Playing Games with Bounded Entropy

Mehrdad Valizadeh and Amin Gohari
Department of Electrical Engineering, Sharif University of Technology

Abstract

We study a two-player zero-sum game in which one of the players is restricted to mixed strategies with limited randomness. More precisely, we consider the maximum payoff that the maximizer (Alice) can secure with limited randomness $h$. This problem finds an operational interpretation in the context of repeated games with non-ideal sources of randomness as shown by Gossner and Vieille, and Neyman and Okada. We begin by simplifying the proof of Gossner and Vieille and also generalize their result. Then, we turn to the computational aspect of the problem, which has not received much attention in the game theory literature. We observe the equivalence of this problem with entropy minimization problems in other scientific contexts. Next, we provide two explicit lower bounds on the entropy-payoff tradeoff curve. To do this, we provide and utilize new results for the set of distribution that guarantee a certain payoff for Alice (mixed strategies corresponding to a security level for Alice). In particular, we study how this set of distribution shrinks as we increase the security level. While the use of total variation distance is common in game theory, our derivation indicates the suitability of utilizing the Renyi-divergence of order two.

1 Introduction

Consider a two-player and zero-sum game between Alice and Bob. The game is played once. A Nash equilibrium assigns a strategy to Alice and Bob such that no player has any incentive to unilaterally change his strategy [1]. It is proven that if the players can randomize on their pure strategies set according to any probability distribution, then the game has at least one Nash equilibrium in the randomized mixed strategies. However, assume that Alice has restrictions on implementing probability distributions when choosing his mixed strategy. More specifically, assume that Alice can only choose a mixed action with entropy at most a given number $h$. For instance, if $h = 0$, Alice is only allowed to play pure actions. We are interested in the maximum payoff that Alice can secure with mixed actions of entropy at most $h$ (regardless of the action of Bob). Let us denote this by $J(h)$. Equivalently, we may ask: in order to guarantee average payoff of $w$, how much randomness needs to be utilized by Alice? Let us denote the minimum entropy of the randomness consumed by Alice to guarantee payoff $w$ by $F(w)$. We may call $F(w)$, the min-entropy function. Observe that $F(\cdot)$ is the inverse function of $J(\cdot)$.

Even though $J(h)$ is defined in a one-shot setting, the (upper concave envelope) of $J(h)$ finds an operational meaning in [2, 4] in the context of repeated games as the payoff that Alice can secure in the long run. For instance, Gossner and Vieille [2] study a repeated game in which Alice cannot randomize freely, but has access to an external i.i.d. source $X, Y, \ldots$ which are revealed symbol by symbol (causally) to Alice as the game is played out. They show that the entropy of the source

\footnote{One should not confuse our “min-entropy function” with the term “min-entropy” commonly used to denote the Rényi entropy of order infinity.}
$H(X)$ characterizes the payoff that Alice can secure in the long run, and the answer is given in terms of $J(H(X))$. This is similar to Shannon’s compression formula $H(X)$ which is defined on a single copy of the source (single letter), but gives the ultimate compression limit when multiple copies of the source are observed. Another motivation for $J(h)$ is given in [5, 6], arguing that limitation on random strategies of players stems from simplicity of humans; that “humans are known to be bad at generating random-like sequences”.

To compute $F(w)$, one has to first consider the set of distributions on the action of Alice that would secure a payoff $w$ for her. This set will be a polytope in the space of all probability distributions. Then, one should solve an entropy minimization problem over this polytope in the space of probability distributions. In fact, minimizing and maximizing entropy arises in a wide range of contexts. Computing maximum entropy under a set of linear constraints is a well-studied problem with a wide range of applications, e.g., see [7] [8, p.367] and the principle of maximum entropy. It is shown in [9] that computing the minimum entropy can be also quite important. Furthermore, many algorithms for clustering and pattern recognition are essentially solving entropy minimization problems [10]. An important special case of the entropy minimization problem (with its own applications) is that of finding a joint probability of minimum entropy given its marginal distributions (the marginal distribution is a linear constraint on the joint probability distribution) [11–13]. Finally, the quantum version of the entropy minimization problem is of key theoretical importance. [14]

While the calculation of the function $F(w)$ has received attention in the game theory literature, entropy minimization problem are known to be an NP-hard non-convex optimization problem [15]. Since the entropy is a concave function over the probability simplex, its minimum occurs at a vertex of the feasible domain. As a result, computation of $F(w)$ leads to a search problem over an exponentially large set. Even though the algorithm of [16] can be used to compute $F(w)$, but it has no guarantee of success.

Our contributions can be summarized as follows:

- We study the properties of $F(w)$ and give a number of easy-to-compute bounds on the value of $F(w)$. One of the bounds on $F(w)$ is expressed in term of a linear program; this linear program has a quite general form. We employ probabilistic tools to study this linear program to prove the following explicit lower bound on $F(w)$:

$$F(w) \geq \log_2 \left( 1 + \frac{(w - v)^2}{(w - m)(m - w)} \right) \quad \forall w : v \leq w \leq w^*,$$

where $m$ and $m$ are the minimum and maximum entries of the entries of the payoff table; $v$ is the payoff that Alice can guarantee with deterministic strategies (pure-strategy security level) and $w^*$ is the Nash value of the game for Alice (payoff that Alice can guarantee with no restriction on her action’s entropy). Because the linear program we consider has a quite general form (and can be converted to other linear programs with a change of variables), our use of probabilistic tools for studying linear programs is novel.

- We give and utilize new results on the set of mixed strategies that guarantee a certain security level. While the literature on game theory makes extensive use of total variation distance between distributions, we propose and illustrate the use of the $\chi^2$-divergence (or the Tsallis divergence of order two) in game theoretic contexts. The $\chi^2$-divergence is defined as $\chi^2(p, q) = \left( \sum_i \frac{p_i^2}{q_i} \right) - 1$, where $p = (p_1, p_2, \cdots, p_n)$ and $q = (q_1, q_2, \cdots, q_n)$ are two probability distributions. To see the applicability of this divergence measure, consider a zero-sum
game between Alice and Bob. Fix an arbitrary (mixed) strategy for Bob. Let \( p_1 \) and \( p_2 \) be two probability distributions for the action of Alice. Let \( W_1 \) and \( W_2 \) denote the payoff of Alice when she plays according to \( p_1 \) and \( p_2 \) respectively. Then, \( E[W_1] \) and \( E[W_2] \) are the payoffs secured by \( p_1 \) and \( p_2 \). Also \( \text{Var}[W_1] \) is a natural object, the risk associated to \( p_1 \). Then, as we see later in Lemma 19 these natural objects in a game come together as follows:

\[
\chi^2(p, q) \geq \frac{(E[W_1] - E[W_2])^2}{\text{Var}[W_1]}. 
\]

• The min-entropy function \( F(w) \) finds its operational interpretation in a repeated game (e.g., the result of Gossner and Vieille in [2]). We simplify and generalize the proof of Gossner and Vieille in Section 3. The generalized setup considers the possibility of leakage of Alice’s random source sequence to Bob in the zero-sum game. More specifically, we assume an i.i.d. sequence of pairs \( (X_1, Y_1), (X_2, Y_2), \ldots \) distributed according to a given \( p(x, y) \). The sequence \( X_1, X_2, \ldots \) is revealed symbol by symbol (causally) to Alice as the game is played out, while the sequence \( Y_1, Y_2, \ldots \) is revealed symbol by symbol to Bob. We can view \( Y_1 \) as the side information that Bob obtains about Alice’s observation. As before, Alice cannot randomize freely and can only use the randomness in the sequence \( X_1, X_2, \ldots \). We show that the upper concave envelope of \( \mathcal{J}(h) \), at \( h = H(X|Y) \) is the maximum payoff that Alice can secure regardless of Bob’s actions; furthermore, Bob can ensure that Alice does not get more than this payoff. This result is a generalization of the result of Gossner and Vieille since when \( Y \) is a constant random variable, the conditional entropy \( H(X|Y) \) reduces to the unconditional entropy \( H(X) \).

The rest of this paper is organized as follows: In Section 2 we give a mathematical definition of the problem under study; in Section 4 we express the main results. Finally, in Section 6 we give the proofs. Some of the details are left for the appendices.

## 2 Problem Statement

Consider a zero-sum game between players Alice (\( A \)) and Bob (\( B \)) with respective pure strategy sets \( \mathcal{A} = \{1, \ldots , n\} \) and \( \mathcal{B} = \{1, \ldots , n'\} \) where \( n \) and \( n' \) are natural numbers. The payoff matrix is denoted by \( U = [u_{ij}] \) where \( u_{ij} \) is the real valued payoff that player \( A \) gets from player \( B \) when \( i \in \mathcal{A} \) and \( j \in \mathcal{B} \) are played. Player \( A \) (\( B \)) wishes to maximize (minimize) the expected payoff. The set of all randomized strategies of players \( A \) and \( B \) are denoted by \( \Delta(\mathcal{A}) \) and \( \Delta(\mathcal{B}) \) respectively which are probability simplexes on sample spaces \( \mathcal{A} \) and \( \mathcal{B} \) respectively. Thus, Alice’s strategy corresponds to a probability mass function (pmf) \( p = (p_1, p_2, \ldots , p_n) \), which can be also illustrated as a column vector with non-negative entries that add up to one.

Assume that player \( A \) uses randomized strategy \( p \). Then the payoff of Alice if Bob plays \( j \in \mathcal{B} \) is \( \sum_i p_i u_{ij} \). We say that Alice secures payoff \( w \) with randomized strategy \( p \) (regardless of the action of player \( B \)) if \( \sum_i p_i u_{ij} \geq w \) for all \( j \in \mathcal{B} \). Thus, the set of all distributions that guarantee payoff \( w \) for player \( A \) can be expressed as

\[
\mathcal{P}_w(w) = \{ p \in \Delta(\mathcal{A}) : p^T U \geq w 1^T \},
\]

where \( p^T \) is the transpose of the column vector \( p \), \( 1 \) is a column vector of all ones and \( v_1 \geq v_2 \) means any element of \( v_1 \) is greater than or equal to the corresponding element at \( v_2 \).
We define

\[ F_U(w) \triangleq \min_{p \in \mathcal{P}_U(w)} H(p), \quad (2) \]

where \( H(p) \) is the Shannon entropy of probability mass function (pmf) \( p \), defined as

\[ H(p) = \sum_{\ell=1}^{k} -p_\ell \log p_\ell, \]

where all the logarithms in this paper are in base two. If the set \( \mathcal{P}_U(w) \) is empty, we set \( F_U(w) = +\infty \).

**A remark on notation:** Two-player zero-sum games are completely characterized by payoff matrix. For the sake of simplicity, we call two-player zero-sum games with their payoff matrix.

Thus, game \( U \) refers to a game with payoff table \( U \).

**Definition 1.** Given a game \( U = [u_{ij}] \), parameters \( m, \overline{m}, v \) and \( w^* \) are defined as:

- \( m \) (\( \overline{m} \)) is the minimum (maximum) element of matrix \( U : m = \min_{i,j} u_{ij} \) (\( \overline{m} = \max_{i,j} u_{ij} \)).
- \( v \) is the maximum payoff secured by pure actions (pure-strategy security level): \( v = \max_i \min_j u_{ij} \).
- \( w^* \) is the Nash value of \( U \), which is the maximum guaranteed payoff with unlimited access to random sources:

\[ w^* = \max_{w : \mathcal{P}_U(w) \neq \emptyset} w. \quad (3) \]

Note that by definition, \( m \leq v \leq w^* \leq \overline{m} \).

According to Definition 1, \( v \) is the payoff that is guaranteed without consumption of any randomness whereas \( w^* \) is the maximum guaranteed payoff when unlimited randomness is available. Thus, it is interesting to consider the min-entropy function \( F_U(w) \) in the domain \( v \leq w \leq w^* \). If \( w \leq v \), then \( F_U(w) = 0 \); if \( w > w^* \) the feasible set of optimization problem in (2) is empty and \( F_U(w) = +\infty \). When \( v \leq w \leq w^* \), the function \( F_U(w) \) is not necessarily convex or concave as a function of \( w \): it is strictly increasing and piecewise concave [3, p. 241].

### 3 On the set \( \mathcal{P}_U(w) \)

The function \( F_U(w) \) is defined in (2) using \( \mathcal{P}_U(w) \), which is the set of all distributions that guarantee a security level \( w \) for player \( A \). Observe that

\[ \mathcal{P}_U(w) = \{ p \in \Delta(A) : p^T U \geq w1^T \}, \quad (4) \]

is a polytope defined via some linear constraints. As the matrix \( U \) is completely arbitrary, with a change of variables, one can convert it to many different equivalent linear programs. We only need to study \( \mathcal{P}_U(w) \) for \( v \leq w \leq w^* \). It is immediate from the definition \( \mathcal{P}_U(w) \) that this set is decreasing in \( w \), i.e., for any \( w_1 \geq w_2 \),

\[ \mathcal{P}_U(w_1) \subseteq \mathcal{P}_U(w_2). \quad (5) \]

We are interested to see if the inclusion in (5) is strict, and if yes, quantify to what extent it is. To do this, we look at the distance between the set \( \mathcal{P}_U(w_1) \) and the compliment of \( \mathcal{P}_U(w_2) \) (that

\[ \text{This property is stated in [3] in terms of the function } J(\cdot). \]
is \( \mathcal{P}_0(w_2) = \Delta(A) - \mathcal{P}_0(w_2) \). The sets \( \mathcal{P}_0(w_1), \mathcal{P}_0^c(w_2) \) and \( \Delta(A) \) are illustrated in Figure 1. The distance between any two sets can be defined as

\[
d(S_1, S_2) \triangleq \inf_{p \in S_1, q \in S_2} d(p, q),
\]

where \( d(p, q) \) can be any arbitrary distance measure. The standard option is the total variational distance

\[
d_1(p, q) = \frac{1}{2} \sum_i |p_i - q_i|.
\]

With this choice of the distance, we have

**Theorem 2.** For any \( w_1, w_2 \) satisfying \( v \leq w_2 \leq w_1 \leq w^* \), we have

\[
d_1(\mathcal{P}_0^c(w_2), \mathcal{P}_0(w_1)) \geq \frac{|w_1 - w_2|}{|m - m'|}.
\]

Observe that the quantities \( m \) and \( m' \) can be simply computed from \( U \). The idea of the proof of Theorem 2 is standard (e.g., see [2, eq. (4)] for a similar derivation), but is included in Section 6.1 for completeness.

In this paper, we propose use of the Rényi divergence of order two between \( p \) and \( q \) to quantify the distance between two distributions:

\[
d_2(p, q) \triangleq \log\left(\sum_i \frac{p_i^2}{q_i}\right) = \log(1 + \chi^2(p, q)).
\]

Our first result gives the following bound:

**Theorem 3.** For any \( w_1, w_2 \) satisfying \( v \leq w_2 \leq w_1 \leq w^* \), we have

\[
d_2(\mathcal{P}_0^c(w_2), \mathcal{P}_0(w_1)) \geq \log\left(1 + \frac{(w_1 - w_2)^2}{(w_1 - m)(m - w_1)}\right).
\]

In this definition, we set \( p_i^2/q_i \) to be zero if \( p_i = q_i = 0 \), and infinity if \( p_i > 0 \) while \( q_i = 0 \). We have that \( d_2(p, q) \geq 0 \), and \( d_2(p, q) = 0 \) if and only if \( p = q \).
The proof can be found in Section 6.1. The above result is derived by a probabilistic approach, which we believe is novel in the context of linear programming. Note that the linear program given in (4) is quite general, and given in terms of an arbitrary payoff matrix $U$. With a proper change of variables, the above result can be applied to a large class of parametric linear programs.

Our second result is less crucial, but still useful. It gives a compact formula for the supporting hyperplanes of $P_U(w)$ in terms of the Nash equilibrium of a game. We need a definition:

**Definition 4.** Let $Nash(U)$ denote the value of a two-player zero-sum game with payoff table $U = [u_{ij}]$; thus $Nash(U)$ is the maximum value that Alice can guarantee using arbitrary mixed strategies. It is known that in a zero-sum game, while the game might have multiple Nash equilibriums, the value of Alice in all of the equilibriums is the same [17, p.145].

Given values $a_1, a_2, \cdots, a_n \in \mathbb{R}$, let us construct a new table whose $(i, j)$ entry is $\tilde{u}_{ij} = u_{ij} + a_i$. In other words, we add $a_i$ to the entries in the $i$-th row of $U$. The new table can be expressed as $\tilde{U} = U + a \cdot 1^T$ where $a$ is a column vector whose entries are $a_1, a_2, \cdots, a_n$ and $1^T$ is a row vector of all ones. Observe that the table $\tilde{U}$ can be intuitively understood as giving an additional incentive $a_i$ to Alice for playing her $i$-th action (it is actually a disincentive or “tax” if $a_i < 0$).

**Theorem 5.** The set $P_U(w)$ can be characterized as follows:

$$P_U(w) = \left\{ p \in \Delta(A) \mid \sum_i a_ip_i \leq Nash(U + a1^T) - w, \ \forall a \right\}.$$

**Remark 6.** Note that $\max_{p \in P_U(w)} (\sum_i a_ip_i)$ is simply a linear program. Equivalence of linear program and Nash equilibriums are known in the literature [18, 19]. However, our construction of the game $\tilde{U}$ based on incentive or tax is new to best of our knowledge.

In Section 6.2, we give the proof of Theorem 5 as well as a geometric picture of the Nash equilibrium strategies of Alice.

## 4 On the Min-Entropy Function

We begin with a property of the min-entropy function. To state the property, we need the following definition:

**Definition 7.** Consider two games with payoff matrixes $U_1$ and $U_2$. Let $U_3 = U_1 \oplus U_2$ be the direct-sum of $U_1$ and $U_2$. Then $U_3$ defines a new game in which players simultaneously play one instance of $U_1$ and one instance of $U_2$ and the resulting payoff is the sum of payoffs from $U_1$ and $U_2$.

**Theorem 8.** Then, we have $F_{U \oplus U}(w) = F_U(w/2)$. Similarly, for every natural number $k$, $F_{\oplus^k U}(w) = F_U(w/k)$ where $\oplus^k U$ is $k$ times direct sum of $U$.

An application of the above theorem is that given an expression $G_U(w)$ that bounds $F_U(w)$ from below for all $w$ and $U$, we can conclude that $G_{\oplus^k U}(kw) \leq F_{\oplus^k U}(kw) = F_U(w)$. Thus, $\max_k G_{\oplus^k U}(kw)$ is also a (potentially better) lower bound to $F_U(w)$. As a result, we expect that a “good” lower (or upper bound) on $F_U(w)$ should have the correct scaling behavior as we simultaneously play more and more copies of the game.
4.1 Lower and upper bounds on the min-entropy function

The min-entropy function \( F_U(w) \) in (2) is the minimum of a concave function on a polytope \( \mathcal{P}_U(w) \). This minimum occurs at a vertex of \( \mathcal{P}_U(w) \). This leads to a search in the exponentially large set of vertices of the polytope \( \mathcal{P}_U(w) \), which is computationally hard. We desire to find bounds on \( F_U(w) \) that are either explicit, or else can be computed in polynomial time. Observe that

\[
F_U(w) = \min_{p \in \mathcal{P}_U(w)} H(p) = \log(|\mathcal{A}|) - \max_{p \in \mathcal{P}_U(w)} D(p||p^u)
\]  

(6)

where \( p^u \) is the uniform distribution over \( \mathcal{A} \), and \( D(p||q) = \sum_i p_i \log(p_i/q_i) \) is the Kullback–Leibler (KL) divergence. Thus, we are interested in finding the vertex of \( \mathcal{P}_U(w) \) which has maximum distance from the uniform distribution (with respect to KL divergence).

**Lower bound:** To prove lower bounds for \( F_U(w) = \min_{p \in \mathcal{P}_U(w)} H(p) \),

one idea is to replace the entropy function with a smaller function and compute the maximum over \( \mathcal{P}_U(w) \). Another idea is to also relax the set of distributions \( \mathcal{P}_U(w) \) and replace it with a potentially bigger set. We proceed with the first idea, and comment on the second idea afterwards. Using the fact that the Rényi entropy is decreasing in its order, we obtain that for any \( \alpha > 1 \)

\[
F_U(w) = \min_{p \in \mathcal{P}_U(w)} H(p) \geq \min_{p \in \mathcal{P}_U(w)} H_\alpha(p),
\]  

(8)

where \( H_\alpha(p) \) is the Rényi entropy of order \( \alpha \):

\[
H_\alpha(p) = \frac{1}{1-\alpha} \log_2 \left( \sum_i p_i^\alpha \right).
\]

The case of \( \alpha = 2 \) is related to the Euclidean norm and results in an optimization problem similar to the one given in [6] for the Euclidean norm instead of the KL divergence, which is still not tractable. However, the case \( \alpha = \infty \) relates to the maximum norm and results in the following lower bound:

\[
G_U^{(1)}(w) = -\log_2 \left( \max_{p \in \mathcal{P}_U(w)} \max_{i \in \mathcal{A}} p_i \right).
\]

For each \( i \), the problem of finding the maximum of \( p_i \) over \( p \in \mathcal{P}_U(w) \) is a linear program. From Theorem 5, we can find an upper bound on the value of this linear program, yielding

\[
G_U^{(1)}(w) \geq -\log_2 \max_i \left( \text{Nash}(U + e_i^T) - w \right),
\]  

(9)

where \( e_i \) is a vector of length \( |\mathcal{A}| = n \) whose \( i \)-th coordinate is one, and all its other coordinates are zero. The lower bound \( G_U^{(1)}(w) \), or its relaxed version in [7] can be found in polynomial time, even though they are not in explicit forms.

To obtain an explicit lower bound, observe that \( \log_2(1/p_i) = d_2(e_i, p) \). Note that the vector \( e_i \) is a probability vector associated to a deterministic random variable that chooses \( i \) with probability one. Take some \( \epsilon > 0 \). By definition, deterministic strategies cannot secure a payoff of more than
of Theorem 8, one also obtains that

\[ G^{(1)}_0(w) = - \log_2 \left( \max_{p \in V_0(w)} \max_{i \in A} p_i \right) \]

\[ = \min_{p \in V_0(w)} \min_{i \in A} \log_2 \left( \frac{1}{p_i} \right) \]

\[ = \min_{p \in V_0(w)} \min_{i \in A} d_2(e_i, p) \]

\[ \geq \min_{p \in V_0(w)} \min_{q \in V_0(w+\epsilon)} d_2(q, p) \]

\[ \geq \log_2 \left( 1 + \frac{(w - v + \epsilon)^2}{(w - m)(m - w)} \right), \]  

(10)

where (10) follows from Theorem 3. Letting \( \epsilon \to 0 \), we obtain

\[ F_0(w) \geq G^{(2)}_0(w) \triangleq \log_2 \left( 1 + \frac{(w - v)^2}{(w - m)(m - w)} \right) \quad \forall w : v \leq w \leq w^*. \]

With a similar argument and using the fact that \( p_i = 1 - d_1(e_i, p) \), we obtain the following lower bound utilizing Theorem 2

\[ F_0(w) \geq G^{(3)}_0(w) \triangleq - \log_2 \left( 1 - \frac{|w - v|}{|m - m|} \right) \quad \forall w : v \leq w \leq w^*. \]

Observe that when \( v = m, G^{(2)}_0(w) \) equals \( G^{(3)}_0(w) \). When \( v \neq m \), a simple calculation shows that \( G^{(2)}_0(w) \geq G^{(3)}_0(w) \) if and only if \( w \geq (m + v)/2 \).

**Example 9.** Consider a game with payoff matrix:

\[
\begin{bmatrix}
-1 & 1 & 1 \\
1 & 0.5 & 1 \\
1 & 1 & 0.5 \\
\end{bmatrix}
\]

From payoff matrix we have \( v = 0.5, m = -1, \overline{m} = 1 \) and \( w^* = 0.778 \). Therefore for \( w \geq 0.75 \), \( G^{(2)}_0(w) \) gives a better lower bound than \( G^{(3)}_0(w) \) on \( F_0(w) \).

**Remark 10.** One can inspect that just like that the min-entropy function, the explicit lower bounds \( G^{(2)}_0(w) \) and \( G^{(3)}_0(w) \) satisfy

\[ G^{(i)}_{0; \geq 0}(w) = G^{(i)}_0(w/2), \quad i = 2, 3, \]

have the correct scaling behavior. Additionally, by replacing entropy with Rényi entropy in the proof of Theorem 8, one also obtains that

\[ G^{(1)}_{0; \geq 0}(w) = G^{(1)}_0(w/2). \]

The function \( G^{(2)}_0(w) \) has second derivative for all \( v \leq w \leq w^* \), while the second derivative of the piecewise concave function \( F_0(w) \) is defined everywhere except for a finite number of kink points. The second derivative of the function \( G^{(2)}_0(w) \) may be positive or negative, while \( F_0(w) \) is piecewise concave. On the other hand, the function \( G^{(1)}_0(w) \) is piecewise convex. The reason is that if \( \max_{i \in A} \max_{p \in V_0(w)} p_i \) is attained by \( v^* \) and a particular vertex of \( V_0(w) \) for \( w \in [w_1, w_2] \), in this interval \( \max_{i \in A} \max_{p \in V_0(w)} p_i \) varies linearly in \( w \). Then, convexity of \( - \log_2(.) \) results in convexity of \( G^{(1)}_0(w) \) in the interval \([w_1, w_2]\).
Remark 11. Inequality (10) shows that
\[
\max_{\mathbf{p} \in \mathcal{P}_0(w)} p_i \leq \left(1 + \frac{(w - v)^2}{(w - m)(m - w)}\right)^{-1} \forall w : v \leq w \leq w^* \text{ and } \forall i = 1, \ldots, n \tag{11}
\]
which gives an upper bound for the linear programming of \(\max_{\mathbf{p} \in \mathcal{P}_0(w)} p_i\). Note that \(\mathcal{P}_0(w)\) is a very generic polytope, parameterized by a variable \(w\). By a change of variables (scaling and shifting), one can convert \(\max_{\mathbf{p} \in \mathcal{P}_0(w)} p_i\) to a wide class of linear programs (with no immediate connection to the probability simplex), and then use the bound given in (11).

Let us now turn to the second idea to prove a lower bound for \(F_0(w)\) in (7), namely replacing the set of distributions \(\mathcal{P}_0(w)\) with a potentially bigger set. As mentioned earlier, minimization of the entropy over the set
\[
\mathcal{P}_0(w) = \{ \mathbf{p} \in \Delta(\mathcal{A}) : \mathbf{p}^T \mathbf{u} \geq w \mathbf{1}^T \}
\]
can be difficult. However, it could be possible to solve it (or find good lower bounds for it) for special choices of the matrix \(\mathbf{U}\). We show how a result for a special case of \(\mathbf{U}\) can be utilized to find a bound (computable in polynomial time) for an arbitrary \(\mathbf{U}\). In particular, let us assume that one has a way to minimize entropy over the set
\[
\mathcal{Q}(\mathbf{r}) \triangleq \{ \mathbf{p} \in \Delta(\mathcal{A}) : \mathbf{p}^T \mathbf{u}^* \geq \mathbf{r}^T \}
\]
for some given matrix \(\mathbf{u}^*\), and any arbitrary column vector \(\mathbf{r}\). Then, we are interested in a value for \(\mathbf{r}\) such that
\[
\mathcal{P}_0(w) \subseteq \mathcal{Q}(\mathbf{r}) \tag{12}
\]
Then, we can relax minimization of the entropy over the set \(\mathcal{P}_0(w)\) by instead, computing its minimum over the set \(\mathcal{Q}(\mathbf{r})\). Note that an appropriate \(\mathbf{r}\) in (12) can be found by solving a number of linear programs: the product \(\mathbf{p}^T \mathbf{u}^*\) consists of a number of linear equations on coordinates of \(\mathbf{p}\), and the minimum of each linear equation over the set \(\mathcal{P}_0(w)\) is a linear program (see also Theorem 5).

Upper bound: It is clear that any \(F_0(w) \leq H(\mathbf{p})\) for any arbitrary choice of \(\mathbf{p} \in \mathcal{P}_0(w)\). The following theorem gives a number of upper bounds, each of which are obtained by identifying \(\mathbf{p} \in \mathcal{P}_0(w)\) in different ways.

Theorem 12. Consider a game with payoff matrix \(\mathbf{U}\) and parameters \(v, m, \overline{m}\) and \(w^*\) defined in Definition 7. Let \(h^*\) be the entropy of some Nash strategy of player 1 and define
\[
Q_0^{(1)}(w) = \min \left\{ h^*, \frac{w - v}{w^* - v} h^* + h\left(\frac{w - v}{w^* - v}\right) \right\}
\]
\[
Q_0^{(2)}(w) = \min_{i \in \mathcal{A}} H(\mathbf{p}_{\max,i}^*), \quad \mathbf{p}_{\max,i}^* \in \arg \max_{\mathbf{p} \in \mathcal{P}(w)} p_i
\]
\[
Q_0^{(3)}(w) = \min_{j \in \mathcal{X}_B} \max_{\mathbf{p} \in \mathcal{P}_0(w) : \mathbf{p}^T \mathbf{w}_{\mathcal{X}_B} = w} H(\mathbf{p})
\]
where \(h(\alpha) = -\alpha \log(\alpha) - (1 - \alpha) \log(1 - \alpha)\) and \(Q_0^{(2)}(w)\) can be defined with any choice of \(\mathbf{p}_{\max,i}^*\) from the argmax set (if there are multiple possible choices). Therefore,
\[
F_0(w) \leq Q_0^{(r)}(w), \quad r = 1, 2, 3.
\]

\[\text{For instance, if each row of } \mathbf{U} \text{ has only one non-zero element, the set of constraints will be on the individual coordinates of the vector } \mathbf{p} \text{ and minimizing entropy for such constraints is tractable.}\]
Figure 2: Illustration of the bounds on min-entropy function for the game defined in example 14. The horizontal line depicts $w$ and vertical line depicts the value of bounds.

Proof of Theorem 12 can be found in Section 6.4.

Remark 13. The second derivative of $Q_U^{(1)}(w)$ is negative for $v \leq w \leq w^*$. Thus $Q_U^{(1)}(w)$ is a concave function of $w$ and one can readily inspect that:

$$Q_U^{(1)}(w) = Q_U^{(1)}\left(\frac{w}{2}\right).$$

As $\arg\max_{p \in P(w)} p_i$ may contain multiple elements, $Q_U^{(2)}(w)$ is not a well defined function of $w$. The function $Q_U^{(3)}(w)$ is not necessarily scalable for game $U \oplus U$.

Example 14. Consider a game with payoff matrix:

$$U = \begin{bmatrix} 3 & 1 & 0 & -2 & 0 & -2 \\ 1 & 3 & -2 & 0 & -2 & 0 \\ 0 & -2 & 3 & 1 & 0 & -2 \\ -2 & 0 & 1 & 3 & -2 & 0 \\ 0 & -2 & 0 & -2 & 3 & 1 \\ -2 & 0 & -2 & 0 & 1 & 3 \end{bmatrix}$$

Figure 2 illustrates the behavior of the bounds for this example. In this example $v = m$; hence $G_U^{(3)}(w)$ coincides with $G_U^{(2)}(w)$ and is not depicted in the figure.

5 Operational interpretation of $F(w)$ in repeated game with an unsecure randomness source

Consider a $T$ stage repeated zero-sum game between players Alice($A$) and Bob($B$) with respective finite action sets $A = \{1, \ldots, n\}$ and $B = \{1, \ldots, n'\}$ where $n$ and $n'$ are natural numbers. Let
$X^T = (X_1, X_2, \ldots, X_T)$ and $Y^T = (Y_1, Y_2, \ldots, Y_T)$ be two sequences of random variables drawn i.i.d. from respective sample spaces $\mathcal{X}$ and $\mathcal{Y}$ with law $p_{XY}$. In every stage $t \in \{1, 2, \ldots, T\}$, Alice and Bob observe respective random sources $X_t$ and $Y_t$ privately and choose actions $A_t \in \mathcal{A}$ and $B_t \in \mathcal{B}$. Then Alice gets stage payoff $u_{A_t, B_t}$ from Bob and both players observe the chosen actions $A_t$ and $B_t$. In order to choose actions at stage $t$, players make use of the history of their observations until stage $t$ which is denoted by $H^t_1 = (X_1, A_1, B_1, \ldots, X_{t-1}, A_{t-1}, B_{t-1}, X_t)$ for Alice and $H^t_2 = (Y_1, A_1, B_1, \ldots, Y_{t-1}, A_{t-1}, B_{t-1}, Y_t)$ for Bob. Let $\sigma_t : (\mathcal{A} \times \mathcal{B})^{t-1} \times \mathcal{X}^t \rightarrow \mathcal{A}$ and $\tau_t : (\mathcal{A} \times \mathcal{B})^{t-1} \times \mathcal{Y}^t \rightarrow \mathcal{B}$ be the functions mapping the history of observations of Alice and Bob to actions at stage $t$, thus $A_t = \sigma_t(H^t_1)$ and $B_t = \tau_t(H^t_2)$. Note that Alice and Bob do not have access to any private sources of randomness, besides $H^t_1$ and $H^t_2$, and have to use deterministic functions $\sigma_t(\cdot)$ and $\tau_t(\cdot)$. We call the $T$-tuples $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_T)$ and $\tau = (\tau_1, \tau_2, \ldots, \tau_T)$ the strategies of Alice and Bob respectively. The expected average payoff for Alice up to stage $T$ induced by strategies $\sigma$ and $\tau$ is denoted by $\lambda_T(\sigma, \tau)$ which is:

$$\lambda_T(\sigma, \tau) = \mathbb{E}_{\sigma, \tau} \left[ \frac{1}{T} \sum_{t=1}^{T} u_{A_t, B_t} \right]$$

where $\mathbb{E}_{\sigma, \tau}$ denotes expectation with respect to the distribution induced by i.i.d. repetitions of $p_{XY}$ and strategies $\sigma$ and $\tau$. Alice (Bob) wishes to maximize (minimize) $\lambda_T(\sigma, \tau)$.

The above repeated zero-sum game between players Alice($A$) and Bob($B$) reduces to the one considered by Gossner and Vieille in [2] if we set $Y_t$ to be constant random variables. We call $X_t$ an unsecure randomness source since it is partially leaked to Bob through $Y_t$.

Definition 15. Let $v$ be arbitrary real value:

- Alice can secure $v$ if there exists a strategy $\sigma^*$ for Alice such that for all strategy $\tau$ of Bob we have $\liminf_{T \to \infty} \lambda_T(\sigma^*, \tau) \geq v$.

- Bob defends $v$ if given an arbitrary strategy $\sigma$ for Alice there exists a strategy $\tau^*$ for Bob such that $\limsup_{T \to \infty} \lambda_T(\sigma, \tau^*) \leq v$.

- $v$ is the maxmin value of the repeated game if Alice can secure $v$ and Bob can defend $v$.

The maxmin value of the repeated game under study is characterized as follows:

Theorem 16. The maxmin value of the repeated game is $J_{cav}(H(X|Y))$ where $J_{cav}(\cdot)$ is the smallest concave function greater than or equal to $J(\cdot)$.

To prove theorem [16] In section 5.1 we show that Alice can secure $J_{cav}(H(X|Y))$ and in section 5.2 we show that Bob can defend $J_{cav}(H(X|Y))$, therefore by definition $J_{cav}(H(X|Y))$ is the maxmin value of the repeated game.

5.1 Alice can secure $J_{cav}(H(X|Y))$

To show that Alice can secure any payoff less than $J_{cav}(H(X|Y))$, we extend and simplify the proof of [2]. The upper concave envelope $J_{cav}(\cdot)$ at $h = H(X|Y)$ can be expressed as the convex combination

$$\gamma J(H(p^1_A)) + (1 - \gamma)J(H(p^2_A))$$
Time slots in which Alice plays pure action $1 \in \mathcal{A}$

Time slots in which Alice draws random action with law $p_A^{(1)}$

Time slots in which Alice draws random action with law $p_A^{(2)}$

Figure 3: Illustration of block Markov strategy

for some $\gamma \in [0,1]$ and input distributions $p_A^{(1)}$ and $p_A^{(2)}$ on $\mathcal{A}$ satisfying

$$\gamma H(p_A^{(1)}) + (1 - \gamma) H(p_A^{(2)}) = H(X|Y).$$

As a result, it suffices to show that for any $p_A^{(1)}$ and $p_A^{(2)}$ satisfying

$$\gamma H(p_A^{(1)}) + (1 - \gamma) H(p_A^{(2)}) < H(X|Y),$$

Alice can secure payoffs arbitrarily close to $\gamma J(H(p_A^{(1)})) + (1 - \gamma) J(H(p_A^{(2)}))$.

The idea is to utilize the so-called “block-Markov” proof technique. Take some $T$ of the form $T = NL$, and divide the total $T$ stages into $N$ blocks of length $L$. Excluding the first block, we generate the action sequence of each block as a function of the random source observed during the previous block (we ignore the payoff of the first block throughout the discussion, since by taking the number of blocks $N$ large enough, the contribution of the first block in Alice’s net average payoff becomes negligible). More specifically, excluding the first block, each block is further divided into two subblocks, with the first subblock taking up $\gamma$ fraction of the block. Alice aims to use its observed random source during the previous block to play almost i.i.d. according to $p_A^{(1)}$ during the first subblock, and almost i.i.d. according to $p_A^{(2)}$ during the second subblock. In addition, Alice wants its action at any given stage to be also (almost) independent of Bob’s previous observation history in that stage. This is depicted in Figure 3. Observe that if Alice could produce actions that are perfectly i.i.d. according to $p_A^{(1)}$ and independent of Bob’s history, then in $\gamma$ fraction of the games in a block, she secures the payoff of $J(H(p_A^{(1)}))$, and in the remaining $1 - \gamma$ fraction secures the payoff of $J(H(p_A^{(2)}))$. This gives Alice a total payoff of $\gamma J(H(p_A^{(1)})) + (1 - \gamma) J(H(p_A^{(2)}))$.

In reality, Alice cannot produce the exactly independent actions that she desires. Thus, the proof of [2] (for the special case of a constant $Y$) goes at length to ensure that approximate independence is enough. We diverge from the proof of [2] at this point. Note that by symmetry, we only need to consider the payoff that Alice gets in one of the blocks. For notational simplicity, we denote the observations of Alice and Bob in the previous block by $X^L$ and $Y^L$ respectively, and use $A^L$ and $B^L$ to denote their actions in the current block. The proof relies on the following proposition whose proof is given in Section 6.5.

**Proposition 17.** Let $0 \leq \gamma \leq 1$ be an arbitrary real number and $p_A^{(1)}$ and $p_A^{(2)}$ be arbitrary distributions on $\mathcal{A}$ such that $\gamma H(p_A^{(1)}) + (1 - \gamma) H(p_A^{(2)}) < H(X|Y)$. Then, for any $\epsilon > 0$, there exists a
natural number \( L \) and a mapping \( \psi : \mathcal{X}^L \to \mathcal{A}^L \) such that

\[
\left\| p_{\mathcal{A}^L,\mathcal{Y}^L}(a^L, y^L) - \frac{1}{L} \sum_{t=1}^{\gamma L} p_A^{(1)}(a_t) \prod_{t=\gamma L+1}^{L} p_A^{(2)}(a_t) \right\|_{TV} < \epsilon,
\]

(13)

where \( A^L = \psi(X^L) \), \((X^L, Y^L)\) are i.i.d. according to \( p(x, y) \) and \( \| \cdot \|_{TV} \) is the total variation distance.

Note that \( p_{\mathcal{Y}^L}(y^L) \prod_{t=1}^{\gamma L} p_A^{(1)}(a_t) \prod_{t=\gamma L+1}^{L} p_A^{(2)}(a_t) \) is the ideal independent actions by Alice, whereas \( p_{A^L,Y^L}(a^L, y^L) \) is the real joint distribution.

Let Alice use the actions \((A_1, A_2, \ldots, A_L)\) in the current block where \( A^L = \psi(X^L) \). Bob’s action at time \( t \) depends on this history and we may represent it by \( p(b_t|y^L, a^{t-1}, b^{t-1}) \). Then, utilizing the following property of total variation for random variables \( Y \) and \( Z \)

\[
\|p_{Y|Z}p_{Z} - q_{Y|Z}p_{Z}\|_{TV} = \|p_{Y} - q_{Y}\|_{TV},
\]

we conclude from (13) that

\[
\left\| p_{\mathcal{A}^L,\mathcal{Y}^L}(a^L, y^L) \prod_{t=1}^{L} p(b_t|y^L, a^{t-1}, b^{t-1}) - p_{\mathcal{Y}^L}(y^L) \prod_{t=1}^{\gamma L} p_A^{(1)}(a_t) p(b_t|y^L, a^{t-1}, b^{t-1}) \prod_{t=\gamma L+1}^{L} p_A^{(2)}(a_t) p(b_t|y^L, a^{t-1}, b^{t-1}) \right\|_{TV} < \epsilon,
\]

(14)

Utilizing the following property of total variation for random variables \( Y \) and \( Z \)

\[
\|p_{Y,Z} - q_{Y,Z}\|_{TV} \geq \|p_{Y} - q_{Y}\|_{TV},
\]

we conclude that the distance between the actual actions \( p_{\mathcal{A}^L,\mathcal{B}^L}(a^L, b^L) \) and the ideal one is less than or equal to \( \epsilon \), i.e.,

\[
\left\| p_{\mathcal{A}^L,\mathcal{B}^L}(a^L, b^L) - \prod_{t=1}^{\gamma L} p_A^{(1)}(a_t) p(b_t|a^{t-1}, b^{t-1}) \prod_{t=\gamma L+1}^{L} p_A^{(2)}(a_t) p(b_t|a^{t-1}, b^{t-1}) \right\|_{TV} < \epsilon.
\]

(15)

By relating the total variation distance to the payoff differences (with a similar derivation as in \((19)\)), we obtain that the payoff under the actual distribution and the ideal one is at most \( \epsilon \) times a constant \( |L\overline{m} - L\underline{m}| \), where \( \overline{m} \) and \( \underline{m} \) are the maximum and minimum entries for each repetition of the game \((T)\). Thus, the distance between the average payoff of the block differs by at most \( \epsilon |\overline{m} - \underline{m}| \) from the average payoff under the ideal distribution. This completes the proof.

Remark 18. We constructed the strategy \( \sigma \) for the case \( T = NL \). In general for \( T = NL + \delta \) where \( \delta < L \) one can extend the first block to contain \( L + \delta \) stages and choose \( N \) large enough to diminish the effect of first block on average payoff.

\( L\overline{m} \) and \( L\underline{m} \) are the maximum and minimum entries of the \( L \) repetitions of the game.
5.2 Bob can defend $J_{\text{cav}}(H(X|Y))$

This is an extension of the proof given in [2]. Let $\sigma$ be an arbitrary strategy for Alice and generate strategy $\tau$ for Bob as follows: given $h_{2}^{t}$, an arbitrary history of observations of Bob until stage $t$, $\tau_{t}(h_{2}^{t})$ is the best choice of Bob that minimizes the expected payoff at stage $t$:

$$\tau_{t}(h_{2}^{t}) \in \arg\min_{j \in B} E_{\sigma} [u_{A_{t},j} | H_{2}^{t} = h_{2}^{t}]$$

where $E_{\sigma}$ denotes expectation with respect to the probability distribution induced by $\sigma$ and $p_{X,Y}$. Thus:

$$E_{\sigma,\tau} [u_{A_{t},B_{t}} | H_{2}^{t} = h_{2}^{t}] \leq J \left(H(A_{t}|H_{2}^{t} = h_{2}^{t})\right) \leq J_{\text{cav}} \left(H(A_{t}|H_{2}^{t} = h_{2}^{t})\right),$$

since conditional on the observations $h_{2}^{t}$ of Bob, Alice’s action $A_{t}$ has entropy $H(A_{t}|H_{2}^{t} = h_{2}^{t})$. Therefore:

$$E_{\sigma,\tau} [u_{A_{t},B_{t}}] = \sum_{h_{2}^{t} \in (A \times B)^{t-1} \times \chi_{2}^{t}} \Pr [H_{2}^{t} = h_{2}^{t}] E_{\sigma,\tau} [u_{A_{t},B_{t}} | H_{2}^{t} = h_{2}^{t}] \leq \sum_{h_{2}^{t} \in (A \times B)^{t-1} \times \chi_{2}^{t}} \Pr [H_{2}^{t} = h_{2}^{t}] J_{\text{cav}} \left(H(A_{t}|H_{2}^{t} = h_{2}^{t})\right) \leq J_{\text{cav}} \left(\sum_{h_{2}^{t} \in (A \times B)^{t-1} \times \chi_{2}^{t}} \Pr [H_{2}^{t} = h_{2}^{t}] H(A_{t}|H_{2}^{t} = h_{2}^{t})\right) \leq J_{\text{cav}} \left(H(A_{t}|H_{2}^{t})\right).$$

The first inequality results from (16) and by using Jensen’s inequality for concave function $J_{\text{cav}}(.)$ the second inequality follows. By definition of $\lambda_{T}(\sigma,\tau)$ and using (17) we have:

$$\lambda_{T}(\sigma,\tau) \leq \sum_{t=1}^{T} \frac{1}{T} J_{\text{cav}} \left(H(A_{t}|H_{2}^{t})\right) \leq J_{\text{cav}} \left(\sum_{t=1}^{T} \frac{1}{T} H(A_{t}|H_{2}^{t})\right) = J_{\text{cav}} \left(\sum_{t=1}^{T} \frac{1}{T} H(A_{t}|Y^{t}, A^{t-1}, B^{t-1})\right) = J_{\text{cav}} \left(\sum_{t=1}^{T} \frac{1}{T} H(A_{t}|Y^{t}, A^{t-1})\right) = J_{\text{cav}} \left(\frac{1}{T} H(A^{T}|Y^{T})\right) \leq J_{\text{cav}} \left(\frac{1}{T} H(X^{T}|Y^{T})\right) = J_{\text{cav}} \left(H(X|Y)\right) \quad (18)$$

where the second inequality follows by using Jensen’s inequality for concave function $J_{\text{cav}}$. Note that given the strategy $\tau$ for Bob, $B^{t-1}$ is a function of $Y^{t}$ and $A^{t-1}$ thus $H(A_{t}|Y^{t}, A^{t-1}, B^{t-1}) = H(A_{t}|Y^{t}, A^{t-1})$ and as $A_{t}$ and $B_{t}$ are causally generated from i.i.d. sequences $X^{T}$ and $Y^{T}$ hence
Take an arbitrary sequence of real numbers \( x, y, \ldots, x_n \) and two probability distributions \( p = (p_1, p_2, \ldots, p_n) \) and \( q = (q_1, q_2, \ldots, q_n) \). Let \( W \) be a random variable that takes value \( x_i \) with probability \( q_i \), and \( \tilde{W} \) be a random variable that takes value \( x_i \) with probability \( p_i \). Then, we have

\[
\chi^2(p, q) \geq \frac{(E[W] - E[\tilde{W}])^2}{\text{Var}[W]}.
\]

Furthermore, the above inequality becomes an equality if we set \( x_i = (p_i - q_i)/q_i \).

Observe that the left hand side of (20) depends only on the probability values \( p_i \) and \( q_i \), while the right hand side depends not only on the probabilities, but also the values that \( W \) and \( \tilde{W} \) take. The proof of this lemma is given in Appendix A. Using this lemma and the fact that \( E[W] < w_2 < w_1 \leq E[\tilde{W}] \), we can conclude

\[
\chi^2(p, q) \geq \frac{(E[W] - w_2)^2}{\text{Var}[W]}.
\]
Observe that $m \leq W \leq \overline{m}$ holds with probability one. The proof is finished by the following lemma.

**Lemma 20.** For any $w_1 > w_2$, we have

$$\frac{(E[W] - w_2)^2}{\text{Var}[W]} \geq \frac{(w_1 - w_2)^2}{(w_1 - m)(\overline{m} - w_1)},$$

provided that $E[W] \geq w_1$, and $m \leq W \leq \overline{m}$.

The proof of this lemma is given in Appendix B.

### 6.2 Proof of Theorem 5

In this section we provide additional details and build a geometric picture. This picture implies Theorem 5, but also gives a geometric interpretation of Nash strategies.

Let

$$L(a_1, a_2, \cdots, a_n) = \text{Nash}(U + a_1^T), \quad \forall a \in \mathbb{R}^n.$$

Observe that the table $\bar{U}$ can be intuitively understood as giving an additional incentive $a_i$ to Alice for playing her $i$-th action (it is actually a disincentive if $a_i < 0$). Also, since

$$L(a_1 + c, a_2 + c, \cdots, a_n + c) = L(a_1, a_2, \cdots, a_n) + c,$$

we only need to understand $L$ when the sum of the incentives $a_i$ is zero.

We need the following definition:

**Definition 21.** Let

$$K(p_1, p_2, \cdots, p_n) = \min \sum_j p_i u_{ij}$$

be the payoff that Alice can guarantee with playing distribution $(p_1, \cdots, p_n)$ with table $U$. We extend the definition of $K(\cdot)$ to arbitrary $(p_1, p_2, \cdots, p_n) \in \mathbb{R}^n$ by setting

$$K(p_1, p_2, \cdots, p_n) = -\infty,$$

when the tuple $(p_1, p_2, \cdots, p_n)$ does not form a valid probability distribution, i.e., when any of the $p_i$’s becomes negative, or $\sum_i p_i \neq 1$.

Note that

$$\mathcal{P}_g(w) = \{ p \mid K(p) \geq w \}.$$

A full geometric picture of $\mathcal{P}_g(w)$ as well as Nash strategies are provided in the following theorem:

**Theorem 22.** We have

1. The function $L(a_1, a_2, \cdots, a_n)$ is the convex conjugate dual of $K(p_1, p_2, \cdots, p_n)$ in the following sense:

$$L(a) = \max_{p \in \mathbb{R}^n} \left[ K(p) + \sum_{i=1}^n p_i a_i \right], \quad \forall a \in \mathbb{R}^n.$$  

The function $L(a_1, a_2, \cdots, a_n)$ is jointly convex in $(a_1, a_2, \cdots, a_n)$, while $K(p_1, p_2, \cdots, p_n)$ is jointly concave in $(p_1, p_2, \cdots, p_n)$. 

16
Furthermore, the supporting hyperplanes to the convex curve $a \mapsto L(a)$ characterize Alice’s Nash strategies as follows: for any arbitrary $a$, $p$ is a Nash strategy of Alice for table $\tilde{U} = U + a\mathbf{1}^T$ if and only if $p$ is a subgradient of the function $L$ at $a$. In other words, take some arbitrary vector $a$. Then,

$$L(b_1, b_2, \ldots, b_n) \geq L(a_1, a_2, \ldots, a_n) + \sum_i (b_i - a_i)p_i, \quad \forall b \in \mathbb{R}^n, \quad (22)$$

if and only if $p$ is a Nash strategy of Alice for the payoff table $\tilde{U} = U + a\mathbf{1}^T$.

2. Given a probability vector $p$, we have

$$L(a_1, a_2, \ldots, a_n) \geq w + \sum_i (a_i - b_i)p_i, \quad \forall a,$n

if and only if $p$ guarantees a payoff of at least $w$ for game $U + b\mathbf{1}^T$. In particular, setting $b_i = 0$,

$$L(a_1, a_2, \ldots, a_n) \geq w + \sum_i a_ip_i, \quad \forall a, \quad (23)$$

if and only if $p$ guarantees a payoff of at least $w$ for game $U$, i.e., $p \in \mathcal{P}_U(w)$. Thus, having a payoff $w$, we look for hyperplanes of the form $w + \sum_i p_i a_i$ that pass through $w$ at $(a_1, a_2, \ldots, a_n) = (0, 0, \ldots, 0)$, and lie below the curve of $L$.

Observe that the second part of Theorem 22 is equivalent with Theorem 5.

Proof of Theorem 22. We begin with the first part of the theorem. Using the max-min formulation for the Nash value of a game $\tilde{U}$, we have

$$L(a_1, a_2, \ldots, a_n) = \max_{p_i \geq 0, \sum_i p_i = 1} \min_j \sum_i p_i (u_{ij} + a_i)$$

$$= \max_{p_i \geq 0, \sum_i p_i = 1} \left[ \left( \min_j \sum_i p_i u_{ij} \right) + \sum_i p_i a_i \right]$$

$$= \max_{p_i \geq 0, \sum_i p_i = 1} \left[ K(p_1, p_2, \ldots, p_n) + \sum_i p_i a_i \right]$$

$$= \max_{p_i \in \mathbb{R}} \left[ K(p_1, p_2, \ldots, p_n) + \sum_i p_i a_i \right]. \quad (24)$$

where (24) follows from the fact that $K(p)$ is minus infinity when $p$ is not a probability distribution. This shows the duality of $L(\cdot)$ and $K(\cdot)$. Next, note that $K(\cdot)$ is a minimum of linear functions; hence it is a concave function. Convexity of $L(\cdot)$ can be directly seen from (22) which implies that at least one supporting hyperplane to its curve exists at any given point (since at least one Nash strategy exists for any arbitrary game). Thus, it remains to prove (22).

Without loss of generality, it suffices to prove (22) for $b = 0$ ($b_i = 0$), and get the result for arbitrary $b$ by changing variable $U \rightarrow U + b\mathbf{1}^T$. The inequality

$$L(a_1, a_2, \ldots, a_n) \geq L(0, 0, \ldots, 0) + \sum_i a_ip_i, \quad \forall a, \quad (25)$$

17
can be also expressed as
\[
\min_a \left( L(a_1, a_2, \ldots, a_n) - \sum_i a_ip_i \right) \geq L(0, 0, \ldots, 0).
\]
From the duality relation (24) and utilizing the Fenchel’s duality theorem, the left hand side is
\[
K(p_1, p_2, \ldots, p_n) \geq L(0, 0, \ldots, 0) = \text{Nash}(U),
\]
which is equivalent with \( p \) being a Nash strategy.

To proof for the second part of the theorem is similar. As before \( b_i \) can be set to zero. Then,
we can express (23) as
\[
\min_a \left( L(a_1, a_2, \ldots, a_n) - \sum_i a_ip_i \right) \geq w.
\]
From the duality relation (24) and the Fenchel’s duality theorem, this is equivalent with
\[
K(p_1, p_2, \ldots, p_n) \geq w,
\]
or \( p \in \mathcal{P}_U(w) \).

### 6.3 Proof of Theorem 8

Let \( X \) and \( Y \) be r.v.s representing the actions of player \( A \) in game \( U \oplus U \) with distribution \( p_{XY} \).
Note that if an arbitrary distribution \( q_X(x) \) secures payoff \( w/2 \) in game \( U \) then \( q_{X,Y}(x, y) = 1(x = y)q_X(x) \) secures payoff \( w \) in game \( U \oplus U \), where \( 1(,) \) is indicator function. This is because the expected value of the sum payoff is the sum of the expected values of the payoffs of the two games.

Note that since \( X = Y \) and \( H(X,Y) = H(X) \), the function \( F_{U \oplus U}(w) \) is bounded above as follows:
\[
F_{U \oplus U}(w) \leq F_U(w/2) \quad (26)
\]
On the other hand, let \( p^*_{XY} \in \mathcal{P}_{U \oplus U}(w) \) be a distribution with minimum entropy that secures a payoff \( w \) in game \( U \oplus U \), i.e., \( H(p^*_{XY}) = F_{U \oplus U}(w) \). Note that such a distribution \( p^*_{XY} \) exist because \( \mathcal{P}_{U \oplus U}(w) \) is compact and closed. We have
\[
w \leq \min_{j_1,j_2 \in \mathcal{B}} \mathbb{E}_{p^*_{XY}}[u_{X,j_1} + u_{Y,j_2}] \quad (27)
\]
\[
= \min_{j_1,j_2 \in \mathcal{B}} \left( \mathbb{E}_{p^*_{XY}}[u_{X,j_1}] + \mathbb{E}_{p^*_{XY}}[u_{Y,j_2}] \right) \quad (28)
\]
\[
= \min_{j_1 \in \mathcal{B}} \mathbb{E}_{p^*_{X}}[u_{X,j_1}] + \min_{j_2 \in \mathcal{B}} \mathbb{E}_{p^*_{Y}}[u_{Y,j_2}] \quad (29)
\]
As a result, there exists \( k \in \{1, 2\} \) such that
\[
\min_{j_k \in \mathcal{B}} \mathbb{E}_{p^*_{X_k}}[u_{X_k,j_k}] \geq \frac{w}{2}. \quad (30)
\]
Thus, \( p^*_{X_k} \) secures payoff \( w/2 \) in game \( U \). Hence,
\[
F_U(w) = H(p^*_{XY}) \overset{(a)}{=} H(p^*_{X_k}) \geq F_U(w/2), \quad (31)
\]
where \( (a) \) follows from properties of entropy.

Equations (26) and (31) conclude \( F_{U \oplus U}(w) = F_U(w/2) \). The above line of proof can be extended for every natural number \( k \) to prove that \( F_{U \oplus U}(w) = F_U(w/k) \).
6.4 Proof of Theorem 12

Let $p^*$ be a Nash strategy for player A where $H(p^*) = h^*$, and $i^* \in \arg \max_{i \in A} \min_{j \in B} u_{ij}$ be the pure strategy that guarantees payoff $v$ for player A. For $v \leq w \leq w^*$ define $\alpha = (w^* - w)/(w^* - v)$ and $p = \alpha e_{i^*} + (1 - \alpha)p^*$ where $e_{i^*}$ is a vertical vector of all zero elements except for its $i^*$th element which is 1. The pmf $p$ guarantees payoff $w$ since

$$p^T U = \alpha e_{i^*}^T U + (1 - \alpha)p^T U \geq \alpha v 1 + (1 - \alpha)w^* 1 = w 1$$

Using properties of entropy one can inspect that:

$$H(p) \leq \alpha H(e_{i^*}) + (1 - \alpha)H(p^*) + H(\alpha, 1 - \alpha) = (1 - \alpha)h^* - \alpha \log_2(\alpha) - (1 - \alpha) \log_2(1 - \alpha).$$

Therefore $F_0(w) \leq H(p) \leq (1 - \alpha)h^* - \alpha \log_2(\alpha) - (1 - \alpha) \log_2(1 - \alpha)$. Additionally, as $h^*$ secures payoff $w^* \geq w$ then $F_0(w) \leq h^*$

These two facts imply $F_0(w) \leq Q_0(1)(w)$ once we substitute the value of $\alpha$.

From the definition of $p_{\text{max},i}$ it follows that $p_{\text{max},i} \in \mathcal{P}(w)$. Therefore for every $i \in A$, $F_0(w) \leq H(p_{\text{max},i})$ and $F_0(w) \leq Q_0(2)(w)$ follows.

For an arbitrary $j \in B$ if $p' \in \{p \in \mathcal{P}(w) : p^T U e_j = w\}$ then as $p'$ also belongs to $\mathcal{P}(w)$ we have $F_0(w) \leq H(p')$. Then, for every $j \in B$:

$$F_0(w) \leq \max_{p \in \mathcal{P}(w) : p^T U e_j = w} H(p)$$

As the above inequality is correct for every $j \in B$, $F_0(w) \leq Q_0(3)(w)$.

6.5 Proof of Proposition 17

To prove Proposition 17 we make use of the following lemmas. Lemma 23 is a direct consequence of [20] Theorem 1] and Lemma 24 is adopted from [21] p.110].

**Lemma 23.** Consider the correlated random sequences $X^L$ and $Y^L$ drawn i.i.d. from respective spaces $X$ and $Y$ by joint probability distribution $p_{X,Y}$. Let $Q^{(L)}$ be a random variable independent of $Y^L$ and uniformly distributed on $\{1, 2, \ldots, 2^{RL}\}$ where $R < H(X|Y)$ is a real number, then there exists a mapping $B : \mathcal{X}^L \rightarrow \{1, 2, \ldots, 2^{RL}\}$ such that

$$\lim_{L \rightarrow \infty} d_1 \left( p_{B(X^L)Y^L, Q^{(L)}Y^L} \right) = 0.$$

**Lemma 24.** Let $X^L$ and $Y^L$ be arbitrary general sequences drawn from $X$ and $Y$ respectively. There exists a mapping $\phi : \mathcal{X}^L \rightarrow \mathcal{Y}^L$ satisfying $\lim_{L \rightarrow \infty} d_1 \left( p_{Y^L, \phi(X^L)} \right) = 0$ provided that $H(X) > H(Y)$, where $H(X)$ and $H(Y)$ are defined as follows.

$$H(X) = p\liminf_{L \rightarrow \infty} \frac{1}{L} \log \frac{1}{p_{X^L}(X^L)}$$

$$H(Y) = p\limsup_{L \rightarrow \infty} \frac{1}{L} \log \frac{1}{p_{Y^L}(Y^L)}$$

while for a random sequence $\{Z_t\}$,

$$p\liminf_{t \rightarrow \infty} Z_t = \sup \left\{ \beta \mid \lim_{t \rightarrow \infty} \Pr[Z_t < \beta] = 0 \right\}$$

$$p\limsup_{t \rightarrow \infty} Z_t = \inf \left\{ \beta \mid \lim_{t \rightarrow \infty} \Pr[Z_t > \beta] = 0 \right\}.$$
Choose a real number $R$ such that $\gamma H(p_A^{(1)}) + (1-\gamma) H(p_A^{(2)}) < R < H(X|Y)$ and $LR$ is a natural number (for a sufficiently large $L$).

We define random variables $Q^{(L)}$ and $\hat{A}^L$ that are mutually independent of each other, and of $Y^L$ with the following marginal distributions: let $Q^{(L)}$ be a uniformly distributed random variable on $\{1, 2, \ldots, 2^{RL}\}$, and $\hat{A}^L$ be distributed as follows:

$$p_{\hat{A}^L}(a^L) = \left\lceil \gamma L \right\rceil \prod_{t=1}^{L} p_A^{(1)}(a_t) \prod_{t=\lceil \gamma L \rceil + 1}^{L} p_A^{(2)}(a_t)$$

where $\lceil a \rceil$ is the smallest integer greater than or equal to $a$. Note that $R < H(X|Y)$; thus according to Lemma 23 there exists a mapping $B : \mathcal{X}^L \to \{1, 2, \ldots, 2^{RL}\}$ satisfying

$$\lim_{L \to \infty} d_1\left(p_{B(X^L)}Y^L, p_Q^{(L)} Y^L\right) = 0.$$  \hspace{1cm} (32)

On the other hand we have

$$\text{p-} \limsup_{L \to \infty} \frac{1}{L} \log \frac{1}{p_{\hat{A}^L}(A^L)} = \gamma H(p_A^{(1)}) + (1-\gamma) H(p_A^{(2)}) < \text{p-} \liminf_{L \to \infty} \frac{1}{L} \log \frac{1}{p_Q^{(L)}(Q^L)},$$

therefore according to lemma 24 there exists a mapping $\varphi : \{1, 2, \ldots, 2^{RL}\} \to A^L$ such that

$$\lim_{L \to \infty} d_1\left(p_{\varphi(Q^{(L))}}Y^L, p_{\hat{A}^L} Y^L\right) = 0.$$  \hspace{1cm} (33)

Considering the fact that $\varphi(Q^{(L)})$ and $\hat{A}^L$ both are independent of $Y^L$, the above equation results in

$$\lim_{L \to \infty} d_1\left(p_{\varphi(Q^{(L)})}Y^L, p_{\hat{A}^L} Y^L\right) = 0.$$  \hspace{1cm} (34)

Furthermore note that

$$d_1\left(p_{\varphi(B(X^L))Y^L, p_{\hat{A}^L} Y^L}\right) \leq d_1\left(p_{\varphi(B(X^L))Y^L, p_{\varphi(Q^{(L))})} Y^L\right) + d_1\left(p_{\varphi(Q^{(L)})}Y^L, p_{\hat{A}^L} Y^L\right) \leq d_1\left(p_{B(X^L))Y^L, p_{\varphi(Q^{(L)})} Y^L\right) + d_1\left(p_{\varphi(Q^{(L)})}Y^L, p_{\hat{A}^L} Y^L\right)$$

where the first inequality follows from the triangular inequality for total variation and the second inequality holds because

$$d_1\left(f(Y), f(Z)\right) \leq d_1(Y, Z)$$

for any arbitrary deterministic function $f(\cdot)$ on the sample space of r.v.s $Y$ and $Z$. Let $A^L = \psi(X^L) = \varphi\left(B\left(X^L\right)\right)$. Then by combining equations (32), (33) and (34) we have

$$\lim_{L \to \infty} d_1\left(p_{A^L} Y^L, p_{\hat{A}^L} Y^L\right) = 0.$$  \hspace{1cm} (35)

Thus $\psi(\cdot) = \varphi(B(\cdot))$ is the desired mapping.
References

[1] J. F. Nash, “Equilibrium points in n-person games,” Proc. Nat. Acad. Sci. USA 36.1 (1950): 48-49.

[2] O. Gossner, N. Vieille, “How to play with a biased coin?” Games and Economic Behavior, 41(2), 206-226, 2002.

[3] A. Neyman and D. Okada, “Repeated games with bounded entropy,” Games and Economic Behavior, 30(2), 228-247, 2000.

[4] A. Neyman, D. Okada, “Growth of strategy sets, entropy, and nonstationary bounded recall,” Games and Economic Behavior, 66(1), 404-425, 2009.

[5] P. Hubacek, M. Naor, and J. Ullman. “When Can Limited Randomness Be Used in Repeated Games?” International Symposium on Algorithmic Game Theory. Springer Berlin Heidelberg, 2015, 259-271.

[6] M. Budinich and L. Fortnow, “Repeated matching pennies with limited randomness,” Proceedings of the 12th ACM conference on Electronic commerce. ACM, 2011, 111-118.

[7] S. C. Fang, J. R. Rajasekera and H. S. J. Tsao, “Entropy optimization and mathematical programming,” Vol. 8, Springer Science & Business Media, 2012.

[8] T. M. Cover and J. A. Thomas, “Elements of information theory,” John Wiley & Sons, 2012.

[9] J. N. Kapur, G. Baciu, and H. K. Kesavan, “The MinMax Information Measure,” Int. J. Systems Sci., vol. 26, pp. 112, 1995.

[10] S. Watanabe, “Pattern Recognition as a Quest for Minimum Entropy,” Pattern Recognition, vol. 13, pp. 381-387, 1981.

[11] M. Kocaoglu, A. G. Dimakis, S. Vishwanath and B. Hassibi, “Entropic Causal Inference, in: 31st AAAI Conference on Artificial Intelligence (AAAI-17), to appear. Also: arXiv: 1611.04035.

[12] F. Cicalese, L. Gargano, U. Vaccaro, “How to Find a Joint Probability Distribution of Minimum Entropy (almost), given the Marginals,” arXiv: 1701.05243.

[13] M. Kovacevic, I. Stanojevic, and V. Senk, “On the Entropy of Couplings, Information and Computation, Vol. 242, (2015) 369382.

[14] P. W. Shor, “Equivalence of additivity questions in quantum information theory,” Communications in Mathematical Physics, 246(3), 453-472, 2004.

[15] M. Kovacevic, I. Stanojevic, V. Senk, “On the hardness of entropy minimization and related problems,” In Information Theory Workshop (ITW), 512-516, 2012.

[16] M. Srikanth, H. K. Kesavan, P. Roe, “Computation of the MinMax Measure,” in Entropy Measures, Maximum Entropy Principle and Emerging Applications, Springer Berlin Heidelberg, pp. 239–251, 2003.

[17] Y. Narahari, “Game Theory and Mechanism Design,” Vol. 4. World Scientific, 2014.
A Proof of Lemma 19

We would like to prove that

\[ \chi^2(p, q) \geq \frac{(E[W] - E[\tilde{W}])^2}{\text{Var}[W]}, \tag{36} \]

where \( W \sim q \) and \( \tilde{W} \sim p \) are defined on some arbitrary set \( X \). To the best of our knowledge, this inequality has not appeared in the game theory or information theory literature before. We had a direct proof of it, until we found out that it can be derived from a result of [22] published in a math journal in 2006. According to [22, Lemma 1], we have

\[ \chi^2(p, q) \geq E[W] - E[\tilde{W}] - \frac{1}{4}E[W^2]. \tag{37} \]

Since \( \text{(37)} \) holds for all \( W \) and \( \tilde{W} \), let us apply the transformation \( W \mapsto a(W - E[W]) \), and \( \tilde{W} \mapsto a(W - E[\tilde{W}]) \). This shows that for any real \( a \), we have

\[ \chi^2(p, q) \geq a \left( E[W] - E[\tilde{W}] \right) - \frac{a^2}{4} \text{Var}[W]. \tag{38} \]

The right hand side is a quadratic expression in terms of \( a \), and reaches its maximum at

\[ a = \frac{2 \left( E[W] - E[\tilde{W}] \right)}{\text{Var}[W]}. \]

Substituting this value of \( a \) into \( \text{(38)} \), we get the desired result. The second part of the theorem that \( \text{(36)} \) becomes an equality for \( x_i = (p_i - q_i)/q_i \) can be verified directly.
B Proof of Lemma 20

Let us minimize the expression \((\mathbb{E}[X] - w_2)^2/\text{Var}[X]\) over all r.v.s \(X\) that satisfy \(m \leq X \leq \overline{m}\) and \(\mathbb{E}[X] \geq w_1\):

\[
\min_{m \leq X \leq \overline{m}} \frac{(\mathbb{E}[X] - w_2)^2}{\text{Var}[X]} = \min_{w_1 \leq \mu \leq \overline{m}} \left( \frac{\min_{m \leq X \leq \overline{m}} (\mathbb{E}[X] - w_2)^2}{\text{Var}[X]} \right) = \min_{w_1 \leq \mu \leq \overline{m}} \left( \frac{(\mu - w_2)^2}{\max_{m \leq X \leq \overline{m}} \text{Var}[X]} \right)
\]

\[
= \min_{w_1 \leq \mu \leq \overline{m}} \left( \frac{(\mu - w_2)^2}{-\mu^2 + \max_{m \leq X \leq \overline{m}} \mathbb{E}[X]^2} \right). \tag{39}
\]

We claim that

\[
\max_{m \leq X \leq \overline{m}} \mathbb{E}[X]^2 = (\overline{m} - \mu)(\mu - m) + \mu^2. \tag{40}
\]

Observe that if \(X^*\) is the following binary random variable

\[
\mathbb{P}[X^* = m] = \frac{\overline{m} - \mu}{\overline{m} - m}, \quad \mathbb{P}[X^* = \overline{m}] = \frac{\mu - m}{\overline{m} - m}
\]

we have \(\mathbb{E}[X^*] = \mu\) and \(\mathbb{E}[(X^*)^2] = (\overline{m} - \mu)(\mu - m) + \mu^2\). As a result,

\[
\max_{m \leq X \leq \overline{m}} \mathbb{E}[X]^2 \geq (\overline{m} - \mu)(\mu - m) + \mu^2. \tag{42}
\]

On the other hand, the function \(f(x) = x^2\) is convex and lies below the line that connects the two points \((m, m^2)\) and \((\overline{m}, \overline{m}^2)\) for any \(x \in [m, \overline{m}]\), i.e.,

\[
x^2 \leq m^2 + (x - m)(\overline{m} + m), \quad \forall x \in [m, \overline{m}].
\]

Thus,

\[
\mathbb{E}[X^2] \leq m^2 + (\mathbb{E}[X] - m)(\overline{m} + m) = (\overline{m} - \mu)(\mu - m) + \mu^2.
\]

Thus, equation (40) holds. As a result, equation (39) becomes

\[
\min_{m \leq X \leq \overline{m}} \frac{(\mathbb{E}[X] - w_2)^2}{\text{Var}[X]} = \min_{w_1 \leq \mu \leq \overline{m}} g(\mu), \tag{43}
\]

where

\[
g(\mu) = \frac{(\mu - w_2)^2}{(\overline{m} - \mu)(\mu - m)}.
\]

Note that the function \(g(\cdot)\) is increasing for any \(\mu\) satisfying \(m \leq w_2 \leq \mu \leq \overline{m}\) as

\[
\frac{dg(\mu)}{d\mu} = \frac{(\mu - w_2) [((\overline{m} - \mu)(\mu + w_2 - 2m) + (\mu - m)(\mu - w_2)]}{(\overline{m} - \mu)^2(\mu - m)^2} \geq 0.
\]

Since \(w_2 \leq w_1\), this would then imply that the minimum on the right hand side of (43) is obtained at \(\mu = w_1\). This will complete the proof.