Chapter 5

Some Reduction Statements for Games

In this chapter we consider problems, solvers, and sometimes reductions to be *systems* with natural composition operations. We denote such systems by boldface symbols like $\mathbf{S}$ or $\mathbf{W}$. These system can in this chapter be seen as abstract system objects,[1] but in Chapter 6 we explain the special case of discrete systems, which is system type usually considered in cryptography.

5.1 Basic Reduction Types

We consider two simple types of reduction functions ρ for game winners and distinguishers: reductions by attaching a (reduction) system, and reductions by multiple invocation.

5.1.1 Multiple Independent Instantiation and Cloning

We introduce two types of operations on random variables: multiple independent copies and multiple clones. These operations can be applied to probabilistic systems, understood as random variables over a set of (deterministic) systems.

Definition 5.1. For an $\mathcal{X}$-random variable X, we denote by X^q the $\mathcal{X}^q$-random variable consisting of q *independent* copies of X. More precisely, $X^q = (X_1, \ldots, X_q)$ where $X_1, \ldots, X_q$ are independent and each X_i has the same (marginal) probability distribution as X. Moreover, we denote by $\langle X \rangle$ the $\mathcal{X}^\infty$-random variable consisting of a countable number *independent* copies of X.[2]

Definition 5.2. For an $\mathcal{X}$-random variable X, we denote by $X^{[q]}$ the $\mathcal{X}^q$-random variable consisting of q *clones* of X. More precisely, $X^{[q]} = (X_1, \ldots, X_q)$ where $X_1 = \cdots = X_q$ and each X_i has the same (marginal) probability distribution as X.

Example 5.1. If X is a binary random variable with uniform distribution, then X^q is the random variable with uniform distribution over $\{0,1\}^q$, and $X^{[q]}$ is the $\{0,1\}^q$-random variable which takes on the two values $(0,0,\ldots,0)$ and $(1,1,\ldots,1)$ with probability $\frac{1}{2}$.

We will use these two concepts for the case where the random variables are probabilistic systems. If $\mathbf{S}$ is a probabilistic system, then we denote by $\mathbf{S}^q$ the parallel composition of q independent copies of $\mathbf{S}$, and by $\mathbf{S}^{[q]}$ the parallel composition of q clones of $\mathbf{S}$ which all behave identically.

5.1.2 Reductions by a Converter

A system $\mathbf{c}$ can be understood as a transformation of a winner $\mathbf{w}$ into another winner, denoted $\mathbf{wc}$, where, because of the associative law (namely, $\mathbf{w}(\mathbf{cg}) = (\mathbf{wc})\mathbf{g}$), we have

$$\omega(\mathbf{wc}, \mathbf{g}) = \omega(\mathbf{w}, \mathbf{cg}). \tag{5.1}$$

One can view a (possibly probabilistic) system $\mathbf{C}$ as a reduction function ρ mapping probabilistic winners to probabilistic winners. We denote this reduction function as $\gamma^{\mathbf{C}}$:

$$\gamma^{\mathbf{C}}: \ \mathbf{W} \mapsto \gamma^{\mathbf{C}}(\mathbf{W}) = \mathbf{WC}.$$

Using (5.1), we thus have the following trivial reduction equality:

$$\overline{\mathbf{CG}} \ = \ \overline{\mathbf{G}}\,\gamma^{\mathbf{C}}, \tag{5.2}$$

where on the left side the converter $\mathbf{C}$ and system $\mathbf{G}$ are composed to form a game, and on the right side the *functions* $\overline{\mathbf{G}}$ and $\gamma^{\mathbf{C}}$ are composed as functions.

5.1.3 Reductions by Multiple Instantiation

The second type of reduction is by mutliple invocation of a solver, for example a winner $\mathbf{W}$. The reduction function ρ mapping $\mathbf{W}$ to $\mathbf{W}^q$ is denoted as σ^q, i.e.,

$$\sigma^q: \ \mathbf{W} \mapsto \sigma^q(\mathbf{W}) = \mathbf{W}^q.$$

[1] only requiring that the composition operations we use are defined

[2] Formally, when considering random variables over $\mathcal{X}^\infty$, one leaves the realm of discrete probability theory since $\mathcal{X}^\infty$ is not countable. The formal treatment then becomes more cumbersome. However, we can think of an infinite sequence as standing for the (infinite) sequence of finite-length prefixes, which means that we consider an infinite sequence of discrete random experiments. This should not cause confusion in the rest of the course.

5.2 Random Self-Reduction

5.2.1 Performance Amplification for Games by Repetition

A natural idea for amplifying the performance of a game winner $\mathbf{W}$ for a game $\mathbf{G}$ is to repeat it independently for the same instance of the problem, hoping that one of the attempts will be successful. We saw in Exercise 4.1 that performance amplification by repetition is not guaranteed to work, i.e., the performance is not necessarily greater than for a single attempt. Nevertheless, repetition is one of the most important reduction techniques. However, as such, it only works for independent instances (see below).

Let $\psi_q(x)$ denote the probability that among q independent binary random variables, each of which is 1 with probability x, at least one of them is 1. Moreover, let $\chi_q : [0,1] \to [0,1]$ denote the inverse function, i.e., $\chi_q = \psi_q^{-1}$:

Definition 5.3. We define

$$\psi_q(x) \;:=\; 1-(1-x)^q$$

and the inverse function

$$\chi_q(x) \;:=\; 1-(1-x)^{1/q}.$$

We note that $\chi_q \circ \psi_q = \mathsf{id}$, the identity function. We also note (using $1+x \le e^x$ for all x) that $\psi_q(x) \;\ge\; 1-e^{-xq}$ and hence that

$$\chi_q(x) \;\le\; \frac{-\ln(1-x)}{q}. \tag{5.3}$$

Note that $\mathbf{G}^q$ is a multi-game and recall that $\mathbf{G}^{q\vee}$ denotes the game consisting of winning one of the q independent copies of the game $\mathbf{G}$. Equation (5.4) of the following lemma states that for any winner $\mathbf{W}$ for $\mathbf{G}$, the performance of $\mathbf{W}^q$ for the problem $\mathbf{G}^{q\vee}$ is (strongly) amplified by the function ψ_q.

Lemma 5.1. *For any game* $\mathbf{G}$ *and any* q *we have*

$$\psi_q\,\overline{\mathbf{G}} \;=\; \overline{\mathbf{G}^{q\vee}}\,\sigma^q. \tag{5.4}$$

Proof. Equation (5.4) (of functions) can also be written as

$$\forall \mathbf{W} \quad \psi_q\,\overline{\mathbf{G}}\,(\mathbf{W}) \;=\; \overline{\mathbf{G}^{q\vee}}\,(\mathbf{W}^q). \tag{5.5}$$

If $\mathbf{W}^q$ is connected to $\mathbf{G}^q$, this corresponds to q independent copies of $\mathbf{W}$ connected to $\mathbf{G}$, i.e., $\mathbf{W}^q\mathbf{G}^q = (\mathbf{W}\mathbf{G})^q$. The q winning events are hence independent, and each occurs with probability $\overline{\mathbf{G}}\,(\mathbf{W})$. Hence their logical OR occurs with probability $\psi_q(\overline{\mathbf{G}}\,(\mathbf{W}))$. This corresponds to (5.5). □

The above reduction only works for independent copies of $\mathbf{G}$, i.e., for $\mathbf{G}^{q\vee}$. What one actually wants is to amplify the performance for a *given* instance $\mathbf{g}$ of a game. In order for this to work, a game must have two properties: it must be clonable and it must be self-reducible, two concepts discussed in the next two subsections.

5.2.2 Cloning Game Systems

In many reductions one needs multiple copies of the *same* instance of a game. For a search problem it is obvious what it means to copy an instance if it is assumed to be represented as a bit-string. In contrast, for general (interactive) games, which can be systems with state, it may not even be possible to repeat the game in the same initial configuration. This is possible only if one can *clone* a given instance of a game.

Definition 5.4. A (game) system $\mathbf{G}$ is called *q-clonable by system* $\mathbf{K}$ if[3]

$$\mathbf{KG} \;=\; \mathbf{G}^{[q]\vee}.$$

This definition implies

$$\overline{\mathbf{KG}} \;=\; \overline{\mathbf{G}^{[q]\vee}}.$$

A cloning system $\mathbf{K}$ can typically be defined as emulating q copies of $\mathbf{G}$ at the left interface, interacting with a winner (designed for the game $\mathbf{G}^{[q]\vee}$), checking any obtained solution (for one of the subgames) for correctness, and then forwarding a correct solution, if there is any, at the right interface to $\mathbf{G}$. If $\mathbf{G}$ is won, this means that one of the clones of $\mathbf{G}$ was won, i.e., that $\mathbf{G}^{[q]\vee}$ is won. Hence we have

$$\overline{\mathbf{G}^{[q]\vee}} \;=\; \overline{\mathbf{G}}\,\gamma^{\mathbf{K}}. \tag{5.6}$$

Exercise 5.1. Explain why the MAC-game does not seem to be clonable by an efficient system. What about the MAC game if the adversary has to forge the MAC for a fixed message, say for the all-zero string of a certain length?

5.2.3 Random Self-Reduction of Games

Definition 5.5. A probabilistic game $\mathbf{G}$ defined as a probability distribution over a set $\mathcal{G}$ (the instance set) is called *random self-reducible* by system $\mathbf{R}$ if

$$\forall \mathbf{g} \in \mathcal{G} : \quad \mathbf{R}\mathbf{g} \;=\; \mathbf{G}.$$

The following lemma states that for a random game $\mathbf{G}$ that is random self-reducible by $\mathbf{R}$, an average-case winner can be transformed by the reduction function $\gamma^{\mathbf{R}}$ into a worst-case winner with the same success probability.

[3] Note that $\mathbf{K}$ depends on q, but to simplify the notation we do not make this explicit.

Lemma 5.2. *If* $\mathbf{G}$ *is random self-reducible by* $\mathbf{R}$*, then*

$$\overline{\mathbf{G}} \;=\; \overline{\mathcal{G}}\,\gamma^{\mathbf{R}}.$$

Proof. For every instance $\mathbf{g} \in \mathcal{G}$ and every winner $\mathbf{W}$ we have $\overline{\mathbf{g}}\,(\mathbf{WR}) = \overline{\mathbf{G}}\,(\mathbf{W})$, hence

$$\overline{\mathbf{G}}\,(\mathbf{W}) \;=\; \inf_{\mathbf{g}\in\mathcal{G}} \overline{\mathbf{g}}\,(\mathbf{WR}) \;=\; \overline{\mathcal{G}}\,(\mathbf{WR}) \;=\; \overline{\mathcal{G}}\,\gamma^{\mathbf{R}}\,(\mathbf{W}).$$

□

5.2.4 Combining Clonability and Random Self-Reduction

We now show that random self-reducibility and clonability of a game $\mathbf{G}$ can be used to amplify the performance of a winner.

Theorem 5.3. *If game* $\mathbf{G}$ *is random self-reducible by* $\mathbf{R}$ *and q-clonable by* $\mathbf{K}$*, then*

$$\psi_q\,\overline{\mathbf{G}} \;=\; \overline{\mathbf{G}}\,\gamma^{\mathbf{K}}\,\sigma^q\,\gamma^{\mathbf{R}}.$$

Proof. If $\mathbf{G}$ is random self-reducible by $\mathbf{R}$, then

$$\mathbf{R}^q\mathbf{G}^{[q]} \;=\; \mathbf{G}^q$$

and hence also

$$\overline{\mathbf{G}^{[q]\vee}}\;\gamma^{\mathbf{R}^q} \;=\; \overline{\mathbf{R}^q\mathbf{G}^{[q]\vee}} \;=\; \overline{\mathbf{G}^{q\vee}}. \qquad (5.7)$$

Using clonability of $\mathbf{G}$ via $\mathbf{K}$ and (5.6), as well as equations (5.7) and (5.4), we obtain

$$\begin{aligned}
\psi_q\,\overline{\mathbf{G}} \;&=\; \overline{\mathbf{G}^{q\vee}}\;\sigma^q\\
&=\; \overline{\mathbf{G}^{[q]\vee}}\;\gamma^{\mathbf{R}^q}\,\sigma^q\\
&=\; \overline{\mathbf{G}}\;\gamma^{\mathbf{K}}\,\gamma^{\mathbf{R}^q}\,\sigma^q\\
&=\; \overline{\mathbf{G}}\;\gamma^{\mathbf{K}}\,\sigma^q\,\gamma^{\mathbf{R}}.
\end{aligned}$$

The last step follows from $\gamma^{\mathbf{R}^q}\sigma^q \;=\; \sigma^q\,\gamma^{\mathbf{R}}$ since

$$\gamma^{\mathbf{R}^q}\,\sigma^q(\mathbf{W}) \;=\; \gamma^{\mathbf{R}^q}\,\mathbf{W}^q \;=\; \mathbf{W}^q\mathbf{R}^q \;=\; (\mathbf{WR})^q \;=\; \sigma^q(\mathbf{WR}) \;=\; \sigma^q\,\gamma^{\mathbf{R}}(\mathbf{W}).$$

□

The reduction function in Theorem 5.3 is $\gamma^{\mathbf{K}}\,\sigma^q\,\gamma^{\mathbf{R}}$, and hence the theorem states that for any winner $\mathbf{W}$ for $\mathbf{G}$, the winning probability of $\gamma^{\mathbf{K}}\,\sigma^q\,\gamma^{\mathbf{R}}(\mathbf{W}) = \mathbf{W}^q\mathbf{R}^q\mathbf{K}$ for $\mathbf{G}$ is strongly amplified, namely by the function ψ_q.

We briefly discuss the consequences of this result in terms of asymptotic statements. If the reduction function $\gamma^{\mathbf{K}}\,\sigma^q\,\gamma^{\mathbf{R}}$ is considered as preserving the efficiency of a winner $\mathbf{W}$, then if no efficient winner can win $\mathbf{G}$ with probability p, this implies that no efficient winner can win $\mathbf{G}$ with probability $\chi_q(p)$. In view of (5.3), this probability $\chi_q(p)$ can be made arbitrarily small, even for p very close to 1, by an appropriate choice of q. There is a trade-off: increasing the parameter q makes the upper bound of the theorem stronger (i.e., smaller), but on the other hand makes $\mathbf{W}^q\mathbf{R}^q\mathbf{K}$ less efficient.

From this statement one can obtain the following asymptotic statement as a corollary: If it is computationally hard to solve $\mathbf{G}$ with probability more than β (for any β, e.g. $\beta = 0.999$) then it is even hard to achieve any non-negligible success probability. In other words, a weak intractability assumption provably implies a strong one.

Example 5.2. The DL problem in group $\mathcal{H} = \langle h\rangle$ is random self-reducible and efficiently clonable. The system $\mathbf{R}$ takes an instance $y = h^x$ as input (at the right interface), chooses $r \in \{0,\ldots,|\mathcal{H}|-1\}$ at random, outputs $y' = y\cdot h^r$ at the left interface, and for the (attempted) solution w at the left interface outputs $w - r$ at the right interface.

This randomizer system $\mathbf{R}$ is correct since the value h^r and hence also $y' = y\cdot h^r$ is a uniformly random group element and because w is a solution for y' if and only if $w - r$ is a solution for y.

Exercise 5.2. Show that the CDH problem is random self-reducible.

5.3 Hardness Amplification for Games

5.3.1 Combining Several Games

One can combine several independent games $\mathbf{G}_1,\ldots,\mathbf{G}_k$ into a single game by requesting that *all* games be won. Recall Definition 4.6 and that this game is denotes as

$$[\mathbf{G}_1,\ldots,\mathbf{G}_k]^\wedge.$$

Example 5.3. Recall the function inversion game for a function f. Given several functions (which could be the same), one can define the combined game of inverting all the functions for independent uniformly random inputs. This is equivalent to inverting the direct product of all functions on a uniformly random input.

5.3.2 The Goal of Hardness Amplification

We want to investigate the following apparently simple statement:

> *If one cannot win game* $\mathbf{G}$ *with probability better than* β *and one cannot win game* $\mathbf{H}$ *with probability better than* γ*, then, if* $\mathbf{G}$ *and* $\mathbf{H}$ *are independent, one cannot win both games with probability better than* $\beta\gamma$*.*

This statement is trivially true for games corresponding to search problems if we consider computationally unbounded winners.[4] If β is the probability that $\mathbf{G}$ can be won and γ is the probability that $\mathbf{H}$ can be won, then $\beta\gamma$ is the probability that both games can be won.

However, if we consider *computationally bounded* winners, things are substantially more involved. One can say that $\mathbf{G}$ is hard above β (denoted $\mathit{hard}(\mathbf{G},\beta)$, and possibly defined precisely later), if no efficient winner has a winning probability of non-negligibly more than β. Then the statement we want to prove is: *If* $\mathbf{G}$ *is hard above* β *and* $\mathbf{H}$ *is hard above* γ*, then* $[\mathbf{G},\mathbf{H}]^\wedge$ *is hard above* $\beta\gamma$*:*

$$\mathit{hard}(\mathbf{G},\beta)\ \wedge\ \mathit{hard}(\mathbf{H},\gamma)\ \Longrightarrow\ \mathit{hard}([\mathbf{G},\mathbf{H}]^\wedge,\beta\gamma).$$

The proof of this apparently simple statement is not as easy as it may seem, and it holds only for clonable games. One has to be careful about what this statement means, i.e., what needs to be proved. It means the following:

> *If there exists an efficient* $\beta\gamma$*-winner for* $[\mathbf{G},\mathbf{H}]^\wedge$*, then there exists either an efficient* β*-winner for* $\mathbf{G}$ or *an efficient* γ*-winner for* $\mathbf{H}$.

A constructive proof of this statement shows how one can construct, given *any* efficient $\beta\gamma$-winner $\mathbf{W}$ for $[\mathbf{G},\mathbf{H}]^\wedge$, either an efficient β-winner for $\mathbf{G}$ or an efficient γ-winner for $\mathbf{H}$.

Before we state the theorem and the proof, we need a lemma.

5.3.3 A Lemma on Multi-Argument $[0,1]$-Valued Functions

In this section we state a general lemma on functions $\mathcal{X}\to[0,1]$. Such a function, say $\mu:\mathcal{X}\to[0,1]$, can be interpreted as follows. We consider a random experiment in which an event $\mathcal{E}$ is defined and where the values $x\in\mathcal{X}$ correspond to (mutually exclusive) cases that can occur. Then $\mu(x)$ can be interpreted as the probability of the event $\mathcal{E}$ in case x. In our application, x will be an instance of a game and $\mathcal{E}$ will be the event that a given winner W wins this game instance.

We now consider the case where $\mathcal{X}=\mathcal{S}\times\mathcal{T}$, i.e., a function $\mu:\mathcal{S}\times\mathcal{T}\to[0,1]$, as well as probability distributions P_S on $\mathcal{S}$ and P_T on $\mathcal{T}$, defining (independent) random variables S and T, respectively. Moreover, we define $\mu_1(s)$ as the average of μ when $S=s$, i.e.,

$$\mu_1(s)\ =\ \mathsf{E}_T[\mu(s,T)]\ =\ \sum_{t\in\mathcal{T}}\mathsf{P}_T(t)\ \mu(s,t)$$

and, similarly, $\mu_2(t)$ as the average of μ when $T=t$:

$$\mu_2(t)\ =\ \mathsf{E}_S[\mu(S,t)]\ =\ \sum_{s\in\mathcal{S}}\mathsf{P}_S(s)\ \mu(s,t).$$

[4] For general games it is also true, but the statement is not trivial (see U. Maurer, K. Pietrzak, and R. Renner, *Indistinguishability amplification*, Proc. CRYPTO 2007).

Note that μ_1 is a function $\mathcal{S}\to[0,1]$ and μ_2 is a function $\mathcal{T}\to[0,1]$. We have

$$\mathsf{E}_{ST}[\mu(S,T)]\ =\ \mathsf{E}_S[\mu_1(S)]\ =\ \mathsf{E}_T[\mu_2(T)].$$

For some $\epsilon\ge 0$ we are interested in the probability (over S) that $\mu_1(S)\ge\epsilon$, i.e., in

$$\mathsf{Pr}^S\left(\mu_1(S)\ge\epsilon\right),$$

and, similarly, for some ϵ', in the probability (over T) that $\mu_2(T)\ge\epsilon'$

$$\mathsf{Pr}^T\left(\mu_2(T)\ge\epsilon'\right).$$

Lemma 5.4. *For every* $0\le\epsilon,\epsilon'<1$ *and every function* $\mu:\mathcal{S}\times\mathcal{T}\to[0,1]$*,*

$$\mathsf{E}_{ST}[\mu(S,T)]\ \le\ \mathsf{Pr}^S\left(\mu_1(S)\ge\epsilon\right)\ \cdot\ \mathsf{Pr}^T\left(\mu_2(T)\ge\epsilon'\right)+\epsilon+\epsilon'.$$

Proof. Let

$$\mathcal{S}'=\{s:\ \mu_1(s)\ge\epsilon\}\qquad\text{and}\qquad\mathcal{T}'=\{t:\ \mu_2(t)\ge\epsilon'\},$$

as well as $\mathcal{S}''=\mathcal{S}\setminus\mathcal{S}'$ and $\mathcal{T}''=\mathcal{T}\setminus\mathcal{T}'$. Using

$$\mathcal{S}\times\mathcal{T}\ =\ (\mathcal{S}'\times\mathcal{T}')\ \cup\ (\mathcal{S}''\times\mathcal{T})\ \cup\ (\mathcal{S}\times\mathcal{T}'') \tag{5.8}$$

we can bound

$$\mathsf{E}_{ST}[\mu(S,T)]=\sum_{(s,t)\in\mathcal{S}\times\mathcal{T}}\mathsf{P}_S(s)\ \mathsf{P}_T(t)\ \mu(s,t) \tag{5.9}$$

as the sum of three terms corresponding to the summations over the three sets on the right side of (5.8).[5] Since $\mu(s,t)\le 1$, the first of these terms can be bounded as

$$\sum_{(s,t)\in\mathcal{S}'\times\mathcal{T}'}\mathsf{P}_S(s)\ \mathsf{P}_T(t)\ \mu(s,t)\ \le\ \underbrace{\mathsf{Pr}^S(S\in\mathcal{S}')}_{=\mathsf{Pr}^S\left(\mu_1(S)\ge\epsilon\right)}\ \cdot\ \underbrace{\mathsf{Pr}^T(T\in\mathcal{T}')}_{=\mathsf{Pr}^T\left(\mu_2(T)\ge\epsilon'\right)}\ . \tag{5.10}$$

Moreover, since $\mu_1(s)<\epsilon$ for $s\in\mathcal{S}''$, we have

$$\begin{aligned}\sum_{(s,t)\in\mathcal{S}''\times\mathcal{T}}\mathsf{P}_S(s)\ \mathsf{P}_T(t)\ \mu(s,t)\quad &=\quad\sum_{s\in\mathcal{S}''}\mathsf{P}_S(s)\underbrace{\sum_{t\in\mathcal{T}}\mathsf{P}_T(t)\mu(s,t)}_{=\mu_1(s)}\\ &\le\quad\mathsf{Pr}^S(S\in\mathcal{S}'')\cdot\epsilon\\ &\le\quad\epsilon\end{aligned} \tag{5.11}$$

and, analogously,

$$\sum_{(s,t)\in\mathcal{S}\times\mathcal{T}''}\mathsf{P}_S(s)\ \mathsf{P}_T(t)\ \mu(s,t)\ \le\ \mathsf{Pr}^T(T\in\mathcal{T}'')\cdot\epsilon'\ \le\ \epsilon'. \tag{5.12}$$

Combining equations (5.8) to (5.12) completes the proof. □

[5] This is best illustrated in a rectangular figure (see lecture).

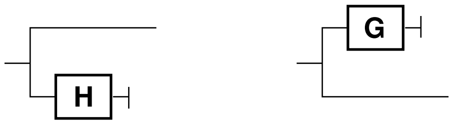

Figure 5.1: The systemss $\underline{\mathbf{H}}$ (left) and $\underline{\mathbf{G}}$ (right). The system $\underline{\mathbf{H}}$ emulates $\mathbf{H}$, connects to a system (say $\mathbf{S}$) at the right interface, and provides an interface to both systems, $\mathbf{H}$ and $\mathbf{S}$, at the left interface. The output at the right interface of $\mathbf{H}$ is ignored. $\underline{\mathbf{G}}$ is defined analogously.

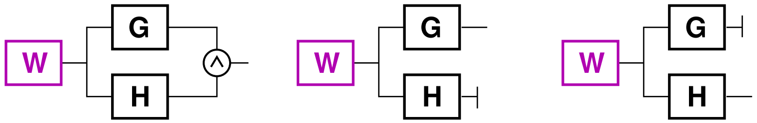

Figure 5.2: The winner $\mathbf{W}$ connected to game $[\mathbf{G},\mathbf{H}]^\wedge$ (left), the winner $\mathbf{W}\underline{\mathbf{H}}$ connected to game $\mathbf{G}$ (middle), and the winner $\mathbf{W}\underline{\mathbf{G}}$ connected to game $\mathbf{H}$ (right).

5.3.4 Hardness Amplification for Two Instances

We consider the problem of winning two independent games $\mathbf{G}$ and $\mathbf{H}$, i.e., we consider the game $[\mathbf{G},\mathbf{H}]^\wedge$ and a winner $\mathbf{W}$ for this game. We assume that $\mathbf{G}$ and $\mathbf{H}$ are clonable by $\mathbf{K}$ and by $\mathbf{L}$, respectively.

Definition 5.6. Let $\underline{\mathbf{H}}$ and $\underline{\mathbf{G}}$ be the systems shown in Figure 5.1.

The idea behind this definition is as follows (see also Figure 5.2). We want to consider the game consisting of $\mathbf{G}$ and $\mathbf{H}$, but where $\mathbf{H}$'s winning bit is ignored (rather than ANDed with $\mathbf{G}$'s winning bit). In other words, while a winner $\mathbf{W}$ "plays" with both games $\mathbf{G}$ and $\mathbf{H}$, the game we consider, which can be written as $\underline{\mathbf{H}}\mathbf{G}$, is won already if $\mathbf{G}$ alone is won. (Note that this is *not* the game $\mathbf{G}$.) Clearly, a winner $\mathbf{W}$ winning game $[\mathbf{G},\mathbf{H}]^\wedge$ also wins game $\underline{\mathbf{H}}\mathbf{G}$, i.e., winner $\mathbf{W}\underline{\mathbf{H}}$ wins game $\mathbf{G}$. More precisely, we have the logical implication

$$\omega(\mathbf{w},[\mathbf{g},\mathbf{h}]^\wedge) \;\to\; \omega(\mathbf{w},\underline{\mathbf{h}}\mathbf{g})$$

for all $\mathbf{g}\in\mathcal{G}$, $\mathbf{h}\in\mathcal{H}$, and $\mathbf{w}\in\mathcal{W}$, which implies

$$\overline{[\mathbf{g},\mathbf{h}]^\wedge}\,(\mathbf{w}) \;\le\; \overline{\underline{\mathbf{h}}\mathbf{g}}\,(\mathbf{w}) \;=\; \overline{\mathbf{g}}\,(\mathbf{w}\underline{\mathbf{h}}). \tag{5.13}$$

Since this inequality holds for all arguments, it also holds on avergage, i.e., we have for example, for every $\mathbf{g}\in\mathcal{G}$,

$$\overline{[\mathbf{g},\mathbf{H}]^\wedge}\,(\mathbf{W}) \;\le\; \overline{\mathbf{g}}\,(\mathbf{W}\underline{\mathbf{H}}). \tag{5.14}$$

To make use of Lemma 5.4, we let $\mathcal{S}=\mathcal{G}$ and $\mathcal{T}=\mathcal{H}$ be the set of instances of game $\mathbf{G}$ and of game $\mathbf{H}$, respectively. Moreover we define, for a given (in the following fixed) α-solver $\mathbf{W}$ for $[\mathbf{G},\mathbf{H}]^\wedge$, the function $\mu:\mathcal{G}\times\mathcal{H}\to[0,1]$ as follows:

$$\mu(\mathbf{g},\mathbf{h}) \;:=\; \overline{[\mathbf{g},\mathbf{h}]^\wedge}\,(\mathbf{W}),$$

i.e., $\mu(\mathbf{g},\mathbf{h})$ is the success probability of $\mathbf{W}$ for the instance $[\mathbf{g},\mathbf{h}]^\wedge$. By definition of probabilistic games we have

$$\mathsf{E}_{\mathbf{GH}}[\mu(\mathbf{G},\mathbf{H})] \;=\; \overline{[\mathbf{G},\mathbf{H}]^\wedge}\,(\mathbf{W}). \tag{5.15}$$

Then $\mu_1(\mathbf{g})=\mathsf{E}_{\mathbf{H}}[\mu(\mathbf{g},\mathbf{H})]$ denotes $\mathbf{W}$'s success probability, given that $\mathbf{G}=\mathbf{g}$. Thus we have

$$\begin{aligned}\mu_1(\mathbf{g}) &= \mathsf{E}_{\mathbf{H}}\big[\mu(\mathbf{g},\mathbf{H})\big]\\ &= \mathsf{E}_{\mathbf{H}}\big[\overline{[\mathbf{g},\mathbf{H}]^\wedge}\,(\mathbf{W})\big]\\ &\le \mathsf{E}_{\mathbf{H}}\big[\overline{\mathbf{g}}\,(\mathbf{W}\underline{\mathbf{H}})\big]\\ &= \overline{\mathbf{g}}\,(\mathbf{W}\underline{\mathbf{H}}),\end{aligned} \tag{5.16}$$

where the inequality follows from inequality (5.14) and the last step corresponds to the fact that (by Definition 4.5) the performance of a probabilistic winner (here $\mathbf{W}\underline{\mathbf{H}}$) is the expected value of the winning probability over the winner's randomness. Similarly, $\mu_2(\mathbf{h})=\mathsf{E}_{\mathbf{G}}[\mu(\mathbf{G},\mathbf{h})]$ denotes $\mathbf{W}$'s success probability, given that $\mathbf{H}=\mathbf{h}$, and we have

$$\mu_2(\mathbf{h}) \;\le\; \overline{\mathbf{h}}\,(\mathbf{W}\underline{\mathbf{G}}). \tag{5.17}$$

Let

$$A := \mathsf{Pr}^{\mathbf{G}}\big(\mu_1(\mathbf{G})\ge\epsilon\big) \tag{5.18}$$

and

$$B := \mathsf{Pr}^{\mathbf{H}}\big(\mu_2(\mathbf{H})\ge\epsilon'\big). \tag{5.19}$$

Lemma 5.4 and equation (5.15) imply that

$$\overline{[\mathbf{G},\mathbf{H}]^\wedge}\,(\mathbf{W}) \;\le\; AB+\epsilon+\epsilon'. \tag{5.20}$$

Equation (5.16), namely $\overline{\mathbf{g}}\,(\mathbf{W}\underline{\mathbf{H}})\ \ge\ \mu_1(\mathbf{g})$, states that, for every game instance $\mathbf{g}\in\mathcal{G}$, the winner $\mathbf{W}\underline{\mathbf{H}}$ has success probability at least $\mu_1(\mathbf{g})$. Thus, according to (5.18), with probability at least A (over instances $\mathbf{g}$ of $\mathbf{G}$), the success probability of $\mathbf{W}\underline{\mathbf{H}}$ is at least ϵ, i.e., $\overline{\mathbf{g}}\,(\mathbf{W}\underline{\mathbf{H}})\ge\epsilon$. Therefore, the q-fold winner $(\mathbf{W}\underline{\mathbf{H}})^q=\mathbf{W}^q\underline{\mathbf{H}}^q$ has success probability at least $A\cdot\psi_q(\epsilon)$ in winning game $\mathbf{G}^{[q]\vee}$ (see Definition 5.3).[6] Thus, for q large enough such that

$$\psi_q(\epsilon) \;\ge\; 1/\sqrt{1+\delta} \tag{5.21}$$

[6] In this argument we ignore that contribution to the success probability of the instances $\mathbf{g}$ for which $\overline{\mathbf{g}}\,(\mathbf{W}\underline{\mathbf{H}})<\epsilon$.

holds, we obtain

$$\overline{\mathbf{G}}\,(\mathbf{W}^q\underline{\mathbf{H}}^q\mathbf{K}) \;=\; \overline{\mathbf{G}^{[q]^\vee}}\,(\mathbf{W}^q\underline{\mathbf{H}}^q) \;\geq\; A\cdot\psi_q(\epsilon) \;\geq\; A/\sqrt{1+\delta}, \tag{5.22}$$

where in the first step we have used the fact that $\mathbf{G}$ is clonable by $\mathbf{K}$, i.e., $\overline{\mathbf{G}^{[q]^\vee}} = \overline{\mathbf{KG}} = \overline{\mathbf{G}}\,\gamma^{\mathbf{K}}$. Similarly, using $\overline{\mathbf{H}^{[q']^\vee}} = \overline{\mathbf{LH}} = \overline{\mathbf{H}}\,\gamma^{\mathbf{L}}$ and assuming that q' is large enough such that

$$\psi_q(\epsilon') \;\geq\; 1/\sqrt{1+\delta}, \tag{5.23}$$

we obtain

$$\overline{\mathbf{H}}\,(\mathbf{W}^{q'}\underline{\mathbf{G}}^{q'}\mathbf{L}) \;\geq\; B\cdot\psi_{q'}(\epsilon') \;\geq\; B/\sqrt{1+\delta}. \tag{5.24}$$

Using equations (5.22) and (5.24) we obtain

$$AB \;\leq\; (1+\delta)\cdot\overline{\mathbf{G}}\,(\mathbf{W}^q\underline{\mathbf{H}}^q\mathbf{K})\cdot\overline{\mathbf{H}}\,(\mathbf{W}^{q'}\underline{\mathbf{G}}^{q'}\mathbf{L}).$$

We can now let $\epsilon = \epsilon' = \delta'/2$ and choose q and q' large enough so that (5.21) and (5.23) are satisfied, which is the case (as one sees after a short calculation) for

$$q \;=\; q' \;\approx\; \frac{2\,\ln(2/\delta)}{\delta'}. \tag{5.25}$$

Using equation 5.20 we have thus proved the following theorem. Recall the notion of a generalized reduction of Section 4.5.5.

Theorem 5.5. *If $\mathbf{G}$ and $\mathbf{H}$ are clonable by $\mathbf{K}$ and $\mathbf{L}$, respectively, then for any $\delta, \delta' > 0$ we have the generalized reduction*

$$\overline{[\mathbf{G},\mathbf{H}]^\wedge} \;\leq\; \lambda\,(\overline{\mathbf{G}}\,,\overline{\mathbf{H}}\,)\,[\rho_1,\rho_2]$$

for

$$\lambda(x,y) \;:=\; (1+\delta)xy+\delta'$$

for $\rho_1(\mathbf{W}) = \mathbf{W}^q\underline{\mathbf{H}}^q\mathbf{K}$ and $\rho_2(\mathbf{W}) = \mathbf{W}^{q'}\underline{\mathbf{G}}^{q'}\mathbf{L}$, where q and q' are as described.

The theorem has two parameters, δ and δ', which one wants to choose as small as possible. Examining (5.25), we note that δ' is the more critical parameter since q and q' are proportional to its inverse, while the dependence of q and q' on δ is only logarithmic.

5.3.5 Hardness Amplification for Many Instances

Hardness amplification can be generalized from $k = 2$ to a general number k of games, i.e., to the game $[\mathbf{G}_1,\ldots,\mathbf{G}_k]^\wedge$. Lemma 5.4 can be generalized as follows, where for simplicity we let all ϵ's be equal.

Lemma 5.6. *For any function $\mu : \mathcal{S}_1\times\cdots\times\mathcal{S}_k \to [0,1]$ we have*

$$\mathsf{E}_{S_1\cdots S_k}[\mu(S_1,\ldots,S_k)] \;\leq\; \prod_{i=1}^{k}\mathsf{Pr}^{S_i}\left(\mathsf{E}_{S_1\cdots S_{i-1}S_{i+1}\cdots S_k}[\mu(S_1,\ldots,S_k)]\geq\epsilon\right)+k\epsilon.$$

Proof. Left as an exercise. □

Theorem 5.5 can now be generalized to the game $[\mathbf{G}_1,\ldots,\mathbf{G}_k]^\wedge$. To state the theorem is left as an exercise.

We are now interested in the special case where all the games $\mathbf{G}_i$ are identical, i.e., we consider the game $\mathbf{G}^{k^\wedge}$ consisting of solving k independent instances of $\mathbf{G}$ simultaneously. We leave as an exercise to prove the following theorem, where ρ must be an appropriately defined reduction which invokes an appropriate number q of independent copies of a winner for $\mathbf{G}^{k^\wedge}$.

Theorem 5.7. *For any $k\in\mathbb{N}$, any $\delta,\delta' > 0$ and any clonable (by $\mathbf{K}$) game $\mathbf{G}$ we have*

$$\overline{\mathbf{G}^{k^\wedge}} \;\leq\; \lambda\,\overline{\mathbf{G}}\;\,\rho$$

for $\lambda(x) = (1+\delta)x^k+\delta'$.

The theorem can be shown to imply

$$\mathit{hard}(\mathbf{G},\beta) \;\Longrightarrow\; \mathit{hard}(\mathbf{G}^{k^\wedge},\beta^k).$$

This is a hardness amplification statement because k independent copies of $\mathbf{G}$ are much harder to solve than a single copy of $\mathbf{G}$.