QUANTUM SAMPLING, SZK & MARKOV CHAINS:

A DIFFERENT LOOK AT QUANTUM ALGORITHMIC PROBLEMS

DORIT AHARONOV, HUJI
& AMNON TA-SHMA, TAU

QUANTUM ALGORITHMS

KNOWN:

FACTORING $N = pq \rightarrow (p, q)$

DISCRETE LOG $y, p, g \rightarrow x \mid g^x \underset{p}{\equiv} y$

HIDDEN SUBGROUP PROBLEM $f(H) = \text{CONST} \rightarrow H$

QUADRATIC RESIDUOSITY $x \overset{?}{=} y^2 \bmod N$

SHIFTED MULTIPLICATIVE CHARACTER $f = \left(\frac{x+s}{p}\right)$

PELL'S EQUATION $x^2 + dy^2 = 1,\ x, y = ?$

OPEN:

GRAPH ISOMORPHISM $G_0 \overset{?}{=} G(G_1)$

CLOSEST VECTOR IN A LATTICE

$v, b_1 \cdots b_n, d$

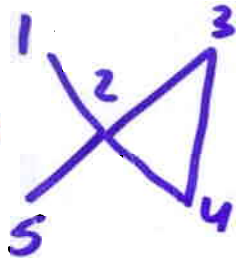
$|v - \sum(b_i)| \lessgtr d$?

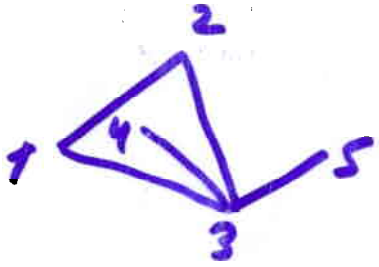
$> \sqrt{n}\, d$

SHORTEST VECTOR IN A LATTICE

⋮

GRAPH ISOMORPHISM

G_0 = 

G_1 = 

$$A_{G_0} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} \qquad A_{G_1} = \begin{pmatrix} 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

INPUT: G_0, G_1 on n NODES

OUTPUT: IS THERE $\sigma \in S_n$ S.t $\sigma(G_0) = G_1$?

REDUCIBLE TO:

INPUT: $|G\rangle$

OUTPUT $|G\rangle|\alpha_G\rangle$

$$|\alpha_G\rangle = \frac{1}{\sqrt{n!}} \sum_{\sigma \in S_n} |\sigma(G)\rangle$$

SIMPLE ALGORITHM:

$A_0 \longrightarrow |\alpha_0\rangle$

$A_1 \longrightarrow |\alpha_1\rangle$

$\langle\alpha_0|\alpha_1\rangle = ?$

$$\frac{(|0\rangle + |1\rangle)}{\sqrt{2}} \xrightarrow{A} \frac{|0\rangle|\alpha_0\rangle + |1\rangle|\alpha_1\rangle}{\sqrt{2}}$$

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad |0\rangle \longrightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$|1\rangle \longrightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\longrightarrow \frac{(|0\rangle + |1\rangle)|\alpha_0\rangle + (|0\rangle - |1\rangle)|\alpha_1\rangle}{2}$$

$$= |0\rangle\left(\frac{|\alpha_0\rangle + |\alpha_1\rangle}{2}\right) + |1\rangle\left(\frac{|\alpha_0\rangle - |\alpha_1\rangle}{2}\right)$$

$$Pr(0) = \left|\frac{|\alpha_0\rangle + |\alpha_1\rangle}{2}\right|^2 = \frac{1 + \langle\alpha_0|\alpha_1\rangle}{2}$$

HOW TO GENERATE $|K_G\rangle$?

$$\pi(G') = \begin{cases} \frac{1}{n!} & \text{IF} \quad G' \sim G \\ 0 & \text{OW} \end{cases}$$

$$|\alpha_G\rangle = \sum_{G'} \sqrt{\pi(G')} \; |G'\rangle$$

Q:

EASY TO SAMPLE FROM π

$\Downarrow$?

EASY TO GENERATE SUPERPOSITION OVER π ?

NOT TRIVIAL.

EASY TO GENERATE

$$\sum |G\rangle|G(G)\rangle \quad (\neq |K_G\rangle)$$

BUT NOT TO FORGET G !!!)

QUANTUM SAMPLING

INPUT: C (A CIRCUIT)

ON UNIFORMLY DISTRIBUTED

x'

$C(x') = x \sim \pi(x)$.

WANTED: $\sum \sqrt{\pi(x)}\,|x\rangle$

↑

THE QUANTUM SAMPLING OF THE DISTRIBUTION π.

IMPORTANCE OF QSAMPLING

FACT

$\exists A, \quad \forall L \in SZK, \quad A(x) = C_0, C_1$

S.T QSAMPLING FROM $\pi(C_0), \pi(C_1)$

$\Downarrow$

$L \in BQP$

NEW PARADIGM

CAST PROBLEMS IN THE FORM OF QSAMPLING.

$L \in SZK \rightarrow L \leq QSAMPLING$

WHAT STATES CAN WE GENERATE,
" DISTRIBUTIONS CAN WE QSAMPLE ?

TOOLS : QSAMPLING A WIDE CLASS OF STATES USING

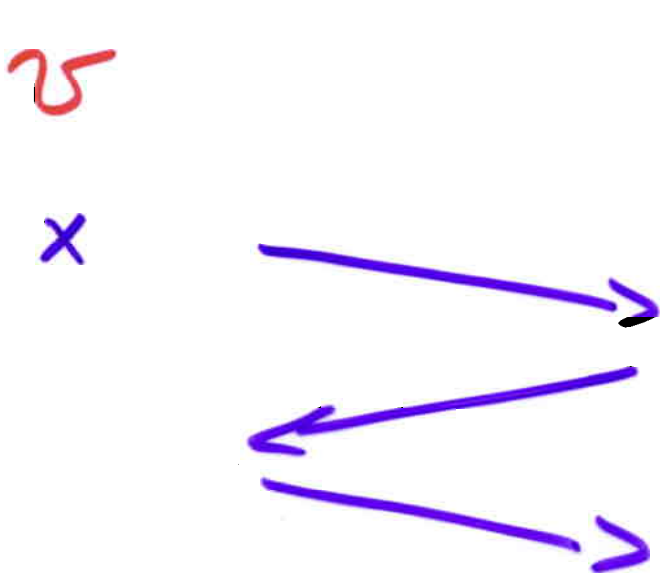
MARKOV CHAINS
ADIABATIC COMPUTATION

HOPE : - UNDERSTAND KNOWN ALGORITHMS IN TERMS OF QSAMPLING.

- ZK PROOFS MIGHT HELP.

- PERHAPS EXTEND TO NEW ALGS.

STATISTICAL ZERO KNOWLEDGE



$x \in L$?

$x \in L \longrightarrow$ V ACCEPTS $P(x)$

$x \notin L \longrightarrow$ V DOES NOT ACCEPT $P^*(x)$

ZK:

V CAN SIMULATE WHAT HE WOULD HAVE SEEN WITHOUT P, $\forall x \in L$.

PERFECT, STATISTICAL, COMPUTATIONAL

COMPLETE PROBLEM: STATISTICAL DIFFERENCE

(VADHAN, SAHAI 2000]

C_0, C_1 $\quad \| \pi(C_0) - \pi(C_1) \| > a$

OR

$\| \pi(C_0) - \pi(C_1) \| < b$

QUANTUMLY:

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \longrightarrow \frac{|0\rangle|\pi_0\rangle + |1\rangle|\pi_1\rangle}{\sqrt{2}}$$

$$\langle \pi_0 | \pi_1 \rangle = \sum_x \sqrt{\pi_0(x)}\sqrt{\pi_1(x)}$$

$$\sim \sum_x |\pi_0(x) - \pi_1(x)|$$

IF WE COULD QSAMPLE FROM π_0, π_1

QUADATIC RESIDUOCITY

$X \equiv y^2$ IN A RING

$\not\equiv y^2$

$$|\alpha_0\rangle = \sum_{x \in R} |x^2\rangle$$

$$|\alpha_1\rangle = \sum |y \cdot x^2\rangle$$

DISCRETE LOG

y, g, P

$g^x = y \bmod p$

[BM 84]

SUFFICE TO KNOW

$x \in [1, \frac{p-1}{2}]$

OR

$x \in [\frac{p-1}{2}, p]$

$x \in [1, \frac{1}{6}\frac{p-1}{2}]$ OR $[\frac{p-1}{2}, \frac{p-1}{2} + \frac{1}{6}\frac{p-1}{2}]$

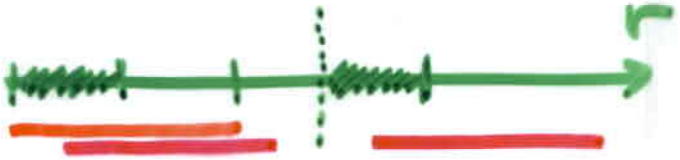
SZKP: $\mathcal{P}$: $b \in \{0,1\}$, $r \in [1, 2\varepsilon(p-1)]$

[GK 91]

$y^b \cdot g^r \longrightarrow$

$\longleftarrow b$

P



QUANTUM

$|b=0\rangle \cdot \Sigma |g^r\rangle$

$+ |b=1\rangle \cdot \Sigma |g^r \cdot y\rangle$

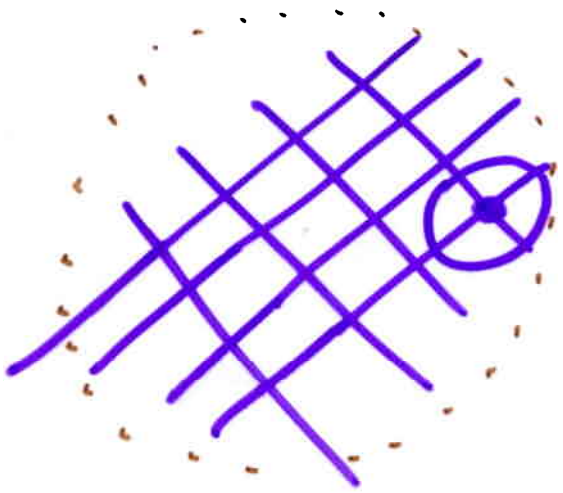
CLOSEST VECTOR IN A LATTICE

$c, b_1 \dots b_n, d,$

[GOLDREICH, GOLDWASSER 98]

SZK:

$\mathcal{V}$:

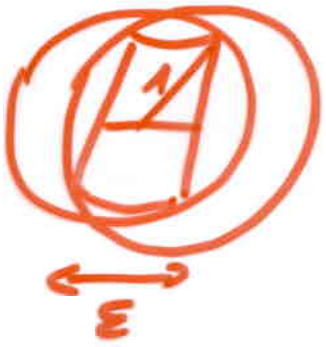


l, r, b

$l + r + c^b$

b

$: P$



$(1-\varepsilon^2)^n$

QUANTUM:

$$|b=0\rangle \sum |l+r\rangle$$

$$+|b=1\rangle \sum |l+r+c\rangle$$

PROBLEM

WHAT DISTRIBUTIONS CAN BE QSAMPLED FROM EFFICIENTLY ?

(WHAT STATES CAN BE GENERATED EFFICIENTLY?)

TRIVIAL OBSERVATION :

AN OVERWHELMING PORTION OF THE DISTRIBUTIONS (STATES) CANNOT BE APPROXIMATED SUBEXPONENTIALY.

(COUNTING ARGUMENTS)

POSSIBLY :

C A SHORT CIRCUIT $\Rightarrow$ QSAMPLE $\pi(C)$.

NOTE : THIS WOULD IMPLY $SZK \subseteq BQP$

AARONSON'S COLLISION LOWER BOUND

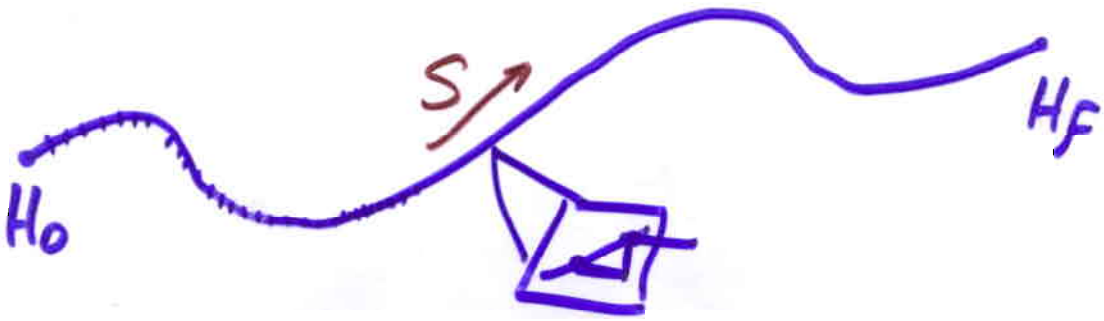
$\hookrightarrow \exists A, SZK^A \not\subseteq BQP^A$

SO SUCH A PROOF WOULD NEED TO BE NON-RELATIVABLE.

ADIABATIC COMPUTATION

['99, FARHI & GUTTMAN]

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H(t)\,|\psi(t)\rangle$$



ADIABATIC THEOREM:

$$|\psi_0\rangle = |GS(0)\rangle \longrightarrow |\psi_f\rangle = |GS(f)\rangle$$

ADDING A DELAY SCHEDULE:

$$i\hbar \frac{d}{ds}|\psi(s)\rangle = \tau(s)\,H(s)\,|\psi(s)\rangle$$

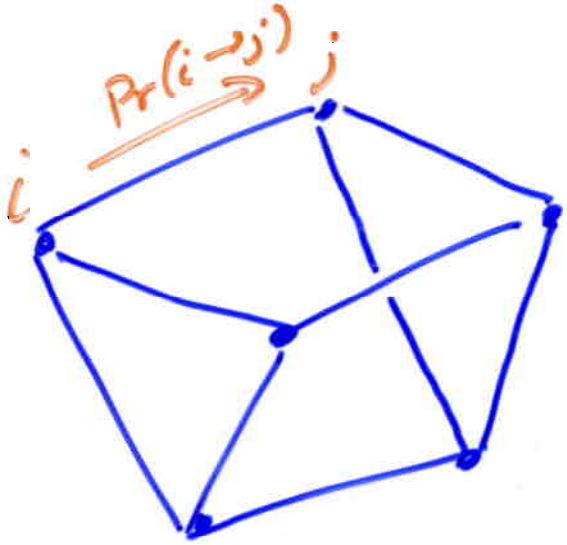
$$s \in [0,1]$$

$$\tau(s) \gg \left|\frac{d}{ds}H(s)\right| / \Delta^2(s)$$

★ VAN DAM, MOSCA, VAZIRANI '01 : CAN SIMULATE ON A QC

★ ANY STATE THAT CAN BE GENERATED CAN BE GENERATED ADIABATICALLY (AND VV)

MARKOV CHAINS



STATE SPACE = Ω

$|\Omega| = EXP(n)$

M_{ij} = TRANSITION MATRIX

$$P_t = M P_{t-1}$$

π = LIMITING DISTRIBUTION

$$\pi = \lim_{t \to \infty} M^t P_0 \qquad \forall P_0$$

RAPID MIXING IF $\lambda_2 < 1 - \frac{1}{n^c}$

(LARGE SPETRAL GAP)

HAMILTONIANS FROM MC's

HAMILTONIAN : HERMITIAN MATRIX

$$H \longleftrightarrow M$$

$$\pi(i) M_{ij} = \pi(j) M_{ji} \qquad \text{REVERSIBLE}$$

$$\begin{pmatrix} \frac{1}{\sqrt{\pi_1}} & & 0 \\ & \ddots & \\ 0 & & \frac{1}{\sqrt{\pi_N}} \end{pmatrix} M \begin{pmatrix} \sqrt{\pi_1} & & 0 \\ & \ddots & \\ 0 & & \sqrt{\pi_N} \end{pmatrix}$$

$$H = I - \frac{1}{\sqrt{\pi}} M \sqrt{\pi}$$

$$\lambda \longleftrightarrow 1-\lambda$$

$$\sum \sqrt{\pi(x)}\,|x\rangle \longleftrightarrow \pi \qquad \text{LIMITING DIST}$$

GROUND STATE

THM

$M_1, \dots M_T$ "NICE" MC's, RAPID MIXING (Δ)

$|\pi_t - \pi_{t+1}| < \frac{\Delta}{10}$

Q SAMPLING π_1 $\Longrightarrow$ Q SAMPLING π_T

[NICE MC's : POLY MANY NEIGHBORS
EASY TO CALCULATE $M_{ij} \neq 0$
★ EASY TO CALCULATE $f \sim \pi$]

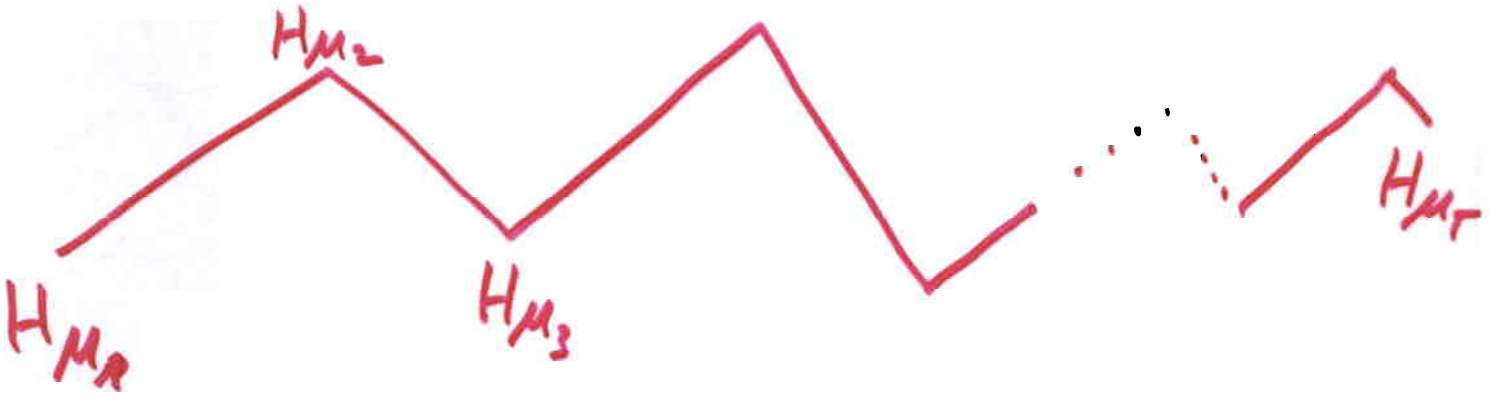
RESULTS

CAN EFFICIENTLY APPROXIMATE

- ALL PERFECT MATCHINGS IN A BIPARTITE GRAPH G
- $\sum \sqrt{\pi(a)}\,|a\rangle$ IF $\pi(a)$ IS LOG CONCAVE AND EASY TO COMPUTE
- ALL GRID POINTS INSIDE A CONVEX BODY IN HIGH DIM
- ALL EXTENTIONS OF A GIVEN PARTIAL ORDER
- SUPER POSITION OVER THE GIBBS DISTRIBUTION FOR VARIOUS STAT. MECH MODELS (POTTS, ISING, ETC ..)

⋮

PROOF OF THEOREM:



WALK ADIABATICALLY ON THE BROKEN LINE CONNECTING THE H_{M_t} IN HAMILTONIAN SPACE

IF 1) Δ_{min} poly big

2) $\frac{dH}{ds}$ poly big

&

3) CAN APPLY $e^{iH(s)\Delta t}$ BY A QC

1) **CLAIM:**

H, H' ARE SUCH THAT $|\alpha\rangle, |\alpha'\rangle$ SATISFY $|\langle\alpha'|\alpha^{\perp}\rangle| < \frac{\Delta}{10}$.

Δ = min spectral gap of H, H'

$$\Longrightarrow \quad \Delta(\eta H + (1-\eta)H') > \frac{\Delta}{2} \quad \forall \eta \in [0,1].$$

PROOF:

- OBSERVE THAT TRUE IF $|\alpha\rangle = |\alpha'\rangle$.
- " " " IF $|H' - H| < \frac{\Delta}{10}$
- PERTURB H' TO GET $H' + E$, $|E| < \frac{\Delta}{10}$ AND $H' + E$ HAVE $|\alpha\rangle$ AS G.S.

LEMMA

H IS SPARSE, $\forall i \; H_{ij} \neq 0$ CAN BE COMPUTED EFFICIENTLY

e^{iHat} CAN BE APPROXIMATED TO WITHIN POLY ACCURACY EFFICIENTLY.

(IMPLICATIONS TO QWALKS ETC.)

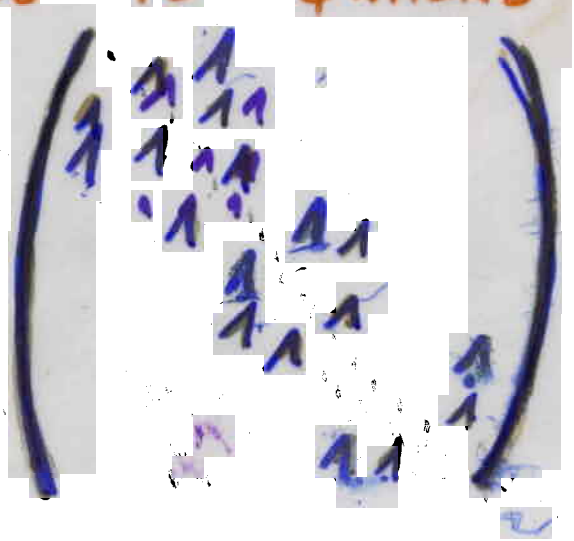
LEMMA

H IS SPARSE, $\forall i\ H_{ij} \neq 0$ CAN BE COMPUTED EFFICIENTLY

⇓

e^{iHat} CAN BE APPROXIMATED TO WITHIN POLY ACCURACY EFFICIENTLY.

(IMPLICATIONS TO QWALKS ETC.)

H= 

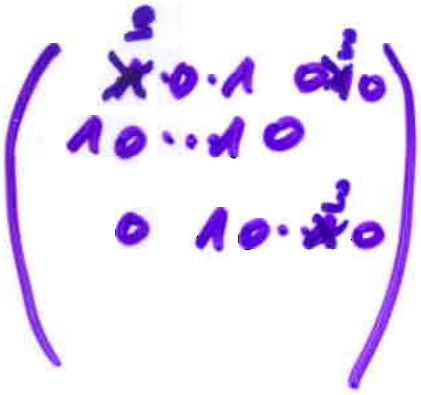
PROOF (OF APPLYING A SPARSE H)

1. WRITE $H = \sum_{b=1}^{poly} H_b$.

TROTTER:

$$e^{iH\Delta t} = e^{i\sum_{b=1}^{poly} H_b \Delta t} \approx \left[\prod_{b=1}^{poly} e^{i\frac{H_b \Delta t}{r}}\right]^r$$

DECOMPOSING H



$deg = d \rightarrow K = d^5$. (# H_b)

$$H = \sum_{b=1}^{K} H_b$$

EACH ELEMENE H_{ij} PICKS $b \in [1, d^5]$ RANDOMLY, WHERE IT WILL APPEAR.

BRANCHING PROCESSES → w.h.p ALL BLOCKS ARE SMALL.

FOR ALL H_b, $b \in [1, d^5]$

PROBLEM : TO DO IN PARALLEL, CAN'T AFFORD THAT EACH ELEMENT PICKS RANDOMLY!

SOLUTION : HASH FUNCTIONS (K-WISE INDEPENDANT)

QALGORITHMS ⟷ QSAMPLING

SZK

ADIABATIC COMPUTATION & MCS

LESS STRUTURED DOMAIN

OPEN

- REDERIVE KNOWN Q ALGORITHMS (BQP ⟷ SZK)

- TOOLS FOR ADIABATIC COMPUTATION (CONDUCTANCE, MULTICOMMODITY FLOWS ETC)