CLEAR- Cahoots-Like Event at Rutgers
Computer Science
Packet by Sam Braunfeld

Finding certain equilibria in these objects is the canonical PPAD-complete problem. Two polytopes are constructed and labels are added and removed to pivot between vertices in the Lemke-Howson algorithm for finding those equilibria in these objects. The ratio of the welfare at the best point and the worst of those equilibria in these objects gives the price of anarchy. Chance nodes that take the expected values of their children are added to one structure that finds solutions for these objects when there is uncertainty, and two constants are maintained, one updated at max nodes and the other at min nodes, in alpha-beta pruning on those structures. For 10 points, linear programming can find optimal mixed strategies in the zero-sum type of what objects?
ANSWER: **game**s [or **solution space**s; accept more specific answers]

When performing this process, Yao's minimax principle can be used to reduce to the case of deterministic algorithms. On splay trees, one type of this process can be performed by defining the rank of a node to be the log of the number of nodes in the subtree it roots, and the potential to be the sum over all the ranks, or by charging each operation an identical cost, storing any extra charge as credit, and always maintaining positive credit. The solution to certain recurrence relations that arise when doing this for divide-and-conquer algorithms is given by the master theorem. One operator commonly used in this process gives the set of functions eventually dominated by some constant times the input function. For 10 points, name this process of bounding the resource cost of algorithms.
ANSWER: **algorithm analysis** [or **asymptotic analysis**; or **run-time analysis**; or **amortized analysis**; accept similar answers or answers mentioning **bound**ing some cost]

McCarthy augmented this system with update and access rules to handle memory expressions. The proof of completeness for this system uses the weakest precondition predicate transformer to reduce to the completeness of assertions. This system's while rule allows the conclusion that the loop invariant is true and the entrance condition is false after the loop ends. In this system, triples with the structure assertion, command, assertion are used to mean that if the first assertion is true and the command is executed and terminates, then the second assertion will be true, and so a separate proof of termination is needed when proving total program correctness. For 10 points, name this system that uses Hoare logic to assign meaning to programs.
ANSWER: **axiomatic semantics**

BQP algorithms can treat other BQP algorithms as these objects, by the Solovay-Kitaev theorem. By a result of Baker, Gill, and Solovay, no solution to the P vs NP problem can respect these objects.. A complexity class B is low for A if A equals itself given one of these objects for B. One of these objects with truly random output commonly replaces hash functions cryptography proofs. In the polynomial hierarchy, sigma *i* plus 1 equals NP given one of these objects for sigma *i*. Given one of these objects for some problem, any problem Turing-reducible to it can be solved, and in a many-one reduction this object is only queried once at the end. For 10 points, name these black boxes that can solve certain problems in a single step.
ANSWER: **oracle**s [or **black box**es before mentioned; or **subroutine**s]

The failure of this property for the context-free languages can be seen by applying the pumping lemma to the language with strings *s*3*s* for *s* in 0,1 star. By finding a non-deterministic log-space algorithm for deciding when one vertex in a digraph is not reachable from another, it was shown NL has this property, and also that context-sensitive languages have this property. The recursively enumerable languages don't have this property, since some of them are not decidable. Deciding whether any propositional formula is a contradiction is NP-complete if and only if NP has this property. For 10 points, the regular languages have this property, which can be shown by switching all the accepting and non-accepting states on a finite state machine.
ANSWER: **closure under complement** [or **equal to its complement**; accept equivalents]

In one structure named for these objects, the contraction-mapping theorem proves the value and policy iteration algorithms converge to a solution. Computing the shortest path through a trellis graph whose nodes are possible states yields the most likely sequence of states in models based on these objects. One of these objects is constructed whose stationary distribution is a distribution to be sampled from in a technique named for them and the Monte

Carlo method. These objects are characterized by a matrix whose rows all sum to 1, their transition matrix. For 10 points, name these discrete stochastic processes who's next state depends only on their current state.
ANSWER: **Markov chain**s

Kannan's theorem, an application of Karp-Lipton, gives one of these results for a sigma 2 problem. One tool for proving these results states that after a random restriction of some of the variables, a DNF formula can be switched to a small CNF formula with high probability. Razborov and Rudich's work on natural proofs dealt a major blow to using these results to prove P doesn't equal NP. One of these results for the parity language states it isn't in AC 0, and so can't be expressed using constant depth. For 10 points, name these results that give bounds on time complexity within a quadratic factor, since the configurations of a Turing machine can be efficiently represented by rows of Boolean gates wired together.
ANSWER: **circuit lower bound**s [prompt on partial answer]

Optimizing this result for a binomial distribution gives a factor of a KL divergence in the exponent. Applying a generalization of this result to the Doob martingale gives the method of bounded differences, and that generalization due to Azuma doesn't require independence. For a random variable X, this result is derived by applying Markov's inequality to *e* to the *t* X. This result is commonly applied to a sum of Poisson trials, and shows algorithms in BPP are efficient even though they need only be correct with probability two-thirds, since the probability that the majority of n runs is incorrect will drop off super-polynomially. For 10 points, name this result giving better tail bounds than Markov's or Chebyshev's inequalities, since they decrease exponentially.
ANSWER: **Chernoff**-Hoeffding **bound** [or **Chernoff**-Hoeffding **inequality**]

If this process can be achieved for determining when a polynomial is identically zero, it will give superpolynomial circuit lower bounds. Adleman's theorem implies this process can be achieved if we allow non-uniformity. Splitting the space in half, computing the probability of finding a desired point in each half, and recursing on the better half, is known as the method of conditional probabilities for doing this process. If P equals NP, this process is always possible because BPP is in the polynomial hierarchy, which will collapse. For 10 points, name this process possible with exponential slowdown simply by enumerating all sequences of possible coin flips, running the BPP algorithm on each one, and taking the majority answer, thus giving a deterministic algorithm.
ANSWER: **derandomization**

Simon's problem can be solved using this algorithm on *n* copies of Z 2. The last step in Kitaev's phase estimation algorithm is the inverse of this algorithm. To apply this algorithm to an input of size *n*, it is recursively applied to an input of size *n* minus 1, and then the $n^{\text{th}}$ input is subjected to *n* minus 1 controlled phase rotations and a Hadamard gate. This algorithm is applied to the first register before measurement and the computation of a continued fraction expansion in Shor's period-finding algorithm. This algorithm operates in big-oh of log squared of *n* time, exponentially faster than its classical counterpart, but the coefficients can only be determined by the probability of measuring the corresponding basis state. For 10 points, name this quantum analog of the FFT.
ANSWER: **q**uantum **F**ourier **t**ransform

Sacks constructed a set for which this property was minimal by forcing with perfect trees. Every set with a sufficiently large value for this property is the join of two smaller sets by Friedberg's inversion theorem. An operator used to create sets with a strictly greater value for this property also gives sigma 0,*n* complete sets in the arithmetical hierarchy. In a technique developed to find sets with a certain value for this property, a requirement may be injured in order to satisfy one of higher priority. Finding a recursively enumerable set with this value between 0 and 0 prime was Post's problem. This property's namesake jump can be done by taking the halting problem relative to a given set. For 10 points, name this measure of the undecidability of a problem.
ANSWER: **Turing degree**

An undirected path in one of these objects is declared active if each triple on the path is active, when using d-separation. One algorithm for sampling from these objects cycles through the variables, sampling each conditioned on the current values of variables in its Markov blanket. Another sampling algorithm for these objects only generates events consistent with the evidence, avoiding the inefficiency of rejection sampling. By summing out over variables as it goes along, variable elimination calculates any entry in the joint probability distribution represented by these objects, starting from the tables of conditional probabilities at every node. For 10 points, name these

directed graphs in which unconnected nodes are independent, and arrows between nodes can informally be thought to indicate causality.
ANSWER: **Bayes**ian **net**works [or **belief net**work; or **Markov random field**; or **graphical model**]

Given one of these objects, taking the xor of a random subset of the input bits gives a hard-core predicate. These objects, when permutations, can be used to construct a bit commitment-scheme, yielding zero-knowledge proofs for all of NP, and taking the product of the permutation type of these objects and a hard-core predicate for it gives a pseudorandom generator. These objects with an auxiliary input making their associated hard problem tractable are the trapdoor type. Candidates for these objects include exponentiation in the units of Z mod $p$ Z as well as the multiplication of large primes, since their inverses are discrete log and factoring. For 10 points, name these functions whose existence implies P doesn't equal NP, since they can be efficiently computed, but inverted with only negligible probability.
ANSWER: **one-way** functions [accept **trapdoor** functions before mentioned]

If every critical pair converges in a system, then it has the local form of this property. Well-founded induction is used to show certain systems with the local form of this property have this property in Newman's lemma. The Knuth-Bendix algorithm constructs a terminating system with this property to solve the word problem in groups. Beta-reductions in the lambda calculus have this property by the Church-Rosser theorem, and therefore each term has at most one normal form. This property can be represented by a diamond, with one term reducing to two terms that both reduce to one term. For 10 points, name this property of rewrite systems that implies that different sequences of rewrites eventually give the same result.
ANSWER: **confluence** [or **Church-Rosser property** before mentioned; or **diamond property** before mentioned]

Given one of these structures, Minkowski's theorem bounds the size until a centrally-symmetric convex set must contain a point in it. Using modular subset sum, hash functions have been constructed whose security is based on worst-case, rather than average-case, hardness of problems involving these structures. An algorithm with exponential error bound used to solve problems on these structures alternates steps of Graham-Schmidt and swapping vectors to give a nearly-orthogonal basis. The closest vector to a point or the shortest vector in these structures can be approximated using the Lenstra-Lenstra-Lovasz algorithm to get a reduced basis. For 10 points, name these integer-combinations of basis vectors, visualizable as regularly spaced points in R $n$.
ANSWER: **lattice**s