

Handout 2: Notation

Instructor: Anna Lysyanskaya

A denotes an algorithm.

$A(\cdot)$ denotes an algorithm with an input.

$A(\cdot, \cdot)$ denotes an algorithm with two inputs.

$A(x)$ is well-defined if A is a deterministic algorithm.

$A(x)$ defines a probability distribution if A is a probabilistic algorithm. More precisely, let $A'(x, R)$ be the deterministic algorithm that represents the behavior of A on input x and random tape R . The uniform distribution on R induces a probability distribution on the output of $A'(x, R)$. We call that distribution $A(x)$.

$x \leftarrow A(y)$ denotes that x is a sample from the distribution $A(x)$; it also means that x was generated by running A on input y .

$x \leftarrow F$, for a set F , means that x was selected from F uniformly at random.

We can now introduce notation that represents a sequence of experiments, for example

$$((x, y) \leftarrow A(3); z \leftarrow B(y))$$

denotes that first we ran algorithm A on input 3 to generate (x, y) , and then we ran B on input y to generate z .

We can specify a probability distribution by describing a series of experiments used to obtain elements of the distribution. For example,

$$D_k = \{x \leftarrow A(1^k); y \leftarrow B(x) : (x, y)\}$$

denotes the distribution on the values (x, y) that were obtained by first running algorithm A on input the string 1^k to obtain x , and then running $B(x)$ to obtain y .

To denote that (x, y) were obtained as a result of this series of experiments, we can write $(x, y) \leftarrow D_k$.

We can also define events of interest. For example, consider the event E that $x \neq y$. Here is how we would express this event in this notation:

$$E = (x \leftarrow A(1^k); y \leftarrow B(x) : x \neq y)$$

Equivalently, since D_k was defined earlier as shorthand for $\{x \leftarrow A(1^k); y \leftarrow B(x) : (x, y)\}$, we can write the same event as follows:

$$E = ((x, y) \leftarrow D_k : x \neq y)$$

Finally, the statement

$$\Pr[x \leftarrow A(1^k); y \leftarrow B(x) : x \neq y] = p$$

means that the probability of event E defined above (which we could also have written simply as $\Pr[E]$), is p .

A Note on Defining Experiments of Interest

As is clear from the above, we generally define experiments in terms of small computational steps. For example, suppose we are analyzing the scenario where Eve gets hold of a ciphertext that Alice sent to Bob, and we are interested in the event that Eve guesses the message correctly.

Here is an imprecise way to define this event:

$$E = (m' \leftarrow \text{Eve}(c) : m' = m)$$

The reason it is imprecise, is that it does not tell us where c and m came from. We should add that information to the description of the experiment. m comes from M , that's easy. c is trickier: c was produced by $\text{Enc}(s, m)$, where s was produced by the key generation algorithm $\text{Gen}(1^k)$, where k is the security parameter. So a better way to define the event is:

$$E = (s \leftarrow \text{Gen}(1^k); m \leftarrow M; c \leftarrow \text{Enc}(s, m); m' \leftarrow \text{Eve}(c) : m' = m)$$

But wait, that's still imprecise! Where does k come from? It's a parameter given to us "from above," the event has to be well-defined no matter what k is. So, we should give k as a parameter to E , for example by writing E_k ($E(k)$ would be OK, too):

$$E_k = (s \leftarrow \text{Gen}(1^k); m \leftarrow M; c \leftarrow \text{Enc}(s, m); m' \leftarrow \text{Eve}(c) : m' = m)$$

Different Descriptions for the Same Distribution

Note that there are different ways to describe experiments that result in the same probability distributions. For example, consider the following distributions (where \oplus denotes XOR):

$$D_1(k) = \{x \leftarrow \{0, 1\}^k; y \leftarrow \{0, 1\}^k; z = x \oplus y : (x, y, z)\}$$

$$D_2(k) = \{x \leftarrow \{0, 1\}^k; z \leftarrow \{0, 1\}^k; y = x \oplus z : (x, y, z)\}$$

These define the *same* probability distributions, because for every possible assignment (x, y, z) , its probability under $D_1(k)$ is the same as under $D_2(k)$. In other words, for all k , for all (a, b, c) ,

$$\Pr[(x, y, z) \leftarrow D_1(k) : (x, y, z) = (a, b, c)] = \Pr[(x, y, z) \leftarrow D_2(k) : (x, y, z) = (a, b, c)]$$

Let us prove that this is the case. Consider k -bit strings (a, b, c) . Let $T(a, b, c) = 1$ if $c = a \oplus b$, and 0 otherwise.

Suppose that we are sampling from distribution $D_1(k)$, so our experiment consists of drawing (x, y, z) as defined by $D_1(k)$.

$$\Pr[(x, y, z) = (a, b, c)] = \Pr[x = a \wedge y = b \wedge z = c] \quad (1)$$

$$= \Pr[x = a] \Pr[y = b \wedge z = c | x = a] \quad (2)$$

$$= \Pr[x = a] \Pr[y = b | x = a] \Pr[z = c | x = a \wedge y = b] \quad (3)$$

$$= \Pr[x = a] \Pr[y = b] \Pr[x \oplus y = c | x = a \wedge y = b] \quad (4)$$

$$= 2^{-k} 2^{-k} T(a, b, c) \quad (5)$$

where steps 2 and 3 follow by Bayes' rule, step 4 follows because we defined D_1 in such a way that x and y are chosen independently from each other; step 5 follows because both x and y are drawn uniformly from $\{0, 1\}^k$, and, conditioned on $(x = a \wedge y = b)$, we know that $x \oplus y = c$ iff $c = a \oplus b$.

Now we must show the very same probabilities for each (a, b, c) under distribution $D_2(k)$:

$$\Pr[(x, y, z) = (a, b, c)] = \Pr[x = a \wedge y = b \wedge z = c] \quad (6)$$

$$= \Pr[x = a] \Pr[z = c \wedge y = b | x = a] \quad (7)$$

$$= \Pr[x = a] \Pr[z = c | x = a] \Pr[y = b | x = a \wedge z = c] \quad (8)$$

$$= \Pr[x = a] \Pr[z = c] \Pr[x \oplus z = b | x = a \wedge z = c] \quad (9)$$

$$= 2^{-k} 2^{-k} T(a, c, b) \quad (10)$$

$$= 2^{-k} 2^{-k} T(a, b, c) \quad (11)$$

where the the first four steps follow by almost the same logic as above, and the last step is because $T(a, b, c) = T(a, c, b)$ the properties of the XOR function.

Other examples of pairs experiments resulting in the same distribution:

$$A_1(k) = \{x \leftarrow \{0, 1\}^k : x\}$$

$$A_2(k) = \{x \leftarrow \{0, 1\}^k; y \leftarrow \{0, 1\}^k : x \oplus y\}$$

Let $\pi_k : \{0, 1\}^k \mapsto \{0, 1\}^k$ be any permutation; then the following are two ways of defining the same distribution:

$$B_1(k) = \{x \leftarrow \{0, 1\}^k : x\}$$

$$B_2(k) = \{x \leftarrow \{0, 1\}^k : \pi_k(x)\}$$