

Symbols

- $A(\cdot)$: The adversary's cost function on \mathcal{X} (see Section 8.1.1). See 203–209, 211, 212, 214, 216, 219–221, 228, 231, 234, 235
- \mathbb{D} : A set of data points (see also: dataset). See 23–26, 183
- N : The number of data points in the training dataset used by a learning algorithm; i.e., $N \triangleq |\mathbb{D}^{(\text{train})}|$. See 21, 23, 25–27, 36, 38–40, 46, 47, 50, 54, 56, 183, 184, 256
- $\mathbb{D}^{(\text{train})}$: A dataset used by a training algorithm to construct or select a classifier (see also: dataset). See 21, 25, 26, 36, 39, 40, 48, 50, 107, 120, 128
- $\mathbb{D}^{(\text{eval})}$: A dataset used to evaluate a classifier (see also: dataset). See 21, 22, 25, 27, 36, 39, 40, 46, 48, 50, 51, 128
- \triangleq : Symbol used to provide a definition. See 23, 24, 26, 57, 58, 60, 107, 108, 137, 139, 141, 142, 149, 153, 204, 206, 256–259, 265, 276, 278, 279, 281, 282
- ϵ -*IMAC* : The set of objects in \mathcal{X}_f^- within a cost of $1 + \epsilon$ of the *MAC*, or any of the members of this set (see also: *MAC* (f, A)). See 204–206, 209–214, 216, 219–221, 225, 229, 231–235, 237, 251
- $f(\cdot)$: The classifier function or hypothesis learned by a training procedure $H^{(N)}$ from the dataset $\mathbb{D}^{(\text{train})}$ (see also: classifier). See 21, 24–27, 39, 40, 48–51, 54, 71, 74, 102, 120, 139, 174, 176–183, 189, 195, 196, 202–207, 209, 210, 212, 215, 217–220, 234–237, 251
- L_ϵ : The number of steps required by a binary search to achieve ϵ -optimality (see Section 8.1.3). See 205, 210–212, 214–218, 220, 221, 225, 228, 232
- MAC* (f, A) : The largest lower bound on the adversary's cost A over \mathcal{X}_f^- (see also: Equation 8.2). See 204, 206, 207, 210, 212–214, 216, 219, 221, 229, 230, 234, 235
- \mathfrak{N} : The set of natural numbers, $\{1, 2, 3, \dots\}$. See 77–79, 81, 83, 88, 137, 256, 257, 276
- \mathfrak{N}_0 : The set of all whole numbers, $\{0, 1, 2, \dots\}$. See 73, 77–79, 81, 82, 86, 256
- $\|\cdot\|$: A non-negative function defined on a vector space that is positive homogeneous and obeys the triangle inequality (see also: norm). See 145, 147, 149, 152, 153, 203, 226, 227, 257

- ℓ_p ($p > 0$): A norm on a multidimensional real-value space defined in Appendix A.1 by Equation (A.1) and denoted by $\|\cdot\|_p$. See 11, 18, 200, 203, 204, 208, 210–214, 216–218, 220, 221, 223, 225–234, 244, 245, 260, 261, 264, 265
- $m_{\mathbb{C}}(\cdot)$: A function that defines a distance metric for a convex set \mathbb{C} relative to some central element $\mathbf{x}^{(c)}$ in the interior of \mathbb{C} (see also: Minkowski metric). See 210, 211
- $N^{(h)}$: The total number of ham messages in the training dataset. See 107, 108, 111, 277–280
- $n_j^{(h)}$: The number of occurrences of the j^{th} token in training ham messages. See 107, 108, 111, 277–280
- $N^{(s)}$: The total number of spam messages in the training dataset. See 107, 108, 111, 119, 277–280
- $n_j^{(s)}$: The number of occurrences of the j^{th} token in training spam messages. See 107, 108, 111, 119, 277–280
- \mathbf{Q} : The matrix of network flow data. See 137, 138, 152
- \mathbf{R} : The routing matrix that describes the links used to route each OD flow. See 138, 142, 152
- \Re : The set of all real numbers. See 23–25, 27, 142, 256–259
- \Re_{0+} : The set of all real numbers greater than or equal to zero. See 26, 203, 211, 256, 276
- \Re_+ : The set of all real numbers greater than zero. See 27, 216, 256, 257
- \Re^D : The D -dimensional real-valued space. See 24, 139, 142, 143, 147, 202, 216, 226, 257, 259
- \mathbf{x} : A data point from the input space \mathcal{X} (see also data point). See 22–24, 138, 139, 141, 145, 147, 148, 200, 203–206, 208–211, 213, 223, 224, 226, 255
- \mathbf{x}^A : A (malicious) data point that the adversary would like to sneak past the detector. See 70, 203–206, 209–215, 217, 218, 221–223, 225, 226, 231, 233–235, 261, 264, 265
- \mathcal{X} : The input space of the data (see also: input space). See 22–25, 49, 202, 203, 206, 208, 210, 211, 224, 233, 235, 236, 259, 260
- D : The dimensionality of the input space \mathcal{X} . See 22, 23, 202–205, 212–218, 220, 223–232, 235, 237, 259
- \mathcal{X}_f^- : The negative class for the deterministic classifier f (see also: negative class). See 203–206, 208, 210–213, 219, 221–224, 226, 231, 233, 235, 236
- \mathcal{X}_f^+ : The positive class for the deterministic classifier f (see also: positive class). See 203, 205, 210–214, 216, 218, 233, 234
- y : A label from the response space \mathcal{Y} (see also: label). See 23, 26, 27, 107
- \mathcal{Y} : The response space of the data (see also response space). See 23–27, 59, 203
- \mathbb{Z} : The set of all integers. See 23, 256, 258