Applications of Randomization

- It is known that randomization combined with (non-trivial) algebraic techniques can lead to important applications.
- In this section, we showcase some of such techniques with respect to verification of identities.
- One such technique is called the fingerprinting technique described as follows.

Applications of Randomization

- Let U be any universe of objects and x and y be any two elements from U.
- The question we ask is, Is x = y?
- One can answer this using at least log |U| bits in a deterministic manner.
- However, consider mapping elements of U to a sparse universe V such that x and y are identical if and only if their images in V are identical, with a good chance.
- These images can be thought of as fingerprints of x and y.

Applications of Randomization

- Let us apply the above technique to matrix product verification. Let F be a field and A and B are two matrices with entries from F.
- Suppose it is claimed that $C = A \cdot B$.
- The fastest known matrix multiplication algorithm runs in time $O(n^{2.376})$.
- This algorithm is very difficult to implement, but the standard algorithms such as the Strassen's recursive algorithm takes time $O(n^{\log_2 7})$.
- So, to verify if C is indeed the product of A and B, it takes time equal to multiplying two matrices.

Applications of Randomization

- However, a simpler and efficient randomized approach exists.
- Let r be any vector with entires being 0 or 1.
- Let each element of r be chosen independently and uniformly at random.
- It is being assumed without loss of generality that 0 and 1 are the additive and multiplicative identities of the field F.

Applications of Randomization

- Compute $x = Br$, and $y = Ax$.
- Similarly, compute $z = Cr$.
- If $A \cdot B = C$ is indeed true, then y must equal z for any r.
- Also, x, y, and z can each be computed in $O(n^2)$ time.
- So, the time efficiency is established.
- It remains to see the verification efficiency.
- The following lemma argues that the verification procedure is efficient.

Applications of Randomization

- Lemma: Let A, B, and C be $n \times n$ matrices from F such that $AxB \neq C$. Then, for r chosen uniformly at random from $\{0, 1\}^n$, $Pr(ABr = Cr) \leq 1/2$.
- Proof. Consider the matrix $D := AB - C$. Since, $AB \neq C$, matrix D is not the matrix of all zeros.
- We are interested in the event that $Dr = 0$.
- Assume without loss of generality that the first row of D has a nonzero entry and all all nonzero entries in that row are before any zero entry.

Applications of Randomization

- Lemma:1 Let A, B, and C be $n \times n$ matrices from F such that AxB $\neq$ C. Then, for r chosen uniformly at random from $\{0, 1\}^n$, Pr(ABr = Cr) $\leq$ 1/2.
- Proof.Consider the first row of D and the scalar obtained by multiplying the first row of D with r.
- The result is zero if and only if: $\mathbf{r}_1 = -\frac{\sum_{i=1}^{k} D_{1i}\mathbf{r}_i}{D_{11}}$
- In the above, it is assumed that there are k > 0 nonzero elements in the first row of D.

Applications of Randomization

- Lemma:1 Let A, B, and C be $n \times n$ matrices from F such that AxB $\neq$ C. Then, for r chosen uniformly at random from $\{0, 1\}^n$, $Pr(ABr = Cr) \leq 1/2$.
- Proof (contd.) Consider the event that $(D.\mathbf{r})_1 = 0$.
- This event is a super-event of the event that Dr = 0.
- Therefore the probability of the event Dr = 0 is upper bounded by the probability of the event $(D.\mathbf{r})_1 = 0$.
- To compute the probability of the event $(D.\mathbf{r})_1 = 0$, imagine that all the choices $r_2, \cdots, r_k$ have been made.
- In that case, the right hand side is a scalar from the field F.
- The left hand size is a value uniformly chosen amongst (at least) two values in F. The required probability therefore cannot exceed 1/2.

Applications of Randomization

- Lemma:1 Let A, B, and C be $n \times n$ matrices from F such that AxB $\neq$ C. Then, for r chosen uniformly at random from $\{0, 1\}^n$, $\Pr(ABr = Cr) \leq 1/2$.
- Proof. To compute the required probability, imagine that all the choices $r_2, \cdot \cdot \cdot, r_k$ have been made.
- In that case, the right hand side (0) is a scalar from the field F.
- The left hand size ($\mathbf{r}_1$) is a value uniformly chosen amongst (at least) two values in F. The required probability therefore cannot exceed 1/2.

Applications of Randomization

- To improve the verification efficiency of the procedure, we can also use repeated independent trials.
- Let us perform t independent trials of the above procedure.
- For $AB \neq C$, the probability that the test fails in each trial is at most 1/2.
- So, in t trials, the probability that all t trials fail is at most $(1/2)^t$.
  - A failure is when indeed $AB \neq C$, and the chosen r is such that $ABr = Cr$.
- For $t = O(\log n)$, the failure probability is polynomially small