Adversarial Leakage in Games

Yuval Emek

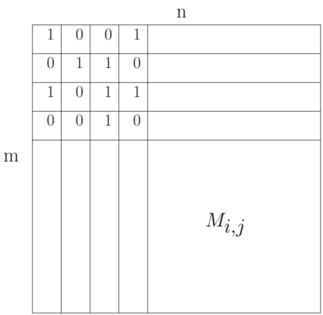
Microsoft Israel R&D Center

Innovations in Computer Science 2009

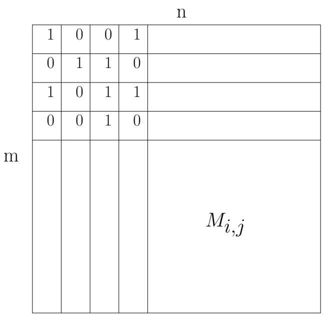
Joint work with
Noga Alon, Michal Feldman, Moshe Tennenholtz

Two-player zero-sum (binary) games

Two-player zero-sum (binary) games



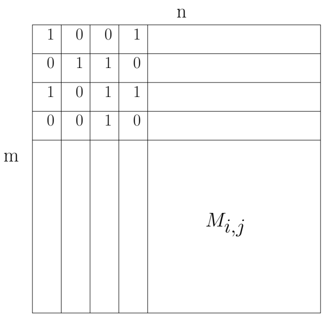
Two-player zero-sum (binary) games



ROW ("good guy") plays some row $i \in [m]$.

COL (adversary) plays some column $j \in [n]$.

Two-player zero-sum (binary) games

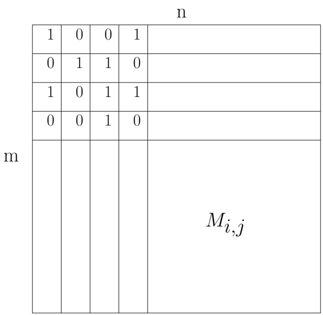


ROW ("good guy") plays some row $i \in [m]$.

COL (adversary) plays some column $j \in [n]$.

ROW wins if $M_{i,j} = 1$; looses if $M_{i,j} = 0$.

Two-player zero-sum (binary) games



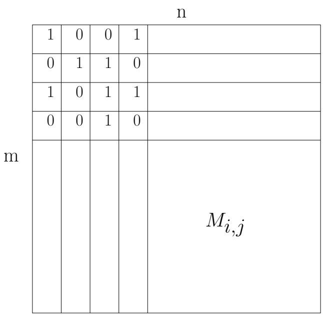
ROW ("good guy") plays some row $i \in [m]$.

COL (adversary) plays some column $j \in [n]$.

ROW wins if $M_{i,j} = 1$; looses if $M_{i,j} = 0$.

When mixed strategies are allowed, it doesn't matter who plays first:

Two-player zero-sum (binary) games



ROW ("good guy") plays some row $i \in [m]$.

COL (adversary) plays some column $j \in [n]$.

ROW wins if $M_{i,j} = 1$; looses if $M_{i,j} = 0$.

When mixed strategies are allowed, it doesn't matter who plays first:

Theorem (von Neumann, 1928)

$$\max_{p \in \Delta(m)} \min_{j \in [n]} \sum_{i \in [m]} p(i) \cdot M_{i,j} = \min_{q \in \Delta(n)} \max_{i \in [m]} \sum_{j \in [n]} q(j) \cdot M_{i,j} .$$

This is defined to be the value of the game, denoted $\mathrm{v}(M)$ = *the probability that ROW wins.*

Information leakage

- Implicit assumption:
  COL may know ROW's mixed strategy — some distribution $p \in \Delta(m)$ — but the coin tosses of ROW are private.

Information leakage

- Implicit assumption:
  COL may know ROW's mixed strategy — some distribution $p \in \Delta(m)$ — but the coin tosses of ROW are private.
- In particular, COL doesn't know the instantiation of p = the pure action $i \in [m]$ that ROW is going to play.

Information leakage

- Implicit assumption:
  COL may know ROW's mixed strategy — some distribution $p \in \Delta(m)$ — but the coin tosses of ROW are private.
- In particular, COL doesn't know the instantiation of p = the pure action $i \in [m]$ that ROW is going to play.
- In some scenarios it is impractical to assume that our opponent knows nothing about our (pure) choices (espionage).

Information leakage

- Implicit assumption:
  COL may know ROW's mixed strategy — some distribution $p \in \Delta(m)$ — but the coin tosses of ROW are private.
- In particular, COL doesn't know the instantiation of p = the pure action $i \in [m]$ that ROW is going to play.
- In some scenarios it is impractical to assume that our opponent knows nothing about our (pure) choices (espionage).
- Information leakage = COL decides on her action after learning b bits of information about the pure action of ROW.

Information leakage

- Implicit assumption:
  COL may know ROW's mixed strategy — some distribution $p \in \Delta(m)$ — but the coin tosses of ROW are private.
- In particular, COL doesn't know the instantiation of p = the pure action $i \in [m]$ that ROW is going to play.
- In some scenarios it is impractical to assume that our opponent knows nothing about our (pure) choices (espionage).
- Information leakage = COL decides on her action after learning b bits of information about the pure action of ROW.
- Question 1:
  what should ROW do now that she knows that COL may learn b bits of information about her pure action?

Information leakage

- Implicit assumption:
  COL may know ROW's mixed strategy — some distribution $p \in \Delta(m)$ — but the coin tosses of ROW are private.
- In particular, COL doesn't know the instantiation of p = the pure action $i \in [m]$ that ROW is going to play.
- In some scenarios it is impractical to assume that our opponent knows nothing about our (pure) choices (espionage).
- Information leakage = COL decides on her action after learning b bits of information about the pure action of ROW.
- Question 1:
  what should ROW do now that she knows that COL may learn b bits of information about her pure action?
- Question 2:
  what happens to the value of the game (probability that ROW wins)?

Strong vs. weak leakage

- Information leakage is formalized in terms of *b* predicates, merged into a function

$$f : [m] \rightarrow \{0, 1\}^b \ .$$

Strong vs. weak leakage

- Information leakage is formalized in terms of b predicates, merged into a function
$$f : [m] \rightarrow \{0,1\}^b .$$

- Let $i \in [m]$ be the action that ROW is going to play.

Strong vs. weak leakage

- Information leakage is formalized in terms of b predicates, merged into a function
$$f : [m] \to \{0,1\}^b \ .$$

- Let $i \in [m]$ be the action that ROW is going to play.
- COL sees $f(i)$ before she decides on her action $j \in [n]$.

Strong vs. weak leakage

- Information leakage is formalized in terms of b predicates, merged into a function
$$f : [m] \rightarrow \{0, 1\}^b \ .$$

- Let $i \in [m]$ be the action that ROW is going to play.
- COL sees $f(i)$ before she decides on her action $j \in [n]$.
- Strong model of leakage: COL decides on $f : [m] \rightarrow \{0, 1\}^b$ when she already knows the mixed strategy p of ROW.

Strong vs. weak leakage

- Information leakage is formalized in terms of b predicates, merged into a function
$$f : [m] \rightarrow \{0, 1\}^b \ .$$

- Let $i \in [m]$ be the action that ROW is going to play.
- COL sees $f(i)$ before she decides on her action $j \in [n]$.
- Strong model of leakage: COL decides on $f : [m] \rightarrow \{0, 1\}^b$ when she already knows the mixed strategy p of ROW.
- Weak model of leakage: COL decides on $f : [m] \rightarrow \{0, 1\}^b$ without knowing the mixed strategy p of ROW.

Strong vs. weak leakage — cont.

Strong leakage:

Weak leakage:

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

Weak leakage:

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \rightarrow \{0, 1\}^b$ (knowing M, b, and p).

Weak leakage:

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M and b).

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M and b).

(2) ROW decides on $p \in \Delta(M)$ (knowing M, b, and f).

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \rightarrow \{0,1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \rightarrow \{0,1\}^b$ (knowing M and b).

(2) ROW decides on $p \in \Delta(M)$ (knowing M, b, and f).

(3) ROW chooses $i \in_p [m]$.

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \rightarrow \{0, 1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \rightarrow \{0, 1\}^b$ (knowing M and b).

(2) ROW decides on $p \in \Delta(M)$ (knowing M, b, and f).

(3) ROW chooses $i \in_p [m]$.

(4) COL decides on $j \in [n]$ (knowing M, b, p, and $f(i)$).

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \rightarrow \{0,1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \rightarrow \{0,1\}^b$ (knowing M and b).

(2) ROW decides on $p \in \Delta(M)$ (knowing M, b, and f).

(3) ROW chooses $i \in_p [m]$.

(4) COL decides on $j \in [n]$ (knowing M, b, p, and $f(i)$).

(5) ROW wins iff $M_{i,j} = 1$.

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M and b).

(2) ROW decides on $p \in \Delta(M)$ (knowing M, b, and f).

(3) ROW chooses $i \in_p [m]$.

(4) COL decides on $j \in [n]$ (knowing M, b, p, and $f(i)$).

(5) ROW wins iff $M_{i,j} = 1$.

Convenient to formalize the (pure) decision of COL in step (4) as a function $g : \{0,1\}^b \to [n]$.

Strong vs. weak leakage — cont.

Strong leakage:

(1) ROW decides on $p \in \Delta(m)$ (knowing M and b).

(2) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M, b, and p).

Weak leakage:

(1) COL decides on $f : [m] \to \{0,1\}^b$ (knowing M and b).

(2) ROW decides on $p \in \Delta(M)$ (knowing M, b, and f).

(3) ROW chooses $i \in_p [m]$.

(4) COL decides on $j \in [n]$ (knowing M, b, p, and $f(i)$).

(5) ROW wins iff $M_{i,j} = 1$.

Convenient to formalize the (pure) decision of COL in step (4) as a function $g : \{0,1\}^b \to [n]$.

ROW wins (step (5)) iff $M_{i,g(f(i))} = 1$.

New game values

New game values

The value of the game M under b leaking bits in the strong model:

$$\mathrm{v}^{\mathsf{s}}(M, b) = \max_{p \in \Delta(m)} \min_{f:[m] \rightarrow \{0,1\}^b} \min_{g:\{0,1\}^b \rightarrow [n]} \sum_{i \in [m]} p(i) \cdot M_{i, g(f(i))} \ .$$

New game values

The value of the game M under b leaking bits in the strong model:

$$\mathrm{v}^{\mathsf{s}}(M, b) = \max_{p \in \Delta(m)} \min_{f:[m] \rightarrow \{0,1\}^b} \min_{g:\{0,1\}^b \rightarrow [n]} \sum_{i \in [m]} p(i) \cdot M_{i, g(f(i))} \ .$$

$p_b^* =$ a mixed strategy of ROW that realizes $\mathrm{v}^{\mathsf{s}}(M, b)$.

New game values

The value of the game M under b leaking bits in the strong model:

$$\mathrm{v}^{\mathsf{s}}(M, b) = \max_{p \in \Delta(m)} \min_{f:[m] \to \{0,1\}^b} \min_{g:\{0,1\}^b \to [n]} \sum_{i \in [m]} p(i) \cdot M_{i, g(f(i))} \ .$$

$p_b^* =$ a mixed strategy of ROW that realizes $\mathrm{v}^{\mathsf{s}}(M, b)$.

The value of the game M under b leaking bits in the weak model:

$$\mathrm{v}^{\mathsf{w}}(M, b) = \min_{f:[m] \to \{0,1\}^b} \max_{p \in \Delta(m)} \min_{g:\{0,1\}^b \to [n]} \sum_{i \in [m]} p(i) \cdot M_{i, g(f(i))} \ .$$

New game values

The value of the game M under b leaking bits in the strong model:

$$\mathrm{v}^{\mathsf{s}}(M, b) = \max_{p \in \Delta(m)} \min_{f:[m] \to \{0,1\}^b} \min_{g:\{0,1\}^b \to [n]} \sum_{i \in [m]} p(i) \cdot M_{i, g(f(i))} .$$

$p_b^* =$ a mixed strategy of ROW that realizes $\mathrm{v}^{\mathsf{s}}(M, b)$.

The value of the game M under b leaking bits in the weak model:

$$\mathrm{v}^{\mathsf{w}}(M, b) = \min_{f:[m] \to \{0,1\}^b} \max_{p \in \Delta(m)} \min_{g:\{0,1\}^b \to [n]} \sum_{i \in [m]} p(i) \cdot M_{i, g(f(i))} .$$

Clearly, $\mathrm{v}^{\mathsf{s}}(M, b) \leq \mathrm{v}^{\mathsf{w}}(M, b) \leq \mathrm{v}(M)$ for every game M and $b \geq 0$.

Strong leakage

Strong leakage

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then the original maximin strategy of* ROW *guarantees* $\mathrm{v}^s(M, b) \geq 1 - 2^b\epsilon$.

Strong leakage

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then the original maximin strategy of* ROW *guarantees* $\mathrm{v}^s(M, b) \geq 1 - 2^b \epsilon$.

There are examples showing that this is essentially tight.

Strong leakage

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then the original maximin strategy of* ROW *guarantees* $\mathrm{v}^s(M, b) \geq 1 - 2^b \epsilon$.

There are examples showing that this is essentially tight.

Corollary

If $\mathrm{v}(M) = 1 - \epsilon$ *and* $b \leq \lg(1/\epsilon) - 1$, *then* $\mathrm{v}^s(M, b) \geq 1/2$.

Strong leakage — cont.

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then* $\mathrm{v}^s(M, b) \leq (1 - \epsilon)^{2^b}$.

Strong leakage — cont.

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then* $\mathrm{v}^s(M, b) \leq (1 - \epsilon)^{2^b}$.

There are examples showing that this is essentially tight as well.
(Explicit construction soon.)

Strong leakage — cont.

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then* $\mathrm{v}^s(M, b) \leq (1 - \epsilon)^{2^b}$.

There are examples showing that this is essentially tight as well. (Explicit construction soon.)

Corollary

If $\mathrm{v}(M) = 1 - \epsilon$ *and* $b \geq \lg(1/\epsilon) + 2$, *then* $\mathrm{v}^s(M, b) \leq e^{-4} < 0.02$.

Strong leakage — cont.

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then* $\mathrm{v}^s(M, b) \leq (1 - \epsilon)^{2^b}$.

There are examples showing that this is essentially tight as well. (Explicit construction soon.)

Corollary

If $\mathrm{v}(M) = 1 - \epsilon$ *and* $b \geq \lg(1/\epsilon) + 2$, *then* $\mathrm{v}^s(M, b) \leq e^{-4} < 0.02$.

Hence the sequence $\{\mathrm{v}^s(M, b)\}_{b=1,2,\ldots}$ exhibits a sharp threshold:

Strong leakage — cont.

Theorem

If $\mathrm{v}(M) = 1 - \epsilon$, *then* $\mathrm{v}^s(M, b) \leq (1 - \epsilon)^{2^b}$.

There are examples showing that this is essentially tight as well.
(Explicit construction soon.)

Corollary

If $\mathrm{v}(M) = 1 - \epsilon$ *and* $b \geq \lg(1/\epsilon) + 2$, *then* $\mathrm{v}^s(M, b) \leq e^{-4} < 0.02$.

Hence the sequence $\{\mathrm{v}^s(M, b)\}_{b=1,2,\ldots}$ exhibits a sharp threshold:
it is $\geq 1/2$ as long as $b \leq \lg(1/\epsilon) - 1$;
it is < 0.02 once $b \geq \lg(1/\epsilon) + 2$.

Explicit construction

Lemma

There exists an infinite sequence of games $M \in \{0,1\}^{m \times m}$, $\mathrm{v}(M) = q(1 \pm o(1))$, *so that if* $b \leq \lg \lg(m) - O(1)$, *then* $\mathrm{v}^s(M, b) \geq q^{2^b}(1 \pm o(1))$.

Explicit construction

Lemma

There exists an infinite sequence of games $M \in \{0,1\}^{m \times m}$, $\mathrm{v}(M) = q(1 \pm o(1))$, *so that if* $b \leq \lg \lg(m) - O(1)$, *then* $\mathrm{v}^s(M, b) \geq q^{2^b}(1 \pm o(1))$.

Prove for $q = 1/2$;
can be easily generalized for any $q = 1/p$ for a prime power p.

Explicit construction

Lemma

There exists an infinite sequence of games $M \in \{0,1\}^{m \times m}$, $\mathrm{v}(M) = q(1 \pm o(1))$, so that if $b \leq \lg\lg(m) - O(1)$, then $\mathrm{v}^s(M, b) \geq q^{2^b}(1 \pm o(1))$.

Prove for $q = 1/2$;
can be easily generalized for any $q = 1/p$ for a prime power p.

- Let r be a sufficiently large integer.

Explicit construction

Lemma

There exists an infinite sequence of games $M \in \{0,1\}^{m \times m}$, $\mathrm{v}(M) = q(1 \pm o(1))$, *so that if* $b \leq \lg\lg(m) - O(1)$, *then* $\mathrm{v}^s(M, b) \geq q^{2^b}(1 \pm o(1))$.

Prove for $q = 1/2$;
can be easily generalized for any $q = 1/p$ for a prime power p.

- Let r be a sufficiently large integer.
- Fix $m = 2^r - 1$.

Explicit construction

Lemma

There exists an infinite sequence of games $M \in \{0,1\}^{m \times m}$, $\mathrm{v}(M) = q(1 \pm o(1))$, *so that if* $b \leq \lg\lg(m) - O(1)$, *then* $\mathrm{v}^s(M, b) \geq q^{2^b}(1 \pm o(1))$.

Prove for $q = 1/2$;
can be easily generalized for any $q = 1/p$ for a prime power p.

- Let r be a sufficiently large integer.
- Fix $m = 2^r - 1$.
- The m rows (and columns) of M are indexed by all non-zero r-dimensional vectors over $GF(2)$.

Explicit construction

Lemma

There exists an infinite sequence of games $M \in \{0,1\}^{m \times m}$, $\mathrm{v}(M) = q(1 \pm o(1))$, *so that if* $b \leq \lg \lg(m) - O(1)$, *then* $\mathrm{v}^s(M, b) \geq q^{2^b}(1 \pm o(1))$.

Prove for $q = 1/2$;
can be easily generalized for any $q = 1/p$ for a prime power p.

- Let r be a sufficiently large integer.
- Fix $m = 2^r - 1$.
- The m rows (and columns) of M are indexed by all non-zero r-dimensional vectors over $GF(2)$.
- $M_{u,v} = 1$ iff the vectors u and v are orthogonal over $GF(2)$.

Explicit construction — cont.

Observation

Every row and column of M contain exactly $2^{r-1} - 1$ 1-entries.

Explicit construction — cont.

Observation

Every row and column of M contain exactly $2^{r-1} - 1$ 1-entries.

Corollary

$\mathrm{v}(M) = \frac{2^{r-1}-1}{2^r-1} = \frac{1}{2}(1 - o(1))$.

Explicit construction — cont.

Observation

Every row and column of M contain exactly $2^{r-1} - 1$ 1-entries.

Corollary

$\mathrm{v}(M) = \frac{2^{r-1}-1}{2^r-1} = \frac{1}{2}(1 - o(1))$.

- Take any column subset J, $|J| = 2^b \leq r(1 - \Omega(1))$.

Explicit construction — cont.

Observation

Every row and column of M contain exactly $2^{r-1} - 1$ 1-entries.

Corollary

$\mathrm{v}(M) = \frac{2^{r-1}-1}{2^r-1} = \frac{1}{2}(1 - o(1))$.

- Take any column subset J, $|J| = 2^b \leq r(1 - \Omega(1))$.
- We argue that there exist $\geq 2^{r-|J|} - 1$ rows u s.t. $M_{u,v} = 1$ for all $v \in J$.

Explicit construction — cont.

Observation

Every row and column of M contain exactly $2^{r-1} - 1$ *1-entries.*

Corollary

$\mathrm{v}(M) = \frac{2^{r-1}-1}{2^r-1} = \frac{1}{2}(1 - o(1))$.

- Take any column subset J, $|J| = 2^b \leq r(1 - \Omega(1))$.
- We argue that there exist $\geq 2^{r-|J|} - 1$ rows u s.t. $M_{u,v} = 1$ for all $v \in J$.
- Indeed, requiring that $M_{u,v} = 1$ for every $v \in J$ yields a homogeneous system of $|J|$ linear equations over $GF(2)$ in r variables;
  it has $\geq 2^{r-|J|} - 1$ non-zero solutions.

Explicit construction — cont.

Observation

Every row and column of M contain exactly $2^{r-1}-1$ 1-entries.

Corollary

$\mathrm{v}(M) = \frac{2^{r-1}-1}{2^r-1} = \frac{1}{2}(1-o(1))$.

- Take any column subset J, $|J| = 2^b \leq r(1-\Omega(1))$.
- We argue that there exist $\geq 2^{r-|J|}-1$ rows u s.t. $M_{u,v}=1$ for all $v \in J$.
- Indeed, requiring that $M_{u,v}=1$ for every $v \in J$ yields a homogeneous system of $|J|$ linear equations over $GF(2)$ in r variables; it has $\geq 2^{r-|J|}-1$ non-zero solutions.
- Playing the uniform distribution on $[m]$ implies the desired $\mathrm{v}^{\mathsf{s}}(M,b) \geq \frac{2^{r-|J|}-1}{m} \geq \left(\frac{1}{2}\right)^{2^b}(1-o(1))$.

Weak leakage

Weak leakage

Theorem

For every fixed $0 < q < 1$ *and* $0 < \delta < 1$*, and for all sufficiently large* m*, there exists a game* $M \in \{0,1\}^{m^2 \times m}$ *so that:*
(1) $\mathrm{v}(M) = q + o(1)$*; and*
(2) $\mathrm{v}^w(M, b) \geq q - \delta$ *for every* $b \leq \lg\lg(m) - O_{q,\delta}(1)$.

Weak leakage

Theorem

For every fixed $0 < q < 1$ *and* $0 < \delta < 1$*, and for all sufficiently large* m*, there exists a game* $M \in \{0,1\}^{m^2 \times m}$ *so that:*
(1) $\mathrm{v}(M) = q + o(1)$*; and*
(2) $\mathrm{v}^w(M, b) \geq q - \delta$ *for every* $b \leq \lg \lg(m) - O_{q,\delta}(1)$*.*

In particular, ROW may be able to retain almost the original value of the game against any constant number of weakly leaking bits.

Weak leakage

Theorem

For every fixed $0 < q < 1$ *and* $0 < \delta < 1$, *and for all sufficiently large* m, *there exists a game* $M \in \{0,1\}^{m^2 \times m}$ *so that:*
(1) $\mathrm{v}(M) = q + o(1)$*; and*
(2) $\mathrm{v}^w(M, b) \geq q - \delta$ *for every* $b \leq \lg \lg(m) - O_{q,\delta}(1)$.

In particular, ROW may be able to retain almost the original value of the game against any constant number of weakly leaking bits.

Theorem

If $\mathrm{v}(M) = q$ *and* $b \geq \lg \lg(m) + O_q(1)$, *then* $\mathrm{v}^w(M, b) = 0$.

Weak leakage

Theorem

For every fixed $0 < q < 1$ and $0 < \delta < 1$, and for all sufficiently large m, there exists a game $M \in \{0,1\}^{m^2 \times m}$ so that:
(1) $\mathrm{v}(M) = q + o(1)$; and
(2) $\mathrm{v}^w(M, b) \geq q - \delta$ for every $b \leq \lg \lg(m) - O_{q,\delta}(1)$.

In particular, ROW may be able to retain almost the original value of the game against any constant number of weakly leaking bits.

Theorem

If $\mathrm{v}(M) = q$ and $b \geq \lg \lg(m) + O_q(1)$, then $\mathrm{v}^w(M, b) = 0$.

Hence there are instances M for which the sequence $\{\mathrm{v}^w(M, b)\}_{b=1,2,\ldots}$ also exhibits a sharp threshold:

Weak leakage

Theorem

For every fixed $0 < q < 1$ and $0 < \delta < 1$, and for all sufficiently large m, there exists a game $M \in \{0,1\}^{m^2 \times m}$ so that:
(1) $\mathrm{v}(M) = q + o(1)$; and
(2) $\mathrm{v}^w(M, b) \geq q - \delta$ for every $b \leq \lg\lg(m) - O_{q,\delta}(1)$.

In particular, ROW may be able to retain almost the original value of the game against any constant number of weakly leaking bits.

Theorem

If $\mathrm{v}(M) = q$ and $b \geq \lg\lg(m) + O_q(1)$, then $\mathrm{v}^w(M, b) = 0$.

Hence there are instances M for which the sequence $\{\mathrm{v}^w(M, b)\}_{b=1,2,\ldots}$ also exhibits a sharp threshold:
it stays close to $\mathrm{v}(M)$ as long as $b \leq \lg\lg(m) - O(1)$;
it drops to 0 once $b \geq \lg\lg(m) + O(1)$.

Computational complexity

Computational complexity

Theorem

Given a game $M \in \{0,1\}^{m \times n}$ *and some* $b \geq 0$, *both* $\mathrm{v}^s(M,b)$ *and* $\mathrm{v}^w(M,b)$ *are NP-hard to approximate to within any factor.*

Computational complexity

Theorem

Given a game $M \in \{0,1\}^{m \times n}$ and some $b \geq 0$, both $\mathrm{v}^s(M,b)$ and $\mathrm{v}^w(M,b)$ are NP-hard to approximate to within any factor.

Reducing set cover to the problem of deciding whether the (strong or weak) value is strictly positive.

Computational complexity

Theorem

Given a game $M \in \{0,1\}^{m \times n}$ and some $b \geq 0$, both $\mathrm{v}^s(M,b)$ and $\mathrm{v}^w(M,b)$ are NP-hard to approximate to within any factor.

Reducing set cover to the problem of deciding whether the (strong or weak) value is strictly positive.

When b is fixed, computing $\mathrm{v}^s(M,b)$ becomes tractable:

Theorem

Given a game $M \in \{0,1\}^{m \times n}$, the optimal mixed strategy p_b^* can be efficiently computed.

conclusions

Polynomial algorithm for constant b

Polynomial algorithm for constant b

Would like to solve the LP

$$\text{maximize } v \text{ s.t.}$$

$$\sum_{i \in [m]} p_i \cdot M_{i,g(f(i))} \geq v \quad \forall f : [m] \to \{0,1\}^b, \forall g : \{0,1\}^b \to [n]$$

$$\sum_{i \in [m]} p_i = 1$$

$$p_i \geq 0 \quad \forall i \in [m] \ .$$

Polynomial algorithm for constant b

Would like to solve the LP

$$\text{maximize } v \text{ s.t.}$$

$$\sum_{i \in [m]} p_i \cdot M_{i,g(f(i))} \geq v \quad \forall f : [m] \to \{0,1\}^b, \forall g : \{0,1\}^b \to [n]$$

$$\sum_{i \in [m]} p_i = 1$$

$$p_i \geq 0 \quad \forall i \in [m] \ .$$

However, there are 2^{bm} different functions f — exponentially many constraints.

Polynomial algorithm for constant b

Would like to solve the LP

$$\text{maximize } v \text{ s.t.}$$
$$\sum_{i \in [m]} p_i \cdot M_{i,g(f(i))} \geq v \quad \forall f : [m] \to \{0,1\}^b, \forall g : \{0,1\}^b \to [n]$$
$$\sum_{i \in [m]} p_i = 1$$
$$p_i \geq 0 \quad \forall i \in [m] \ .$$

However, there are 2^{bm} different functions f — exponentially many constraints.

The composition $g \circ f$ is a mapping $h : [m] \to [n]$ with $|\mathrm{image}(h)| \leq 2^b$.

Polynomial algorithm for constant b

Would like to solve the LP

$$\begin{aligned}
&\text{maximize } v \text{ s.t.} \\
&\sum_{i\in[m]} p_i \cdot M_{i,g(f(i))} \geq v \quad \forall f : [m] \rightarrow \{0,1\}^b, \forall g : \{0,1\}^b \rightarrow [n] \\
&\sum_{i\in[m]} p_i = 1 \\
&p_i \geq 0 \quad \forall i \in [m] \; .
\end{aligned}$$

However, there are 2^{bm} different functions f — exponentially many constraints.

The composition $g \circ f$ is a mapping $h : [m] \rightarrow [n]$ with $|\text{image}(h)| \leq 2^b$.

Fixing some $J \subseteq [n]$, $|J| \leq 2^b$, it is easy to compute the mapping h_J that is worst for ROW out of all mappings h with $\text{image}(h) = J$:

Polynomial algorithm for constant b

Would like to solve the LP

$$\begin{aligned}
&\text{maximize } v \text{ s.t.} \\
&\sum_{i \in [m]} p_i \cdot M_{i,g(f(i))} \geq v \quad \forall f : [m] \rightarrow \{0,1\}^b, \forall g : \{0,1\}^b \rightarrow [n] \\
&\sum_{i \in [m]} p_i = 1 \\
&p_i \geq 0 \quad \forall i \in [m] \, .
\end{aligned}$$

However, there are 2^{bm} different functions f — exponentially many constraints.

The composition $g \circ f$ is a mapping $h : [m] \rightarrow [n]$ with $|\mathrm{image}(h)| \leq 2^b$.

Fixing some $J \subseteq [n]$, $|J| \leq 2^b$, it is easy to compute the mapping h_J that is worst for ROW out of all mappings h with $\mathrm{image}(h) = J$:
h_J simply maps each row $i \in [m]$ to the column $j \in J$ that minimizes $M_{i,j}$.

Polynomial algorithm for constant b — cont.

Sufficient to solve the LP

$$\text{maximize } v \text{ s.t.}$$

$$\sum_{j \in J} \sum_{i : h_J(i) = j} p_i \cdot M_{i,j} \geq v \quad \forall J \subseteq [n], |J| \leq 2^b$$

$$\sum_{i \in [m]} p_i = 1$$

$$p_i \geq 0 \quad \forall i \in [m] \ .$$

Size = polynomial when b is fixed.

Conclusions

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.
- In reality, complete privacy is often impractical.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.
- In reality, complete privacy is often impractical.
- This leads to the study of adversarial leakage of information in games.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.
- In reality, complete privacy is often impractical.
- This leads to the study of adversarial leakage of information in games.
- We cover the basic model of uni-directional leakage in two-player zero-sum binary games.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.
- In reality, complete privacy is often impractical.
- This leads to the study of adversarial leakage of information in games.
- We cover the basic model of uni-directional leakage in two-player zero-sum binary games.
- The investigation of more complicated models deserves further study: leakage in both directions, arbitrary games.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.
- In reality, complete privacy is often impractical.
- This leads to the study of adversarial leakage of information in games.
- We cover the basic model of uni-directional leakage in two-player zero-sum binary games.
- The investigation of more complicated models deserves further study: leakage in both directions, arbitrary games.

Conclusions

- The validity of von Neumann's theorem for two-player zero-sum games requires mixed strategies.
- The randomization phase must be private.
- In reality, complete privacy is often impractical.
- This leads to the study of adversarial leakage of information in games.
- We cover the basic model of uni-directional leakage in two-player zero-sum binary games.
- The investigation of more complicated models deserves further study: leakage in both directions, arbitrary games.

謝謝您