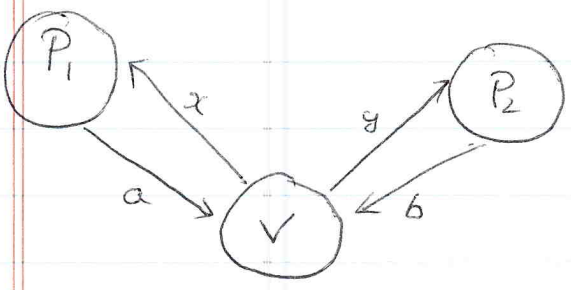
Parallel Repetition Theorem

Game G



$V(x,y,a,b) \stackrel{?}{=} 1$

V chooses $(x,y) \leftarrow (X,Y)$
V sends x to P_1, y to P_2
P_1 replies w/ a
P_2 replies w/ b
V accepts if "$V(x,y,a,b)=1$"

P_1, P_2 cannot communicate once protocol has begun, but can share randomness R before protocol begins.

Provers Strategy

$\pi_1 : X \times R \to A$; $\pi_2 : Y \times R \to B$.

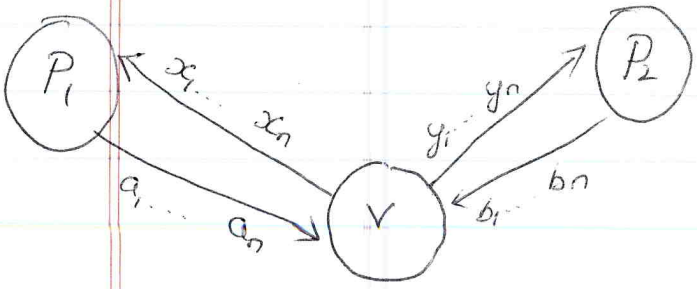
Value of Game ($\omega(G)$)

$$\omega(G) = \max_{\pi_1,\pi_2} \Pr_{\substack{(x,y)\leftarrow(X,Y) \\ r \leftarrow R}} \left[V(x,y,\pi_1(x,r),\pi_2(y,r)) = 1 \right]$$

---

n-repeated game G^n

G^n



$\forall i,\ V(x_i,y_i,a_i,b_i) = 1$

V chooses $(x_1,y_1),(x_2,y_2)\ldots(x_n,y_n)$ independently from (X,Y)
V sends $\begin{cases} (x_1 \ldots x_n) \text{ to } P_1 \\ (y_1 \ldots y_n) \text{ to } P_2 \end{cases}$
P_1 replies w/ $a_1 \ldots a_n$
P_2 replies w/ $b_1 \ldots b_n$
V accepts if $\forall i,\ V(x_i,y_i,a_i,b_i)=1$

What is $\omega(G^n)$?

Fortnow-Rompel-Spaer '88: (proposed parallel repetition
"Claim": $\omega(G^n) = (\omega(G))^n$

Claim is false
Counterexample (due to Fortnow & Then Feige)

Game F

- V chooses $b_0, b_1 \leftarrow_R \{0,1\}$ (2 random bits)
- V sends $\begin{cases} b_0 & \text{to Prover } P_0 \\ b_1 & \text{to Prover } P_1 \end{cases}$
- Provers P_i respond w/ (c_i, d_i)
- Verifier accepts if

$$\begin{cases} (c_0, d_0) = (c_1, d_1) = (c, d), \text{ say} \\ d = b_c \end{cases}$$

(ie, Provers replies with "Prover P_{c_i} got bit d_i"
Verifier accepts only if both provers respond identically & furthermore, it matches w/ actual outcome)

Clearly, $\omega(F) = 1/2$.
What about $\omega(F^2)$?
Suppose Provers respond as

$P_1 \rightarrow (0, b_0^{(1)}), (1, b_0^{(1)})$
$P_2 \rightarrow (0, b_1^{(2)}), (1, b_1^{(2)})$

} where superscript is round #

Clearly, Provers win if $b_0^{(1)} = b_1^{(2)}$ which happens w/p $1/2$

Hence $\omega(F^2) \geq 1/2$ (In fact $\omega(F^2) \leq \omega(F) = 1/2$)

Hence, FRS claim is follow

However

Claim [Feige]: $\forall\ k,\ \omega(G^{2k}) = 2^{-k}$

So, though FRS claim is false, value of game goes down exponentially.

Theorem [Raz's Parallel Repetition Theorem]

For every game G, $\exists$ constant α_G such that

$$\omega(G^n) \leq (\alpha_G)^n$$

Below Holenstein's prof of Raz's Theorem.

Suppose $\omega(G) = 1-\delta$.

Suffices to prove the following lemma

Lemma: For every game G with $\omega(G) \leq 1-\delta$, there exists $m = \mu(G)n$ indices $i_1, \ldots, i_m$ such that

$\forall\ k = 1, \ldots, m$

Pf

Holenstein's Proof

G – game with value $\omega(G) = 1-\delta$

G^n – n repeated game

π_1, π_2 – Best prover strategies for G^n

Hence, $\omega(G^n) = \underset{\substack{(\bar{x},\bar{y}) \leftarrow (X,Y)^n \\ r \leftarrow R \\ (a_1 \ldots a_n) = \pi_1(\bar{x}, r) \\ (b_1 \ldots b_n) = \pi_2(\bar{x}, r)}}{Prob} [\forall i.\ V(x_i, y_i, a_i, b_i) = 1]$

For random variables

$(X_1, Y_1), \ldots (X_n, Y_n), R$

$\& (A_1 \ldots A_n) = \pi_1((X_1 \ldots X_n), R)$

$(B_1 \ldots B_n) = \pi_2((Y_1 \ldots Y_n), R)$

Let

W_i – event "$V_i(X_i, Y_i, A_i, B_i) = 1$"

$\overline{W} = W_1 \wedge \ldots \wedge W_n$

Hence, $\omega(G^n) = Pr[\overline{W}] = Pr[W_1 \wedge \ldots \wedge W_n]$.

Suffices to prove following lemma

Lemma: There exists $\mu = \mu(\delta, |A|, |B|)$ s.t. there exists $m = \mu n$ indices $i_1 \ldots i_m$

$\forall k = 1 \ldots m$

$$Pr[W_{i_1} \wedge W_{i_2} \wedge W_{i_m}] \leq (1 - \delta/2)^{m-1}$$

(Lemma implies Raz's Theorem since ~~$Pr[\overline{W}] \leq (1-\delta/2)^m \leq \exp(-\delta\mu n)$~~)

We will actually prove the following ~~proposition~~ lemma.

Lemma: $\forall\ m \le n \le k > m$

let

$$Pr[W_k / W_1 \wedge \ldots W_m] = \omega(G) + \epsilon_k = 1 - \delta + \epsilon_k$$

then

$$\frac{1}{n-k} \sum_{k=m+1}^{n} \epsilon_k \le O\left(\sqrt{\frac{1}{n-m}\left(m \log |A||B| + \log\left(\frac{1}{P_m}\right)\right)}\right)$$

where $P_m = Pr[W_1 \wedge \ldots \wedge W_m]$

Proof of Earlier Lemma from above lemma:

For $i = 1 \ldots n$, choose i_m such that

- $Pr[W_{i_m} / W_{i_1} \wedge \ldots \wedge W_{i_{m-1}}]$ is minimized.

Let $P_m = Pr[W_{i_1} \wedge \ldots \wedge W_{i_m}]$

By above lemma

$$P_{m+1}/P_m \le 1 - \delta + O\left(\sqrt{\left(\frac{1}{n-m}\right)\left(m \log |A||B| + \log\left(\frac{1}{P_m}\right)\right)}\right)$$

Prove ~~lemma~~ by induction that for $m \le \mu n$ (μ - to be defined)

$$P_m \le (1 - \delta/2)^{m-1}$$

Clearly, true for $m = 1$

Now from P_m to P_{m+1}

If $P_m \le (1 - \delta/2)^m$, then so is P_{m+1} hence done

Otherwise $\frac{P_{m+1}}{P_m} \le 1 - \delta + O\left(\sqrt{\left(\frac{1}{n-m}\right)\left(m \log |A||B| + m \log\left(\frac{1}{1-\delta/2}\right)\right.}\right.$

There exists $\mu = \mu(|A|/|B|, \delta)$ s.t. if

if

$m \leq \mu n$ then

$$O\left(\sqrt{\left(\frac{m}{n-m}\right)\left(m \log |A|/|B| + \log\left(\frac{1}{1-\delta/2}\right)\right)}\right) \leq \delta/2$$

Hence, $P_{m+1} \leq P_m (1-\delta/2)$

Thus, Lemma proven

Now to proof of lemma

The lemma finds prob of W_k conditioned on

$$W = W_1 \wedge W_2 \ldots \wedge W_m$$

It'll be easier for us to condition not only on W, but also on the answers $(A_1 \ldots A_m) = (B_1 \ldots B_m)$ in the first m rounds.

For some $v = (a_1 \ldots a_m, b_1 \ldots b_m)$

let

$E(v)$ - event that $W \wedge (A_i = a_i) \wedge (B_i = b_i)$

Note $W = \bigvee_v E(v)$

$$Pr[W] = \sum_v Pr[E(v)]$$

Let $V = (A_1 \ldots A_m, B_1 \ldots B_m)$

Thus $E(v) = W \wedge (V = v)$

We'll now prove the following lemma.

Lemma: $\forall m \le n$, $k > n$ & $v \in (|A||B|)^m$, let

$$Pr[W_k / E(v)] = \omega(G) + \epsilon_k$$

then $$\frac{1}{n-k} \sum_{k=m+1}^{n} \epsilon_k \le O\left(\sqrt{\frac{1}{(n-m)} \log \frac{1}{Pr[E(v)]}}\right)$$

Proof of Earlier lemma from above.

$$Pr[W_k / W_1 \wedge \ldots \wedge W_m] = Pr[W/W]$$

$$= \sum_v Pr[W/E(v)] \cdot Pr[V=v/W]$$

$$= \omega(G) + \sum_v Pr[\cancel{V=v}] \cdot \epsilon_k \cdot Pr[V=v/W]$$

$$= \omega(G) + \delta_k \quad (\text{say})$$

Now $$\frac{1}{n-k} \sum_{k=m+1}^{n} \delta_k = \sum_v \frac{1}{n-k} \sum_{k=m+1}^{n} Pr[V=v/W] \cdot \epsilon_k$$

$$= \sum_v Pr[V=v/W] \cdot O\left(\sqrt{\frac{1}{(n-m)} \log \frac{1}{Pr[W \wedge (V=v)]}}\right)$$

$$\le O\left(\sqrt{\frac{1}{(n-m)} \log \sum_v \frac{Pr[V=v/W]}{Pr[W \wedge (V=v)]}}\right) \quad (\text{Jensen's inequality})$$

$$= O\left(\sqrt{\frac{1}{(n-m)} \log\left(\frac{1}{Pr[W]} \sum_v 1\right)}\right)$$

Lemma follows since $\sum_v 1 = (|A||B|)^m$

We need following 2 proposition

Proposition 1:

If $U = U_1 \dots U_n$ is a product distribution & E - event, then

$$\frac{1}{n} \sum_{i=1}^{n} \| U_i - U_i|_E \| \leq \sqrt{\frac{1}{n} \cdot \log \frac{1}{P_n[E]}}$$

Pf: Req Rel Entropy $D(p\|q) = \sum p_i \log \frac{p_i}{q_i}$

Facts: (1) $D(P\|Q) \geq \|P-Q\|^2$

(2) If $U = U_1 \dots U_n$ - product & $V = V_1 \dots V_n$ then $D(V\|U) \geq \sum D(V_i \| U_i)$

$$\left(\sum_{i=1}^{n} \| U_i - U_i|_E \| \right)^2 \leq n \cdot \sum \| U_i - U_i|_E \|^2 \quad \text{(Cauchy-Schwarz)}$$

$$\leq n \cdot \sum D(U_i|_E \| U_i)$$

$$\leq n \cdot D(U|_E \| U)$$

$$= n \sum_{u^k} P_n[U|_E = u^k|E] \cdot \log \frac{P_n[U=u^k|E]}{P_n[U=u^k]}$$

$$= n \log \frac{1}{P_n[E]} + n \sum_{u^k} P_n[U=u^k|E] \log \frac{P_n[U=u^k \wedge E]}{P_n[U=u^k]}$$

$$\leq n \log \frac{1}{P_n[E]}$$

Kla

Proposition 1':

$U = U_1 \dots U_n$ a T-ri.vs such that for all $t \in \mathrm{Supp}(T)$; $U|_{T=t} = U_1|_{T=t} \dots U_n|_{T=t}$ - product dist

then for all events E

$$(\star) = \sum_t P_{\mathcal{R}}[T=t \mid E] \left(\frac{1}{n} \sum_{i=1}^{n} \| U_i|_{T=t} - U_i|_{T=t \wedge E} \| \right) \leq \sqrt{\frac{1}{n} \log \frac{1}{P_{\mathcal{R}}[E]}}$$

Pf From ~~cor~~ Prop 1

$\forall t \in \mathrm{Supp}(T)$

$$\frac{1}{n} \sum_{i=1}^{n} \| U_i|_{T=t} - U_i|_{T=t \wedge E} \| \leq \sqrt{\frac{1}{n} \log \frac{1}{P_{\mathcal{R}}[E \mid T=t]}}$$

Hence ~~$\sum_t$~~ $(\star) \leq \sum_t P_{\mathcal{R}}[T=t \mid E] \sqrt{\frac{1}{n} \log \frac{1}{P_{\mathcal{R}}[E \mid T=t]}}$

$$\leq \sqrt{\frac{1}{n} \log \left(\sum \frac{P_{\mathcal{R}}[T=t \mid E]}{P_{\mathcal{R}}[E \mid T=t]} \right)} \quad \text{(Jensen's)}$$

$$\leq \sqrt{\frac{1}{n} \log \frac{1}{P_{\mathcal{R}}[E]} \sum_t P_{\mathcal{R}}[T=t]}$$

$$= \sqrt{\frac{1}{n} \log \frac{1}{P_{\mathcal{R}}[E]}}.$$

Proposition 2: ∃ procedure A that takes 2 i/ps
- random string R
- desc of dist D

such that:

(a) $A(D,R)$ is dist exactly accg to D

(b) If D & D' are dist s.t $\|D-D'\| \le \epsilon$ then $\Pr[A(D,R) \neq A(D',R)] \le 2\epsilon$

(ie, on 2 close dist, A (when run on the same random string) o/p's near identical string

Pf: A: Interprets Random string R as sequence of samples

$\langle x_1, \alpha_1 \rangle, \langle x_2, \alpha_2 \rangle, \ldots$

where $x_i \in Supp(D)$ & $\alpha_i \in [0,1]$

A: [For $i \leftarrow 1$ to ∞
if $D(x_i) > \alpha_i$, output x_i

Clearly, $A(D,R)$ is dist accg to D

Also $A(D,R) \neq A(D',R)$ if the smallest i for which $\alpha_i < \max(D(x_i), D'(x_i))$ satisfies $\alpha_i > \min(D(x_i), D'(x_i))$

Hence

$$\Pr[A(D,R) \neq A(D',R)] = \frac{\sum_x |D(x) - D'(x)|}{\sum_x \max(D(x), D'(x))} \le 2\|D-D'\|$$

Need to show

$$P_R[W_k \mid E(v)] \approx_{\varepsilon_k} \omega(G)$$

where $E(v) = W \wedge$ "$V = v$"

~~Consider the following~~

For RV $(X_1, Y_1) \ldots (X_n, Y_n)$

Define r.v $T_1 \ldots T_n$ as follows

For $i = 1 \ldots m$

$$T_i = (X_i, Y_i)$$

For $i = m+1, \ldots n$

$$T_i = (b_i, Z_i)$$

where $\begin{cases} b_i \text{ is a random bit chosen independently} \\ Z_i = \begin{cases} X_i & \text{if } b_i = 0 \\ Y_i & \text{if } b_i = 1 \end{cases} \end{cases}$

$$T = (T_1, T_2, \ldots T_n)$$

$$T_{-k} = (T_1, T_2, \ldots T_{k-1}, T_{k+1}, \ldots T_n)$$

~~Suppose~~ Suppose we have

$$(X_k, Y_k) \equiv (X_k, Y_k)\big|_{E(v)} \quad (\#1)$$

For all $(x,y) \leftarrow (X_k, Y_k)\big|_{E(v)}$,

$$\begin{cases} T_{-k}\big|_{X_k = x \wedge E(v)} \equiv T_{-j}\big|_{X_k = x \wedge Y_k = y \wedge E(v)} & (\#2) \\ T_{-k}\big|_{Y_k = y \wedge E(v)} \equiv T_{-k}\big|_{X_k = x \wedge Y_k = y \wedge E(v)} & (\#3) \end{cases} \quad (\#)$$

Then the 2 provers on input (X, Y) can do the following

Prover 1: On i/p x
samples t' acc to $T_i / x_k = x \wedge E(v)$
completes t' to obtain $(x_1 \ldots x_n)$ s.t $x_k = x$
finds ans $a_1 \ldots a_n$
replies w/ a_k

Similarly Prover 2.

Then, the $Pr[V \text{ acc}] = Pr[W_k / E(v)]$

Hence,

$$Pr[W_k / E(v)] \leq \omega(G)$$

However (#) is not true.

Use Prop 1 & Prop 2 to show that (#) is true w/ error of most ϵ_k

Hence $Pr[W_k / E(v)] \leq \omega(G) + \epsilon_k$

Let $\alpha_r = \sqrt{\frac{1}{n-m} \log \frac{1}{P_m[E(v)]}}$

From Prop 1

$\| (X_k, Y_k) - (X_k, Y_k)|_{E(v)} \| = \delta_k$, then $\frac{1}{n-m} \sum \delta_k$

$\leq \sqrt{\frac{1}{n-m} \log \frac{1}{P_m[E(v)]}}$

$= \alpha_r$

Thus, (#1) is true w/ error δ_k.

From Prop 1'

$$\sum_t P_m[T = t / E(v)] \; \| (X_k, Y_k)|_{T=t \wedge E(v)} - (X_k, Y_k)|_{T=t} \| = \mu_k$$

then $\frac{1}{n-m} \sum \mu_k \leq \alpha_r$

We are actually interested in T_k not T

Hence

$$\mu_k = \sum_{t', t_k} P_m[T_{-k} = t' \wedge T_k = t_k / E(v)] \; \| (X_k, Y_k)|_{T_{-k}=t' \wedge T_k = t_k \wedge E(v)}$$

$$- (X_k, Y_k)|_{T_{-k}=t' \wedge T_k = t_k} \| =$$

$$= \sum_{t', t_k} P_m[T_{-k} = t' \wedge T_k = t_k / E(v)] \; \| (X_k, Y_k)|_{T_{-k}=t' \wedge T_k = t_k \wedge E(v)} - (X_k, Y_k)|_{T_k = t_k} \|$$

Now $T_k = (0, z)$ w/p exactly $1/2$

Hence

$$\sum_{t'} P_m[T_{-k} = t' \wedge X_k = x / E(v)] \; \| (X_k, Y_k)|_{T_{-k}=t' \wedge X_k = x \wedge E(v)} - (X_k, Y_k)|_{X_k = x} \|$$

$\leq 2\mu_k$

Hence

$$\sum_{\ell', x} Pr\left[T_{-k} = \ell' \wedge X_k = x \mid E(v)\right] \left\| Y_k\big|_{T_{-k}=\ell' \wedge X_k = x \wedge E(v)} - Y_k\big|_{X_k = x} \right\|$$

$$\leq 2\mu_k$$

However

$$\sum_{\ell', x} Pr\left[T_{-k} = \ell' \wedge X_k = x \mid E(v)\right] \left\| Y_k\big|_{X_k = x} - Y_k\big|_{X_k = x \wedge E(v)} \right\|$$

$$\leq 2\delta_k$$

Hence,

$$\sum_{\ell', x} Pr\left[T_{-k} = \ell' \wedge X_k = x \mid E(v)\right] \left\| Y_k\big|_{T_{-k}=\ell' \wedge X_k = x \wedge E(v)} - Y_k\big|_{X_k = x \wedge E(v)} \right\|$$

$$\leq 2\mu_k + 2\delta_k$$

Changing Order of summation

$$\sum_{x, y} Pr\left[X_k = x \wedge Y_k = y \mid E(v)\right] \left\| T_{-k}\big|_{X_k = x \wedge Y_k = y \wedge E(v)} - T_{-k}\big|_{X_k = x \wedge E(v)} \right\|$$

$$\leq 2\mu_k + 2\delta_k$$

This implies (#2) is true w/ error $\leq 2\mu_k + 2\delta_k$

Similarly, (#3) is true w/ error $\leq 2\mu_k + 2\delta_k$

Hence total error $= \delta_k + 4(2\mu_k + 2\delta_k) = 8\mu_k + 9\delta_k$

$$\leq \alpha_v \cdot = \rho_k$$

Hence $\frac{1}{n-m} \sum \rho_k \leq O(\alpha_v)$

Thus, proved.