Approximating CVP is NP-hard (referuje Marek Krčál) Dinur, Kindler, Raz, Safra

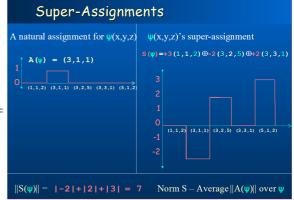
$L(v_1,\ldots,v_n)$	lattice: $\{\sum_i a_i v_i \mid a_i \in \mathbf{Z}\}$, where v_1, \ldots, v_n
,	independent in \mathbf{Z}^k
$\overline{ ext{CVP}}$	IN: $(v_1, \dots v_n), y \in \mathbf{R}^k$
	OUT: $v \in L(v_1, \ldots, v_n)$
	GOAL: minimize $ l-y _1$
SVP	IN: $(v_1, \ldots v_n)$
	OUT: $0 \neq v \in L(v_1, \ldots, v_n)$
	GOAL: minimize $ l _1$
tests	$\Psi = (\psi_1 \dots, \psi_n)$
variables	$\mathcal{V} = (x_1, \dots, x_m)$
lists of satisfying	$\mathcal{R}_{\psi_1}, \dots, \mathcal{R}_{\psi_n}, ext{ where } \mathcal{R}_{\psi_i} \subseteq \mathbf{F}^{\mathcal{V}_{\psi_i}} ext{ where } \mathcal{V}_{\psi_i}$
assignments	is set of variables of ψ_i and F a field.
super assign-	function $S: \psi \mapsto S(\psi) \in \mathbf{Z}^{\mathcal{R}_{\psi}}$ for each $\psi \in \Psi$
ment S	$S(\psi) = (S(\psi)[r_1], \dots, S(\psi)[r_k])$ where $\mathcal{R}_{\psi} = (S(\psi)[r_k])$
	$\{r_1,\ldots,r_k\}$
projection	$\forall a \in \mathbf{F} \text{ set } S(\psi) _x[a] := \sum_{r,r _x=a} S(\psi)[r] \text{ where } x$
$S(\psi) _x$	variable of ψ
S consistent	$\forall \psi, \phi \in \Psi, x \in \mathcal{V} \text{ holds } S(\psi) _x = S(\phi) _x$
S natural	$S(\psi) = (0, \dots, 0, 1, 0, \dots, 0)$ for each ψ
S non-trivial	$S(\psi) \neq (0, \dots, 0)$ for each ψ
norm $ S $	$ S := (1/ \Psi) \sum_i S(\psi_i) _1$
$g extbf{-}\mathbf{SSAT}$	$ extbf{IN}: (\Psi, \mathcal{V}, \mathcal{R}_{\psi_1}, \dots, \mathcal{R}_{\psi_n})$
	OUT:distinguish
	YES: \exists consistent natural S
	NO: \forall consistent non-trivial S holds $ S > g$.
g-CVP	$\mathbf{IN}: v_1, \dots, v_n \in \mathbf{Z}^k, y \in \mathcal{R}^k, d \in \mathbf{R}$
	OUT:distinguish
	YES: $\exists v \in L(v_1,, v_n) \text{ s. t. } y - v _1 \le d$
	NO: $\forall v \in L(v_1, \dots, v_n) \text{ holds } y - v _1 > gd.$
g-SIS	IN :integer matrix $B = (b_1, \ldots, b_n)$, target vector
	$t \in L(b_1, \dots, b_n)$ and $d \in \mathbf{R}$
	OUT:distinguish
	YES: \exists solution $\sum_{i} a_i b_i = t$ with $ b _1 \le d$
	NO: \forall solutions $\sum_i a_i b_i = t$ holds $ b _1 > gd$

OUTLINE: g'-CVP> g'-SIS> g-SSAT(> PCP) > SAT where $g^{(')} = n^{c^{(')}/\log\log n}$ where $n = |\Psi|$ and $c^{(')} > 0$ is some constant.

SAT[F] as a consistency problem Input $\Phi=\psi_1,...,\psi_n$ Boolean functions - 'tests' $x_1,...,x_m$ variables with range F for each test: a list of satisfying assignments Problem Is there an assignment to the tests that is consistent? $\psi_1(x,y,z)$ $\psi_2(w,x,z)$ $\psi_3(y,w,x)$ $\psi_4(x,y,z)$ $\psi_2(x,z)$ $\psi_3(y,w,z)$ $\psi_4(x,y,z)$ $\psi_2(x,z)$ $\psi_3(y,z)$ $\psi_4(y,z)$ $\psi_4(y,z)$ $\psi_4(y,z)$ $\psi_4(y,z)$ $\psi_4(y,z)$ $\psi_4(z,z)$ $\psi_4(z,z)$

(3,2,2)

(2,1,5)



Consistency

(3,1,1)

In the SAT case:

$$A(\psi) = (3,2,5)$$

 $A(\psi)|_{x} := (3)$

 $\forall x \forall \phi, \psi$ that depend on x: $A(\phi)|_{x} = A(\psi)|_{x}$

Consistency

$$S(\psi) = +3$$
 (1) 1,2) \oplus -2 (3) 2,5) \oplus 2 (3,3,1)
$$S(\psi)|_{\chi} := +3$$
 (1) \oplus 0 (3)
$$\begin{cases} (1,1,2) & (3,3,1) \\ (1) & (2) & (3) \end{cases}$$

$$\begin{cases} (1,1,2) & (3,3,1) \\ (1) & (2) & (3) \end{cases}$$

$$(3,2,5)$$
Consistency: $\forall x \forall \phi, \psi \text{ that depend on } x : S(\phi)|_{\chi} = S(\psi)|_{\chi}$

g-SSAT - Definition

Input:

 Φ = $\phi_1,...,\phi_n$ tests over variables $x_1,...,x_m$ with range F for each test ϕ_i - a list of sat. assign. $R\phi_i$

Problem: Distinguish between
[Yes] There is a natural assignment for Φ [No] Any non-trivial consistent super-assignment is of

Theorem: SSAT is NP-hard for $g=n^{c/\log\log n}$.

(conjecture: $g=n^{\epsilon}$, ϵ = some constant)