# Содержание

# 1 Модель вычислений

Будем рассматривать следующую задачу. Есть два участника процесса(два человека или два компьютера), которые должны совместно вычислить значение функции $f: X \times Y \to Z$, где $X, Y, Z$ некоторые конечные множества. В качестве $Z$ обычно будем рассматривать множество значений бита $\{0, 1\}$. Традиционно этих участников называют Алиса и Боб, поэтому для удобства и соответствия литературе будем называть их так же. Сложность их задачи состоит в том, что аргумент, на котором необходимо посчитать значение функции, разделен на две части: у Алисы есть только $x \in X$, а у Боба только $y \in Y$.

Однако в их распоряжении есть некий абстрактный канал связи, через который они могут передавать друг другу данные. Передача по этому каналу связи может быть дорогой(или занимать значительное время), поэтому необходимо минимизировать количество битов, передаваемых в процессе вычисления функции.

Так же предполагается, что Алиса и Боб заранее знают функцию $f$ и договариваются о протоколе - наборе соглашений о том, как и в каком порядке будет происходить обмен информацией.

**Определение 1** *Коммуникационным протоколом для вычисления некоторой функции $f: X \times Y \to Z$ называется ориентированное двоичное дерево, такое что:*

1. *Каждой **листовой** вершине ставится в соответствие некоторый элемент их $Z$.*
2. *Каждая **внутренняя** вершина помечена значением из $\{A, B\}$*
3. *Для для каждой вершины $v_i$ с пометкой $A$ задана функция $g_i: X \to \{0, 1\}$*
4. *Для для каждой вершины $v_j$ с пометкой $B$ задана функция $h_j: Y \to \{0, 1\}$*
5. *Каждому ребру приписано значение из {0, 1}, а из каждой вершины, не являющегося листом, исходит ровно одно ребро с пометкой 0 и ровно одно с пометкой 1.*

Выполнение протокола участниками вычисления начинается в корневой вершине. На каждом шаге, переход осуществляется следующим образом. Пусть пометка очередной вершины $v_i$ равна $A$. Это означает, что сейчас Алиса должна применить функцию $g_i(x)$(соответствующую вершине $v_i$) к ее значению $x$. Если результат 0, то она отсылает Бобу значение 0 и переходит по ребру с меткой 0. Аналогично с 1. Если же пометка $B$, то аналогично действовать должен Боб, применяя функцию $h_j(y)$ к его значению $y$.

Если текущая вершина это лист, то соответствующее ему значение $z \in Z$ объявляется результатом выполнения. Это отражает идею, что к этому моменту все участники расчета знают этот ответ.

**Определение 2** *Протокол вычисляет функцию* $f: X \times Y \to Z$, *если* $\forall x \in X \ \forall y \in Y$ *при движении по графу протокола по описанным правилам исполнители попадут в лист, которому соответсвует* $z = f(x, y)$.