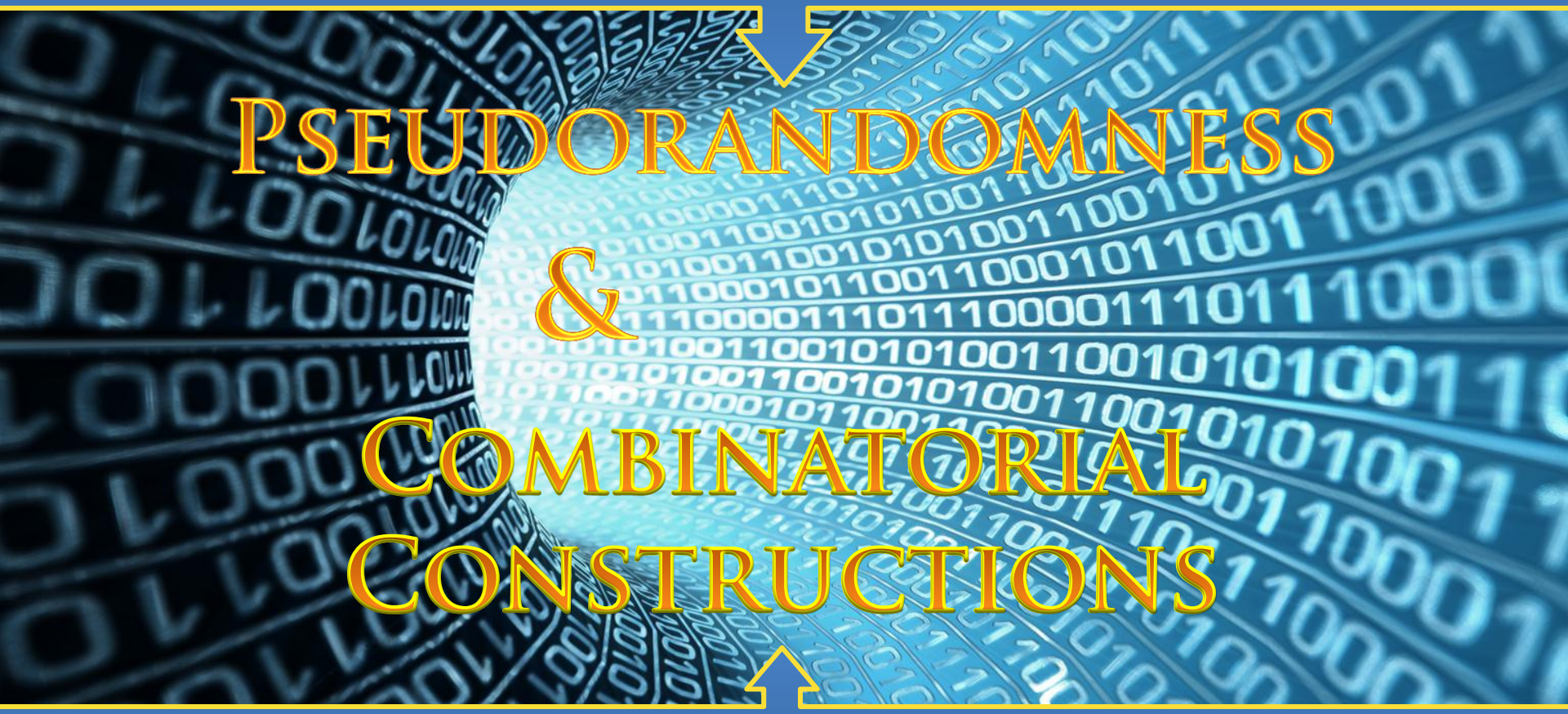
Pseudorandomness = Μη αληθής + Τυχαιότητα

* Συνήθως παίρνουμε μια στατιστική τυχαιότητα από μια ντετερμινιστική επεξεργασία.
* Η παραγωγή ψευδοτυχαιότητας είναι πιο εύκολη από την πραγματική τυχαιότητα.
* Για πραγματική τυχαιότητα χρειαζόμαστε ακριβείς μετρήσεις σε πραγματικά ντετερμινιστικές διεργασίες.
* Ένα παράδειγμα πραγματικής τυχαιότητας είναι οι:

«Hardware Random Number Generators»



Combinatorial Constructions = Κατασκευές Συνδυαστικής

* Αφορά τη μελέτη των πεπερασμένων ή μετρήσιμα διακριτών δομών.
* Στην περίπτωσή μας είναι χρήσιμες στη μελέτη και εκτίμηση κατά την ανάλυση των αλγορίθμων.

Probabilistic Method

- Τι είναι;

  Ένα χρήσιμο εργαλείο με το οποίο μπορούμε να αποδεικνύουμε την ύπαρξη «προϊόντων» της Συνδυαστικής που έχουν συγκεκριμένες ιδιότητες.

- Πόσο εύκολο είναι να κατασκευάσουμε αυτά τα προϊόντα;

  Πολλές φορές είναι πολύ δύσκολο ή δε γνωρίζουμε τον τρόπο.

- Πιθανοτικοί ή Ντετερμινιστικοί Αλγόριθμοι

  Για το ίδιο πρόβλημα, πολλές φορές οι Πιθανοτικοί αλγόριθμοι είναι πιο απλοί και αποτελεσματικοί από τον πιο καλό γνωστό ντετερμινιστικό αλγόριθμο.

- Είναι οι Πιθανοτικοί Αλγόριθμοι αποτελεσματικοί;

  Μετά από κάποιες παραδοχές της θεωρίας της πολυπλοκότητας, κάθε Πιθανοτικός αλγόριθμος έχει μια αποτελεσματική ντετερμινιστική Προσομοίωση.

- Που χρησιμοποιείται η Πιθανοτική Μέθοδος;

Χρησιμοποιείται για να αποδείξουμε ότι ένα τυχαίο αντικείμενο έχει κάποια ιδιότητα με θετική πιθανότητα.

- Πότε χρησιμοποιήθηκε για πρώτη φορά;

Η ιδέα χρησιμοποιήθηκε για πρώτη φορά από τον Paul Erdös (1947) και στη συνέχεια βρήκε μεγάλη ανάπτυξη, χαρίζοντάς μας μερικά από τα πιο γνωστά φράγματα στα περισσότερα προβλήματα της Συνδυαστικής.

- Ποιο ερώτημα ήθελε αρχικά να απαντήσει ο Erdös;

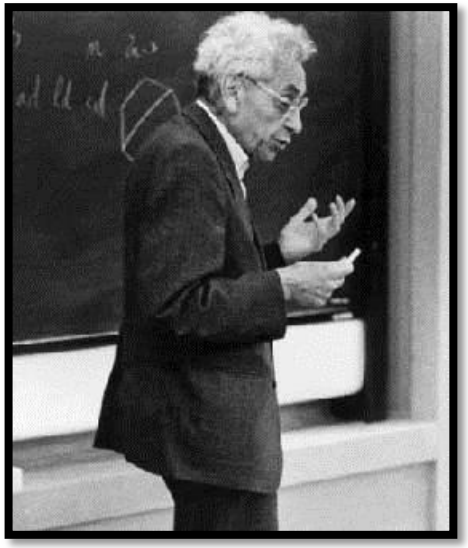
Ορίζουμε ως $R(k,k)$ τη μικρότερη τιμή n, τέτοια ώστε να θέλουμε κάθε γράφημα με n κορυφές, να έχει είτε ένα Ανεξάρτητο Σύνολο μεγέθους τουλάχιστον k ή μια Κλίκα μεγέθους τουλάχιστον k.

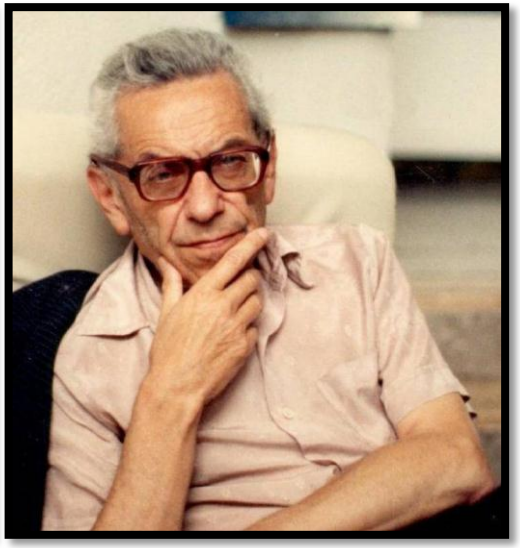
- Τι ξέραμε γι' αυτό μέχρι τότε;

Ότι το $R(k,k)$ είναι πεπερασμένο και είναι το πολύ 4^k. Προσπαθούσαμε να βρούμε κάποιο καλύτερο φράγμα, μέχρι που ο Erdös το απέδειξε για ένα τυχαίο γράφημα με $2^{k/2}$ κορυφές και μας έδωσε ότι $R(k,k) \geq 2^{k/2}$.

Paul Erdös

1913 - 1996



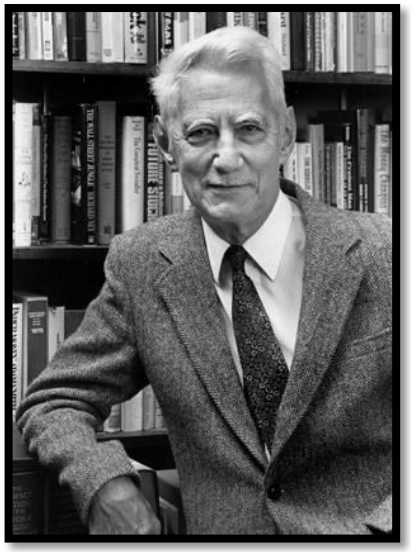


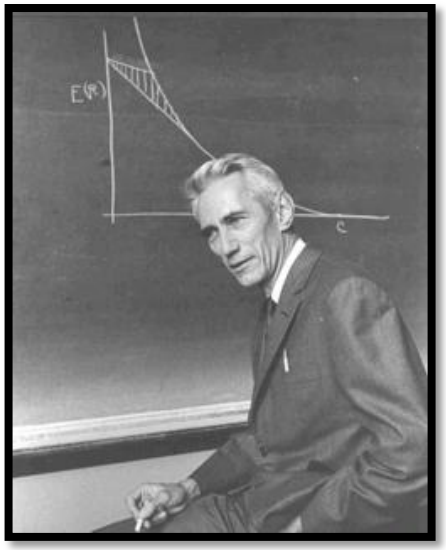
Ειδικότητα: ***Μαθηματικός***
Εθνικότητα: ***Ουγγαρία***
Πεδία Ενδιαφέροντος:
Συνδυαστική, Θεωρία Γραφημάτων, Θεωρία Αριθμών, Κλασσική Ανάλυση, Προσεγγιστική Θεωρία, Θεωρία Συνόλων και Πιθανοτική Θεωρία
Μερικές αγαπημένες συνήθειες:
Ονόμαζε τα μικρά παιδιά ως «ε», τις γυναίκες ως «αφεντικά» και τους άνδρες «δούλους». Γι' αυτόν, όποιος σταματούσε τα μαθηματικά, θεωρούνταν νεκρός. Θεωρούσε το αλκοόλ ως δηλητήριο και τους παντρεμένους ως αιχμαλώτους.

Η φωτογραφία έχει τραβηχτεί σε μια Επισκοπική εκκλησία, τον Αγ. Γρηγόριο τον Νύσση, η οποία βρίσκεται στο Σαν Φρανσίσκο και παριστάνει την πομπή των Αγίων που χορεύουν.
Στη φωτογραφία, εκτός από τον Erdös, μπορούν να διακριθούν από αριστερά προς τα δεξιά οι: Seraphim, Gandhi, Erdös, Martin Luther και Thomas Merton.
Η συγκεκριμένη εκκλησία φιλοξενεί πολλούς επιστήμονες σε διάφορε παραστάσεις.

Claude Shannon

1916 - 2001





Ειδικότητα: ***Μαθηματικός, Ηλεκτρολόγος Μηχανικός και Κρυπτογράφος***

Εθνικότητα: ***Αμερική***

Χαρακτηρισμός:

Πατέρας της Θεωρίας της Πληροφορίας

Μερικά κατορθώματά του:

Έβαλε τα θεμέλια της Θεωρίας της Πληροφορίας το 1948 με ένα paper που κυκλοφόρησε ενώ λίγο πιο πριν, το 1937, είχε θεμελιώσει τη θεωρία του ψηφιακού υπολογιστή και του ψηφιακού κυκλώματος. Αυτό το έκανε σε ηλικία 21 ετών, όταν ήταν Μεταπτυχιακός φοιτητής στο MIT και στη διπλωματική του έδειξε πως οι ηλεκτρονικές εφαρμογές της Boolean άλγεβρας θα μπορούσαν να λύσουν κάθε λογική και αριθμητική σχέση.

- Τι έκανε ο Shannon;

Εφαρμόζοντας την ίδια ιδέα με τον Erdös, απέδειξε την ύπαρξη συστημάτων κωδικοποίησης που θα μπορούσαν να διορθώσουν τα λάθη ενός «θορυβώδους» καναλιού επικοινωνίας και να πετύχουν τη βέλτιστη δυνατή συμπίεση των δεδομένων.

- Γιατί είναι ο πατέρας της «Θεωρίας της Πληροφορίας»;

Επειδή η «Θεωρία της Πληροφορίας» προέκυψε από την προσπάθεια μετατροπής των Αποτελεσμάτων του Shannon σε αλγοριθμικά συστήματα κωδικοποίησης και αποκωδικοποίησης.

Probabilistic Algorithms

- Μερικά παραδείγματα Πιθανοτικών Αλγορίθμων

1. *Οι πιθανοτικοί αλγόριθμοι πολυωνυμικού χρόνου που ελέγχουν αν ένας ακέραιος είναι πρώτος ή όχι.*

   Σε αυτούς τους αλγόριθμους ψάχνουμε για κάποιο «πιστοποιητικό» που να μας δείχνει αν ένας αριθμός n είναι σύνθετος. Ένα τέτοιο πιστοποιητικό θα μπορούσε να είναι ένας ακέραιος a τέτοιος ώστε $a^n \not\equiv a(mod n)$ *ή τέσσερεις διακεκριμένες τετραγωνικές ρίζες* $(mod n)$ *του ίδιου ακεραίου. Οι Rabin, Solovay, και Strassen απέδειξαν ότι έχουμε πολλές πιθανότητες να βρούμε αυτά τα πιστοποιητικά αν αρχίσουμε να τα επιλέγουμε τυχαία.*

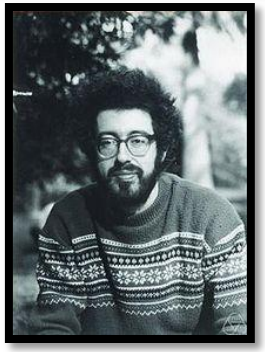
2. *Ένα άλλος αλγόριθμος είναι αυτός που ελέγχει αν δύο πολυώνυμα πολλών μεταβλητών είναι ίδια.*

3. *Ένας αλγόριθμος που ελέγχει αν δύο κορυφές σε ένα γράφημα συνδέονται με κάποιο μονοπάτι. Για να το κάνουμε αυτό, παίρνουμε έναν τυχαίο περίπατο από την πρώτη κορυφή και ελέγχουμε αν φτάνουμε στη δεύτερη κορυφή μετά από έναν συγκεκριμένο αριθμό βημάτων.*

Rabin, Solovay & Strassen

Michael O. Rabin (1931)

Ειδικότητα: ***Πληροφορική***
Εθνικότητα: ***Ισραήλ***
Μερικά για τα οποία είναι γνωστός:
Miller-Rabin primality test, Rabin cryptosystems, Oblivious transfer, Randomized algorithms κα.
Βραβεία:
Turing Award, Israel Prize, Emet Prize, Harvey Prize, Dan David Prize



Robert M. Solovay (1938)

Ειδικότητα: ***Μαθηματικός***
Εθνικότητα: ***Αμερική***
Μερικά για τα οποία είναι γνωστός:
Solovay's Theorem, Isolating the notion of $0^{\#}$, Set Theory proofs

Volker Strassen (1936)

Ειδικότητα: ***Μαθηματικός***
Εθνικότητα: ***Γερμανία***
Μερικά για τα οποία είναι γνωστός:
Analysis of Algorithms, Strassen's algorithm (matrix multiplication), Primality Test
Βραβεία:
Cantor medal, Paris Kanellakis Award, Kruth Prize, Konrad Zuse Medal

Computational Theory of Pseudorandomness

- Ποιοι είναι πιο ισχυροί, οι πιθανοτικοί ή οι ντετερμινιστικοί αλγόριθμοι;

Αρχικά, θεωρούσαν τους πιθανοτικούς αλγόριθμους ως πιο ισχυρούς από τους ντετερμινιστικούς, επειδή υπήρχαν προβλήματα που οι πρώτοι μπορούσαν να λύσουν σε πολυωνυμικό χρόνο ενώ οι δεύτεροι όχι.
Όμως αυτή η άποψη ανατράπηκε από την περαιτέρω ανάπτυξη της Υπολογιστικής Θεωρίας της Ψευδοτυχαιότητας. Την αρχή έκαναν οι: Blum, Goldwasser, Micali και Yao, με το να αναπτύξουν γερά θεμέλια στην Κρυπτογραφία.

Manuel Blum
1938
(Venezuela)
Carnegie Mellon

Shafrira Goldwasser
1958
(Israel - America)
MIT

Silvio Micali
1954
(Italy - America)
MIT

Andrew Yao
1946
(China)
Chinese U. of Hong Kong

Derandomization

- Τι είναι derandomization;

Η διαδικασία κατά την οποία αφαιρούμε ή περιορίζουμε σημαντικά την τυχαιότητα σε κάποιον τυχαιοκρατικό αλγόριθμο.

- Μερικά αποτελέσματα απαλοιφής της τυχαιότητας υπό όρους:

Για θεωρήματα της παρακάτω μορφής:

Εάν μια υπόθεση X είναι αληθής, τότε κάθε πρόβλημα που μπορεί να λυθεί από έναν Πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου, μπορεί να λυθεί κι από έναν Ντετερμινιστικό αλγόριθμο με χρόνο εκτέλεσης Y.

Ο Yao έδειξε ότι μπορούμε να πάρουμε το X να είναι:

Δεν υπάρχει κανένας αλγόριθμος πολυωνυμικού χρόνου που με την είσοδο ενός τυχαίου ακεραίου να μας δώσει την ανάλυση του σε γινόμενο πρώτων αριθμών.

Και το Y να είναι:

Χρόνου ίσου με $2^{n^{\epsilon}}$, για $\epsilon > 0$.

- Υπάρχει κάτι καλύτερο;

Στις δεκαετίες του 1980 και 1990 έγιναν αρκετές προσπάθειες για να «κάνουν» το Υ να είναι πολυωνυμικού χρόνου για κάποιο X.
Το 1997, οι Impagliazzo και Wigderson το κατόρθωσαν σε δύο βήματα:

1. *Έδειξαν πως μια υπόθεση που ισχύει στην περίπτωση της χειρότερης πολυπλοκότητας κάποιων προβλημάτων, μπορεί να μας οδηγήσει σε κάποια ισχυρότερη υπόθεση που θα ισχύει και για την μέση περίπτωση της πολυπλοκότητας των ίδιων προβλημάτων. Με άλλα λόγια, απλοποιούμε τη δύσκολη υπόθεση της χειρότερης πολυπλοκότητας σε μια υπόθεση μέσης περίπτωσης.*

2. *Έδειξαν ότι η υπόθεση της μέσης περίπτωσης είναι αρκετή για να κατασκευάσουμε μια συγκεκριμένη πολύ ισχυρή γεννήτρια ψευδοτυχαιότητας. Κι επιπλέον, η γεννήτρια αυτή είναι αρκετή για να προσομοιώσει ντετερμινιστικά, κάθε Πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου, σε πολυωνυμικό χρόνο.*

- Πού καταλήγουμε;

Σε κάθε Πιθανοτικό αλγόριθμο πολυωνυμικού χρόνου, μπορούμε να αφαιρέσουμε ή να μειώσουμε την τυχαιότητα, ακόμη και σε Προσεγγιστικούς αλγορίθμους, εφαρμόζοντας τη μέθοδο των Sinclair και Jerrum.

- Αν τελικά βρίσκαμε κάποιον τρόπο να απαλείψουμε την τυχαιότητα από όλους τους Πιθανοτικούς αλγορίθμους σε πολυωνυμικό χρόνο, θα σταματούσαμε να την χρησιμοποιούμε στην Επιστήμη των Υπολογιστών;

Η απάντηση είναι «Όχι», και κυρίως για δύο λόγους:

1. *Το πιθανότερο είναι μια τέτοια απαλοιφή να μην είναι πρακτική.*
2. *Υπάρχουν αρκετές εφαρμογές στην Επιστήμη των Υπολογιστών στις οποίες η χρήση της τυχαιότητας είναι αναπόφευκτη. Για παράδειγμα, σκεφτείτε να θέλουμε να κατασκευάσουμε ένα ασφαλές κρυπτογραφικό πρωτόκολλο στο οποίο όλα τα εμπλεκόμενα μέρη συμπεριφέρονται ντετερμινιστικά.*

Russell Impagliazzo
1963
(America)
San Diego University

Avi Wigderson
1956
(Israel)
Princeton

Alistair Sinclair
1951
(Britain)
Berkeley

Mark Jerrum
1955
(Britain)
Queen Mary, U. London

Pseudorandom Objects: Codes and Graphs

- Πως λειτουργούν οι Error-Correcting Codes;

Επιλέγουμε ένα τυχαίο σύνολο:

$$S \subseteq \{0,1\}^n \text{ μεγέθους } 2^k, \text{ με } k < n$$

Εάν $k = \frac{n}{2}$, *τότε είναι εύκολο να δείξουμε ότι υπάρχει μια απόλυτη σταθερά* $\delta > 0$, *τέτοια ώστε υπάρχει μεγάλη πιθανότητα κάθε δύο στοιχεία* $u, v \in S$ *να διαφέρουν σε τουλάχιστον* δn *συντεταγμένες.*

Επιπλέον, μπορούμε να παρατηρήσουμε ότι υπάρχει μια απόλυτη σταθερά c, *τέτοια ώστε για κάθε* $\epsilon > 0$, *να είναι πολύ πιθανό κάθε δύο στοιχεία του* S *να διαφέρουνε σε τουλάχιστον* $\left(\frac{1}{2} - \epsilon\right) n$ *συντεταγμένες, με* $k \leq c\epsilon^2 n$.

Τώρα, κάνουμε κάτι παρόμοιο με το παραπάνω, και παίρνουμε μια τυχαία συνάρτηση $C: \{0,1\}^k \to \{0,1\}^n$ *που θα μας δώσει και πάλι τα ίδια φράγματα.*

Για δύο strings $u, v \in \{0,1\}^n$, *η Hamming απόσταση μεταξύ των* u *και* v, *που συμβολίζεται με* $d_H(u, v)$ *είναι ο αριθμός των συντεταγμένων στις οποίες τα* u *και* v *διαφέρουν, δηλαδή:*

$$d_H(u, v) := |\{i : u_i \neq v_i\}|$$

- Ορισμός του Error-Correcting Code

Έστω $C: \{0,1\}^k \to \{0,1\}^n$ *ένας* (n, k, d)*-κώδικας, εάν για κάθε δύο διακεκριμένα* $x, y \in C$*,*

$$d_H(C(x), C(y)) \geq d$$

- Ορισμός του List-Decodable Code

Έστω ότι *η* (L, δ)*-λίστα αποκωδικοποιεί* το $C: \{0,1\}^k \to \{0,1\}^n$ *εάν για κάθε* $u \in \{0,1\}^n$*,*

$$\left|\{x \in \{0,1\}^k : d_H(C(x), u) \leq \delta n\}\right| \leq L$$

- Expander Graphs

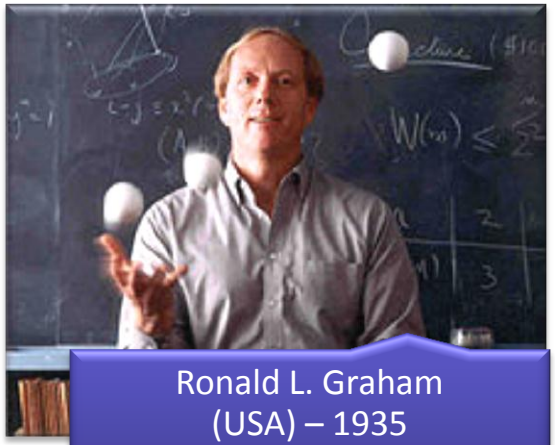
Θα επιλέξουμε τυχαία έναν γράφο με βάση την κατανομή $G_{n,\frac{1}{2}}$.

Η κατανομή $G_{n,\frac{1}{2}}$ *είναι η κανονική κατανομή πάνω στο σύνολο των* $2^{\binom{n}{2}}$ *γράφων με* n *κορυφές. Αν κάνουμε έναν απλό υπολογισμό, θα βρούμε ότι για κάθε δύο ξένα σύνολα κορυφών* A, B*, θα υπάρχουν* $\left(\frac{1}{2} \pm o_n(1)\right)|A||B|$ *ακμές με τη μια άκρη στο* A *και την άλλη στο* B.

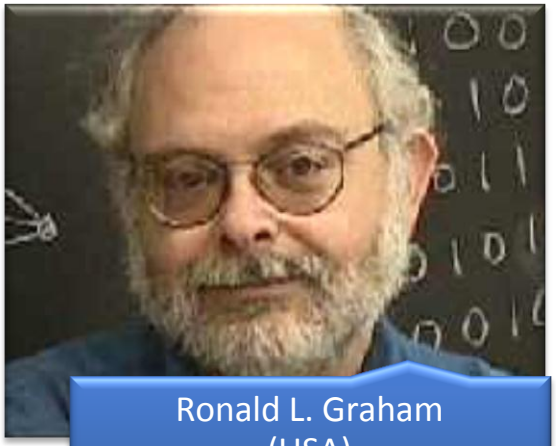
Οι Chung, Graham και Wilson αποκαλούν την οικογένεια των γράφων που ικανοποιούν τις παραπάνω ιδιότητες, ως την οικογένεια των quasi-random γράφων και απέδειξαν ότι έξι εναλλακτικοί ορισμοί της quasi-randomness είναι όλοι τους ισοδύναμοι.

Contribution to:
Error-Correcting Codes & Expander Graphs

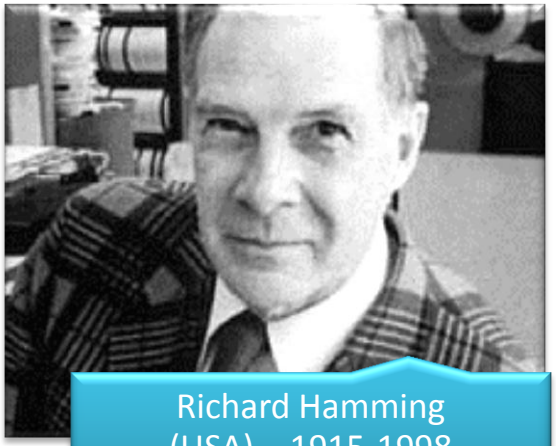
Fan R. K. Chung
(Taiwan) – 1949
San Diego



Ronald L. Graham
(USA) – 1935
San Diego



Ronald L. Graham
(USA)
California Inst. Of Technol.



Richard Hamming
(USA) – 1915-1998
Naval Postgraduate Sch.

Randomness Extractor

- Τι είναι;

Οι Randomness Extractors είναι διεργασίες που σχεδιάστηκαν για να λύσουν το πρόβλημα παραγωγής τυχαίων bits.

Οι Randomness Extractors είναι ένα είδος ψευδοτυχαίων γράφων, μπορούν να κατασκευαστούν με τεχνικές ψευδοτυχαιότητας και συνδέονται πολύ με κατασκευές όπως οι error-correcting codes, expanders κι άλλα αντικείμενα της Συνδυαστικής που μοιάζουν ως τυχαιοκρατικά.

ΠΑΡΑΓΟΝΤΑΣ ΤΥΧΑΙΑ BITS

- Τι χρειαζόμαστε;

Ένα φυσικό φαινόμενο που θα μπορούσε να χαρακτηριστεί ως τυχαίο.
Ας πούμε σε έναν υπολογιστή θα μπορούσε να είναι:

- *Στατιστικά από τις δακτυλογραφήσεις του χρήστη ή τη χρήση του mouse*
- *Ο χρόνος καθυστέρησης του σκληρού δίσκου*
- *Κάποια θερμοκρασία κτλ.*

- Και μετά;

Χρειαζόμαστε μια «hash function», δηλαδή μια συνάρτηση που θα αντιστοιχεί μεγάλα σύνολα δεδομένων μεταβλητού μήκους σε μικρότερα σύνολα δεδομένων με σταθερό μήκος.

Στη συνέχεια θα πάρουμε τα δεδομένα του φυσικού φαινομένου, χρόνο, ταχύτητα, θερμοκρασία κτλ., τα οποία υποτίθεται ότι έχουν μια τυχαιότητα (entropy) και θα τα περάσουμε μέσα από τη «hash function».

Το αποτέλεσμα που θα πάρουμε θεωρείται ως μια συχνότητα πραγματικά τυχαίων bits.

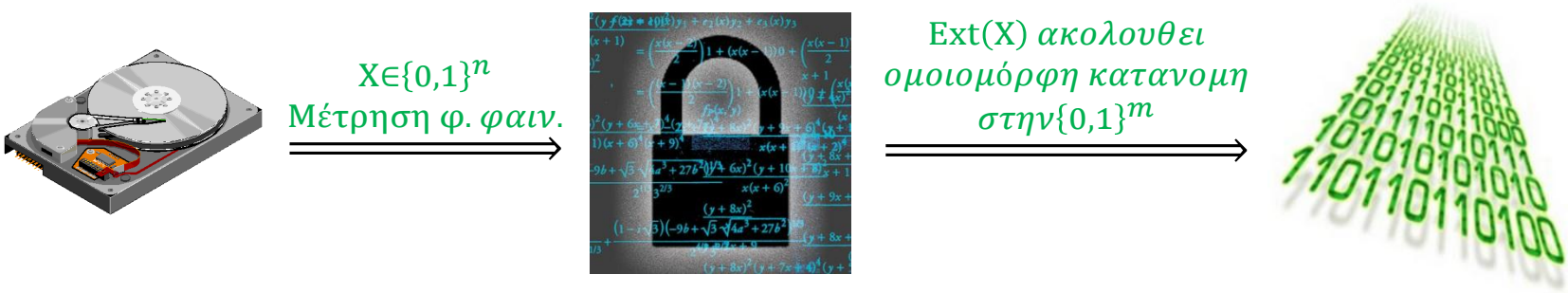
- Ας δούμε μια πιο Μαθηματική έκφραση αυτού που περιγράψαμε:

Έχουμε μια τυχαία μεταβλητή X, που θα παριστάνει τη μέτρηση από το φυσικό φαινόμενο, και θα κυμαίνεται στο $\{0,1\}^n$.

Στη συνέχεια, θέλουμε να κατασκευάσουμε μια συνάρτηση:

$$Ext: \{0,1\}^n \to \{0,1\}^m$$

Τέτοια ώστε κάνοντας όσο το δυνατόν λιγότερες υποθέσεις στη X, να μπορούμε να αποδείξουμε ότι η $Ext(X)$ ακολουθεί την ομοιόμορφη κατανομή στο $\{0,1\}^m$ ή τουλάχιστον την προσεγγίζει.



- Ποιες ήταν οι δύο προσεγγίσεις που έγιναν πάνω στο δύσκολο πρόβλημα της παραγωγής τυχαιότητας για πολύ μεγάλες κλάσεις κατανομών X;

Αρχικά, το όλο πρόβλημα φάνταζε αδύνατο να επιλυθεί.

Όμως δύο προσεγγίσεις που ακολούθησαν, φάνηκαν να προσπαθούν να το παρακάμψουν την όποια δυσκολία:

1. *Η πρώτη προσέγγιση είναι να θεωρήσουμε ένα μοντέλο με μικρό αριθμό μεταβλητών,* $X_1, \dots, X_k$ που είναι ανεξάρτητες μεταξύ τους και ικανοποιούν κάποιες περιορισμένες απαιτήσεις τυχαιότητας. Πρόκειται για μια προσέγγιση που δεν παρουσίασε κάποια ανάπτυξη για πολύ καιρό. Όμως πρόσφατα, το 2004, οι Barak, Impagliazzo και Wigderson έφεραν επανάσταση στο χώρο της Συνδυαστικής με το έργο τους «Extracting randomness using few independent sources» και έδωσαν τροφή για περαιτέρω έρευνα, διευρύνοντας το συγκεκριμένο πεδίο.
2. Η άλλη προσέγγιση, που αναπτύχθηκε από τους Umesh Vazirani και Vijay Vazirani, προτείνει την επιλογή ενός απλού δείγματος X και στη συνέχεια υποθέτει ότι έχουμε έναν τυχαιοκρατικό αλγόριθμο A (που κάνει τυχαίες επιλογές με μεγάλη πιθανότητα) και μια είσοδο x. Αυτό που προσπαθεί να βρει αυτή η προσέγγιση είναι αν μπορούμε να βρούμε αποτελεσματικά ποιο είναι το πιθανότερο αποτέλεσμα που θα μας δώσει ο $A(x)$.

- Ας δούμε μια πιο Μαθηματική έκφραση της δεύτερης προσέγγισης:

Έστω ότι έχουμε ένα Πιθανοτικό αλγόριθμο $A()$ που παίρνει στην είσοδό του δύο στοιχεία:

- *Μια τυχαία είσοδο r*
- *Μια κανονική είσοδο I*

Μπορούμε να ισχυριστούμε ότι ο αλγόριθμος A μπορεί να υπολογίσει μια συνάρτηση f με μεγάλη πιθανότητα, αν για κάθε I:

$$\mathbb{P}[\mathrm{A}(r, I) = f(I)] \geq .9$$

Έστω τώρα U_n μια τυχαία μεταβλητή ομοιόμορφα κατανεμημένη στο $\{0,1\}^n$.

Έστω στη συνέχεια ότι ο αλγόριθμος μας A, απαιτεί m τυχαία bits προκειμένου να επεξεργαστεί κάποια είσοδο x.

Στη συνέχεια, έστω ότι ορίζουμε μια συνάρτηση $Ext: \{0,1\}^n \times \{0,1\}^d \rightarrow \{0,1\}^m$, τέτοια ώστε αν το X αποτελεί την πηγή των μεγεθών που μας δίνει η Φύση και αν η U_d ακολουθεί την ομοιόμορφη κατανομή στο $\{0,1\}^d$, τότε η συνάρτηση $Ext(X, U_d)$ ακολουθεί την ομοιόμορφη κατανομή στο $\{0,1\}^m$.

- Πώς όμως μπορεί να γίνει η προσομοίωση των όσων είπαμε πιο πριν;

Προσομοίωση του αλγορίθμου $\mathrm{A}()$ *πάνω σε μια πηγή Φυσικών μεγεθών* X*:*

1. *Παίρνουμε ένα δείγμα* $x \sim \mathrm{X}$.
2. *Για κάθε* $s \in \{0,1\}^d$*, θα υπολογίσουμε τη σχέση:* $a_s := A(Ext(x,s), I)$.
3. *Τέλος θα πάρουμε στην έξοδο εκείνη την τιμή του* a_s *που εμφανίζεται τις περισσότερες φορές.*

Πιθανότητα υπολογισμού της $f(I)$ *από τον αλγόριθμο* A*, για κάποιο* X*:*

- *Όπως είπαμε πριν, έχουμε:*

$$\mathbb{P}[\mathrm{A}(\mathrm{Ext}(U_d, X), I) = f(I)] \geq .9$$

- Κι επομένως θα έχω:

$$\mathbb{P}_{\mathrm{X}}\left[\mathbb{P}_{\mathrm{U}_d}[\mathrm{A}(\mathrm{Ext}(U_d, X), I) = f(I)] > \frac{1}{2}\right] \geq .8$$

Ο χρόνος εκτέλεσης της προσομοίωσης του A *είναι* 2^d *φορές ο χρόνος εκτέλεσης του* A*, που θα είναι πολυωνυμικός, δεδομένου του χρόνου εκτέλεσης του* A *και αν το* d *είναι λογαριθμικό.*

ΣΤΑΤΙΣΤΙΚΗ ΑΠΟΣΤΑΣΗ

- Είναι απαραίτητο η $Ext(X, U_d)$ να ακολουθεί αυστηρά την ομοιόμορφη κατανομή;

  Όχι! Αρκεί να προσεγγίζει την ομοιόμορφη κατανομή κατά έναν τεχνικό τρόπο.

- Πώς όμως γίνεται αυτό;

  Έστω X και Y δύο τυχαίες μεταβλητές που παίρνουν τιμές από το Ω, τότε θα ορίσουμε Τη Στατιστική τους Απόσταση ως εξής:

$$\|X - Y\|_{SD} \coloneqq max_{T \subseteq \Omega} |\mathbb{P}[\mathrm{X} \in \mathrm{T}] - \mathbb{P}[\mathrm{Y} \in \mathrm{T}]|$$

Αν $\|X - Y\|_{SD} \leq \epsilon$, *τότε λέμε ότι το* X *είναι* ϵ*-κοντά στο* Y.

Με άλλα λόγια λέμε ότι η $Ext: \{0,1\}^n \to \{0,1\}^d \to \{0,1\}^m$ *είναι ένας seeded extractor για κάποιο κατανομή X που επιδέχεται κάποιο σφάλμα* ϵ*, αν η* $Ext\{\mathrm{X}, \mathrm{U}_d\}$ *είναι* ϵ*-κοντά στη* U_m.

ΕΦΑΡΜΟΓΕΣ

- Οι Μηχανές που παράγουν τυχαιότητα έχουν πάρα πολλές εφαρμογές. Μερικές από αυτές είναι:

    - *Simulation of randomized algorithms*
    - *Cryptographic Settings for privacy amplification*
    - *Cryptographic Settings for everlasting security*
    - *Design of pseudorandom generators for space-bounded algorithms.*

- Τι είναι ο χρόνος εκτέλεσης του Αλγορίθμου;

    Ο αριθμός των βημάτων που απαιτεί μια εφαρμογή του αλγορίθμου σε μια Μηχανή Turing.

Circuit Complexity

- Τι είναι Circuit Complexity;

Έστω ότι ένα σύνολο $L \subseteq \{0,1\}^*$ μπορεί να αποφασιστεί σε χρόνο $t(n)$ εάν υπάρχει κάποιος αλγόριθμος που για κάποια είσοδο $x \in \{0,1\}^n$, αποφασίζει σε χρόνο $\leq t(n)$ αν το $x \in$ L.

*Αν θέλουμε να πάρουμε ένα πιο καλό μέτρο για την πολυπλοκότητα, τότε αυτό είναι η **Circuit Complexity**.*

Έτσι, για ακεραίους n και $i \leq n$, θα ορίσουμε το σύνολο

$$\mathrm{P}_{i,n} \coloneqq \{(a_i, \dots, a_n) \in \{0,1\}^n : a_i = 1\}$$

Τότε λέμε ότι ένα σύνολο $S \subseteq \{0,1\}^n$ έχει ένα circuit μεγέθους K *εάν υπάρχει κάποια ακολουθία συνόλων $S_1, \dots, S_k$ τέτοια ώστε:*

1. $\mathrm{S}_K = S$
2. *Κάθε S_j είναι ένα από τα ακόλουθα:*

   - Σύνολο του $\mathrm{P}_{i,n}$

   - Το συμπληρωματικό ενός συνόλου S_h, με $h < j$

   - Η ένωση δύο συνόλων $\mathrm{S}_h \cup \mathrm{S}_l$, με $h, l < j$

   - Η τομή δύο συνόλων $\mathrm{S}_h \cap \mathrm{S}_l$, με $h, l < j$

Τότε λέμε ότι μια συνάρτηση $f : \{0,1\}^n \to \{0,1\}$ έχει ένα circuit μεγέθους K εάν είναι η χαρακτηριστική συνάρτηση ενός συνόλου που έχει circuit μεγέθους K.

Η Circuit Complexity ενός συνόλου S είναι το ελάχιστο K, για το οποίο το S έχει ένα circuit μεγέθους K.

Pseudorandom Generators

- Computational Indistinguishability:

Δύο κατανομές μ_X και μ_Y στο $\{0,1\}^m$ είναι (K, ϵ)-indistinguishable αν για κάθε σύνολο $T \subseteq \{0,1\}^m$ που έχει circuit complexity το πολύ K:

$$\left|\mathbb{P}_{x\sim\mu_X}[x \in T] - \mathbb{P}_{y\sim\mu_Y}[y \in T]\right| \leq \epsilon$$

- Pseudorandomness:

Μια κατανομή μ_X στο $\{0,1\}^m$ είναι (K, ϵ)-pseudorandom αν είναι (K, ϵ)-indistinguishable από την ομοιόμορφη κατανομή. Έτσι, για κάθε σύνολο $T \subseteq \{0,1\}^m$ που έχει circuit complexity το πολύ K:

$$\left|\mathbb{P}_{x\sim\mu_X}[x \in T] - \frac{|\mathrm{T}|}{2^m}\right| \leq \epsilon$$

Thank You !!!