Sensitivity of voting coin tossing protocols, Nov 1

Lecturer: Elchanan Mossel

Scribe: Radu Mihaescu

Slides partially stolen from

Ryan O'Donnell

Tossing coins from cosmic source

	x	01010001011011011111	(n bits)
			first bit
Alice	y^1	01010001011011011111	0
Bob	y^2	01010001011011011111	0
Cindy	y^3	01010001011011011111	0
∘ ∘ ∘		∘ ∘ ∘	
Kate	y^k	01010001011011011111	0

0

Broadcast with ε errors

	x	01010001011011011111	(n bits)
			first bit
Alice	y^1	01011000011011011111	0
Bob	y^2	01010001011110011011	0
Cindy	y^3	11010001011010011111	1
∘ ∘ ∘		∘ ∘ ∘	
Kate	y^k	01010011011001010111	0

Broadcast with ε errors

	x	01010001011011011111	(n bits)
			majority
Alice	y^1	01011000011011011111	1
Bob	y^2	01010001011110011011	1
Cindy	y^3	11010001011010011111	1
∘∘∘		∘ ∘ ∘	
Kate	y^k	01010011011001010111	1

1

The parameters

- n bit uniform random "source" string x
- k parties who cannot communicate, but wish to agree on a uniformly random bit
- ε each party gets an independently corrupted version y^i, each bit flipped independently with probability ε
- f (or $f_1 \ldots f_k$): balanced "protocol" functions

Our goal

For each n, k, ε,

find the best protocol function f (or functions $f_1 \ldots f_k$) which maximize the probability that all parties agree on the same bit.

Our goal

For each n, k, ε,

find the best protocol function f (or functions $f_1 \ldots f_k$) which maximize the probability that all parties agree on the same bit.

Coins and voting schemes

- For $k=2$ we want to maximize $P[f_1(y^1) = f_2(y^2)]$, where y_1 and y_2 are related by applying ε noise twice.
- Optimal protocol: $f_1 = f_2 =$ dictatorship.
- Same is true for k=3 (M-O'Donnell).

Proof that optimality is achieved at $f_1=f_2=x_1$

- We want to maximize $E[f_1 T_\eta f_2]$ for $\eta=1-2\varepsilon$. But

$$f_i = \sum_{|S|\neq 0} \hat{f}_i(S) u_S$$

$$E[f_1 T_\eta f_2] = \sum_{|S|\neq 0} \hat{f}_1(S)\hat{f}_2(S)\eta^{|S|}$$

- By Cauchy-Schwartz

$$E[f_1 T_\eta f_2] \leq \sqrt{\sum_{|S|\neq 0} \hat{f}_1^{\,2}(S)\eta^{|S|}}\sqrt{\sum_{|S|\neq 0} \hat{f}_2^{\,2}(S)\eta^{|S|}} \leq \eta \| f_1 \|_2 \| f_2 \|_2 = \eta$$

- Equality is trivially achieved for $f_1=f_2=x_1$

Proof that optimality is achieved for $f_1=f_2=f_3=x_1$

- For 3 functions, disagreement means that two agree and the third disagrees. Therefore:

$$P[f1=f2=f3]=1-\tfrac{1}{2}\left(P[f_1(y^1)\neq f_2(y^2)]+P[f_1(y^1)\neq f_3(y^3)]+P[f_3(y^3)\neq f_2(y^2)]\right)=$$
$$=1-\tfrac{1}{2}(3-P[f_1(y^1)=f_2(y^2)]-P[f_1(y^1)=f_3(y^3)]-P[f_3(y^3)=f_2(y^2)])$$

- Now each term in the sum above can be maximized independently.

Notation

We write:

$S(f_1, \ldots, f_k; \varepsilon) \quad = \quad \Pr[f_1(y^1) = \cdots = f_k(y^k)]$,

$S_k(f; \varepsilon)$ in the case $f = f_1 = \cdots = f_k$.

Further motivation

- Noise in "Ever-lasting security" crypto protocols (Ding and Rabin).
- Variant of a decoding problem.
- Study of noise sensitivity: $|T_\varepsilon(f)|_{\underline{k}}^k$ where T_ε is the Bonami-Beckner operator.

protocols

- Recall that we want the parties' bits, when agreed upon, to be uniformly random.
- To get this, we restricted to balanced functions.
- However this is neither necessary nor sufficient!
- In particular, for $n = 5$ and $k = 3$, there is a balanced function f such that, if all players use f, they are more likely to agree on 1 than on 0!.
- To get agreed-upon bits to be uniform, it suffices for functions be *antisymmetric*:
- Thm[M-O'Donnell]: In optimal $f_1 = \ldots = f_k = f$ and f is monotone (Pf uses convexity and symmetrization).
- We are thus in the same setting as in the voting case.

Proof of M-O'Donnell Theorem

- **Claim 1:** in optimal protocol, $f_1=f_2=\ldots=f_k=f$.
- Proof: Let $f_1, f_2 \ldots f_M$ be all the possible functions, where $M=2^{2^n}$. Let $t_1, t_2 \ldots t_M$ be the numbers of players using each function. Then

$$P_{agree}(t_1, t_2, \ldots t_M) = E[(T_\eta f_1)^{t_1} (T_\eta f_2)^{t_2} \ldots (T_\eta f_M)^{t_M}] +$$
$$+ E[(1-T_\eta f_1)^{t_1} (1-T_\eta f_2)^{t_2} \ldots (1-T_\eta f_M)^{t_M}]$$

- But for each value of x, $0<Tf_i(x)<1$, and therefore for each value of x, the both terms above are convex. Therefore the expectation of the sum is also convex in $(t_1, \ldots t_M)$. Which implies that the optimum is achieved at (k,0,0,…0).

Proof of M-O'Donnell Theorem (continued)

- **Claim 2:** Optimum is achieved when f is monotone.
- Proof: We will use the technique of shifting (as in the proof of the isoperimetric inequality).
- If $f(0,x_2,\ldots x_n)= f(1,x_2,\ldots x_n)$, then set $g(0,x_2,\ldots x_n)= g(1,x_2,\ldots x_n)= f(0,x_2,\ldots x_n)= f(1,x_2,\ldots x_n)$. If $f(0,x_2,\ldots x_n)= f(1,x_2,\ldots x_n)$, then set $g(0,x_2,\ldots x_n)= 0$ and $g(1,x_2,\ldots x_n)= 1$.
- **Subclaim:** g is "better" than f, even if conditioned on the values of (y_j^i) for $j\geq 2$ and $1\leq i\leq k$.
- Proof of subclaim: Suppose a functions are identically 0, b are identically 1 and c are non-trivial (having fixed the (y_j^i)'s). If both $a,b>0$, agreement is with probability 0.

Proof of M-O'Donnell Theorem (continued)

- Suppose a=b=0. Let $c=c_{up}+c_{down}$, where c_{up} is the number of increasing functions and c_{down} is the number of decreasing functions. Then the probability of agreement for f is

$$P^f_{agree} = (1-\varepsilon)^{c_{up}}\,\varepsilon^{c_{down}} + \varepsilon^{c_{up}}(1-\varepsilon)^{c_{down}}$$

- On the other hand, the probability of agreement for g is

$$P^g_{agree} = (1-\varepsilon)^c + \varepsilon^c$$

and $P_{agree}{}^g > P_{agree}{}^f$ by convexity.

- For a>0 and b=0 or vice-versa the analysis is identical save for a factor of ½.■

■ Thm.

More results [M-O'Donnell]

- When $k = 2$ or 3, the first-bit function is best.
- For fixed n, when $k \to \infty$ majority is best.
- For fixed n and k when $\varepsilon \to 0$ and $\varepsilon \to \frac{1}{2}$, the first-bit is best.
  - Proof for $\varepsilon \to 0$ uses isoperimetric inq for edge boundary.
  - Proof for $\varepsilon \to \frac{1}{2}$ uses Fourier.
- For unbounded n, things get harder… in general we don't know the best function, but we can give bounds for $S_k(f; \varepsilon)$.
- Main open problem for finite n (odd): Is optimal protocol always a majority of a subset?
- Conjecture M: No
- Conjecture O: Yes.

For fixed n and ε, when k→∞ majority is best

- **Proof:** We have seen that in the optimal case all the f's are equal and monotone. Then

$$P[f_1 = ... = f_k] = 2^{-n}\left(\sum_{x\in\{0,1\}^n}(Tf(x))^k + \sum_{x\in\{0,1\}^n}(1-Tf(x))^k\right).$$

- But when $k\to\infty$, we only care about the dominant term, i.e. $(Tf(1))^k+(1-Tf(0))^k$. (Tf is monotone when f is monotone.)

- We are therefore trying to maximize the following quantity over f

$$Tf(1) = \sum_y (1-\varepsilon)^{\#_1(y)}\varepsilon^{\#_0(y)} f(y).$$

- But $\varepsilon \leq 1/2$, therefore maximization is achieved when one picks the top half of the distribution, i.e. majority. ■

Unbounded n

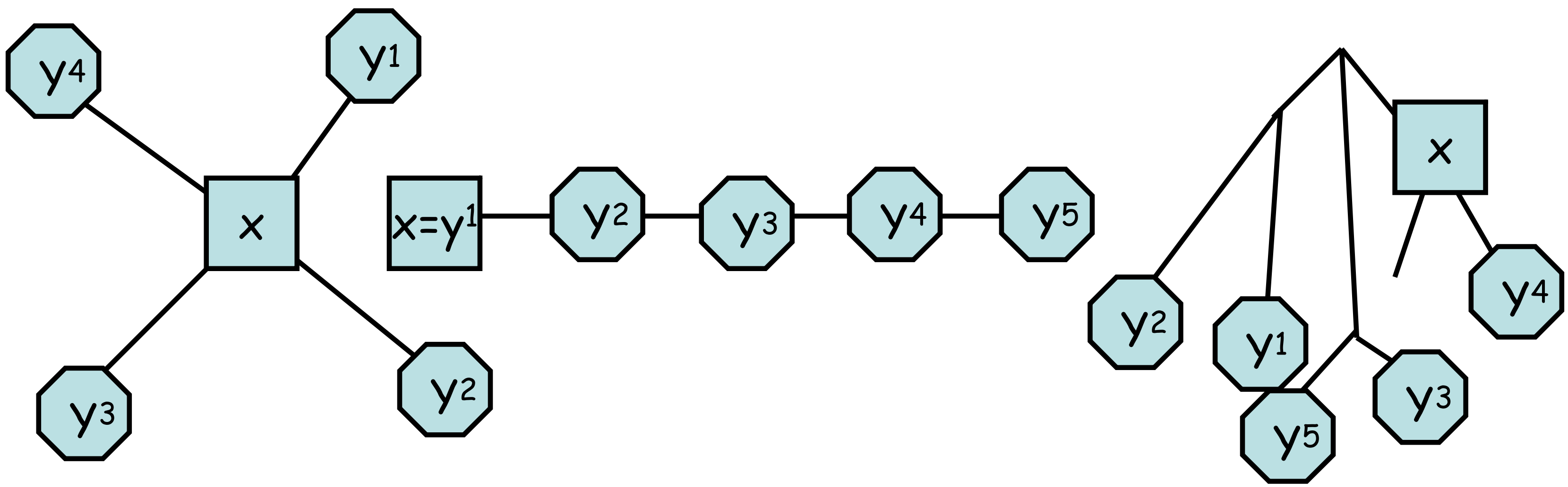
- Fixing ε and $n = \infty$, how does $h(k,\varepsilon) := P[f_1 = \ldots = f_k]$ decay as a function of k?
- First guess: $h(k,\varepsilon)$ decays exponentially with k.
- But!
- Prop[M-O'Donnell]: $h(k,\varepsilon) \geq k^{-c(\varepsilon)}$ where $c(\varepsilon) > 0$.
- Conj[M-O'Donnell]: $h(k,\varepsilon) \to 0$ as $k \to \infty$.
- Thm[M-O'Donnell-Regev-Steif-Sudakov]: $h(k,\varepsilon) \cdot k^{-c'(\varepsilon)}$

Harmonic analysis of Boolean functions

- To prove "hard" results need to do harmonic analysis of Boolean functions.
- Consists of many combinatorial and probabilistic tricks + "Hyper-contractivity".
- If $p-1=\eta^2(q-1)$ then
- $|T_\eta f|_q \cdot |f|_p$ if $p > 1$ (Bonami-Beckner)
- $|T_\eta f|_q \geq |f|_p$ if $p < 1$ and $f > 0$ (Borell).
- Our application uses 2nd – in particular implies that for all A and B: $P[x \in A, N_\varepsilon(x) \in B] \geq P(A)^{1/p} P(B)^{q}$.
- Similar inequalities hold for Ornstein-Uhlenbeck processes and "whenever" there is a log-sob inequality.

Coins on other trees

- We can define the coin problem on trees.
- So far we have only discusses the star.



- Some highlights from MORSS:
- On line dictator is always optimal (new result in MCs).
- For some trees, different f_i's needed.

Wrap-up

- We have seen a variety of "stability" problems for voting and coins tossing.
- Sometimes it is "easy" to show that dictator is optimal.
- Sometimes majority is (almost) optimal, but typically hard to prove (why?).
- Recursive majority is really (the most) unstable.

Open problems

1. Does f monotone anti-symmetric, μ FKG and $\mu[X_i] = p > \frac{1}{2}$, $e_i < \delta \quad \Rightarrow \mu[f] \geq 1 - \varepsilon$?
2. For μ the i.i.d. measure the (almost) most stable f with $e_i = o(1)$ is maj (for $k=2$? All k?).
3. The most stable f for Gaussian coin problem is $f(x) = \mathrm{sign}(x)$ and result is robust.
4. For the coin problem, the optimal f is always a majority of a subset.