POLYNOMIAL TIME SOLVABILITY AND INVARIANTS OF THE WITNESS SET

BY MARIO SZEGEDY, RUTGERS CS

szegedy@cs.rutgers.edu

PROPERTIES OF THE WITNESS SET

// INVARIANCE UNDER SOME TRANSFORMATION

↕ POLYNOMIAL TIME SOLVABILITY

PROBLEMS (HOPEFULLY) AMENABLE TO THIS APPROACH:

- Variables $X_1, \dots, X_n$ ranging in A ($|A| = \text{CONST}$, $A = \mathbb{R}$)
- Constraints $C(X_1, \dots, X_n)$ of simple type

$$\text{Input} = \{C_1, C_2, \dots, C_m\}$$

$$\text{Output} = 1 \text{ iff } \exists X_1, \dots, X_n:$$

$$C_1(X_1, \dots, X_n) \wedge C_2(X_1, X_2, \dots, X_n) \wedge \dots \wedge C_m(X_1, \dots, X_n)$$

MANY IMPORTANT PROBLEMS ARE IN THIS FRAMEWORK:

- All CSP (Constraint Satisfaction Problems)
- Graph Isomorphism
- Linear Programming
- Perfect Matching

e.t.c.

CONSTRAINT SATISFACTION PROBLEMS

- $|A| < \infty$ is fixed, independent of n
- Every C_i depends only on a constant number of variables

$\exists$ Clean algebraic approach, gives an amazing, rich structure
Explored by Jeqvors and co-authors
(Bulatov, Dalmau, Barto, Kozik, Krokhin, Cohen, Gyssens, Maroti, Larose, Zadori ....)

UNDERSTANDING (AND GENERALIZING) GAUSSIAN ELIMINATION

Example:

$$X_1 + X_2 + X_3 = 1$$
$$X_1 + X_3 + X_5 = 0 \qquad (1)$$
$$X_2 + X_4 + X_5 = 1$$

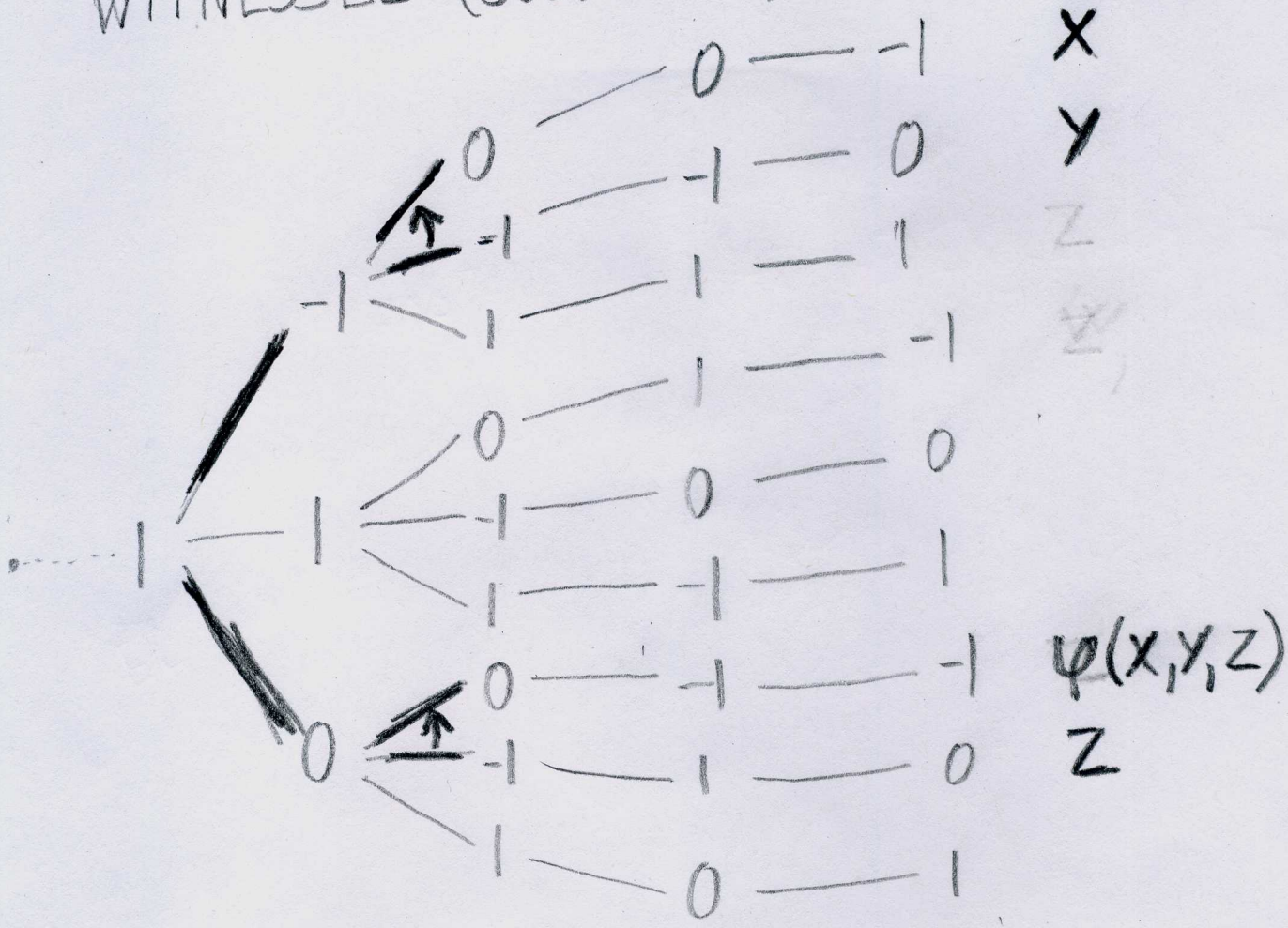
3 indep. lin. equations, 5 variables →
Solution is a 2-dim affine subspace
in the mod 3 arithmetic (GF(3))
9 witnesses

Invariance property:

$X = (X_1, \ldots, X_n)$
$Y = (Y_1, \ldots, Y_n)$ are witnesses, then so is
$Z = (Z_1, \ldots, Z_n)$

$$X - Y + Z = (X_1 - Y_1 + Z_1, \ldots, X_n - Y_n + Z_n)$$

WITNESSES (SOLUTIONS) TO EQUATION (1):



Witness set $R \subseteq \{-1,0,1\}^5$

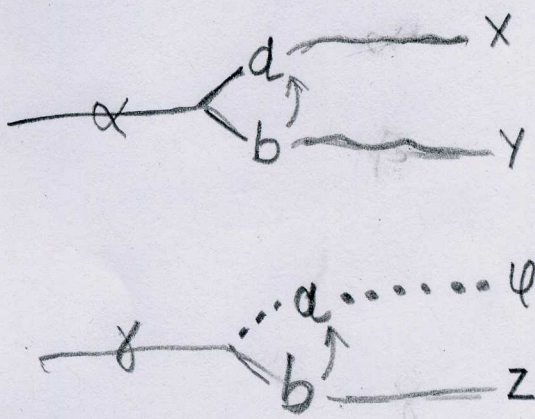
$\varphi : \{-1,0,1\}^3 \to \{-1,0,1\}$ $\quad \varphi(a,b,c) = a-b+c$

$\varphi(X,Y,Z) \stackrel{\text{def}}{=} (\varphi(x_1,y_1,z_1), \varphi(x_2,y_2,z_2), \ldots, \varphi(x_n,y_n,z_n))$

$\{\varphi(x,y,z) \mid x,y,z \in R\} \subseteq R$ Invariance of R

RECTANGLE PROPERTY

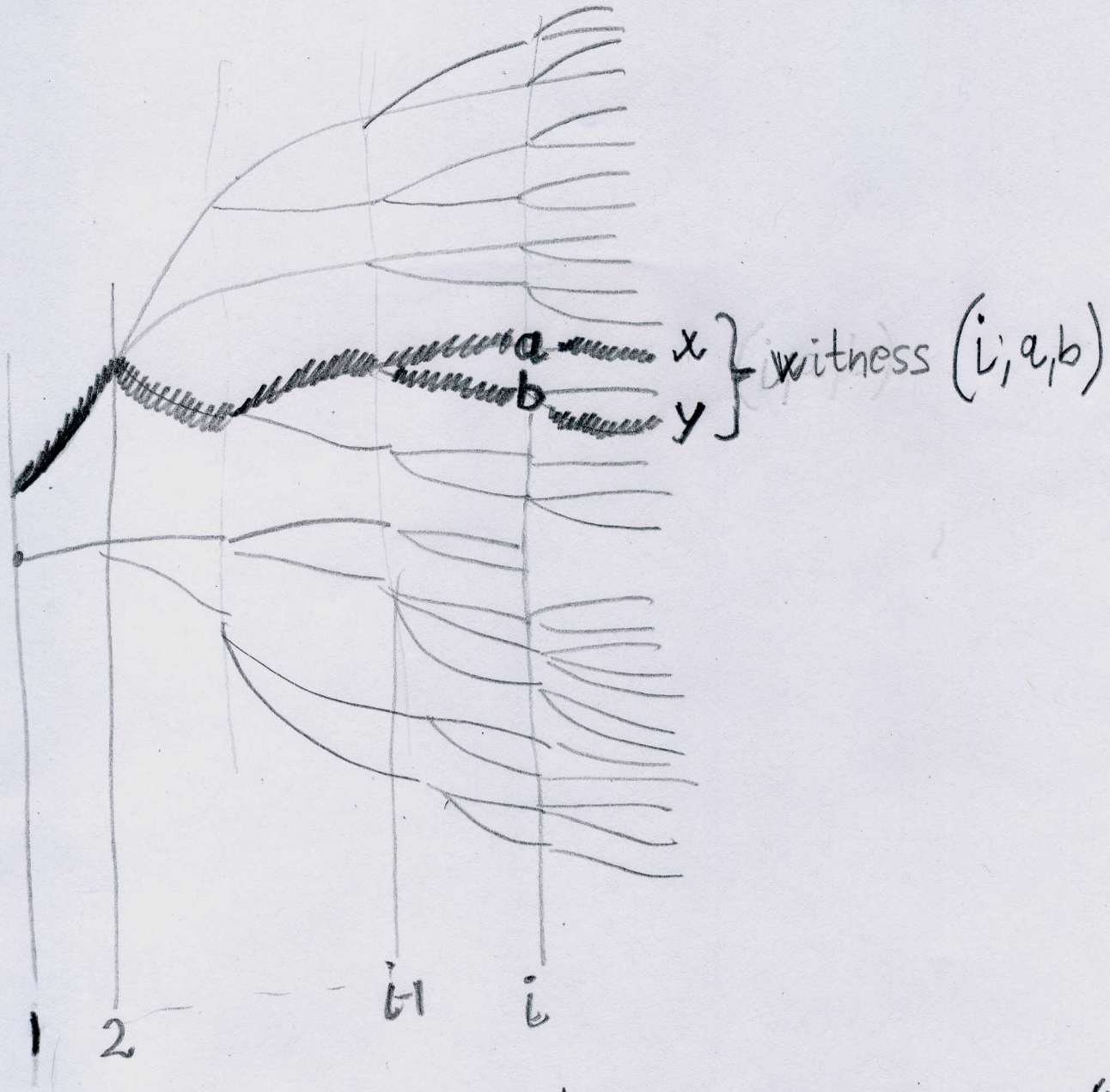
$$\frac{\alpha_1\alpha_2\cdots\alpha_{i-1}\ \mathbf{a}\ \alpha_{i+1}\cdots\alpha_n \qquad \alpha_1\alpha_2\cdots\alpha_{i-1}\ \mathbf{b}\ \beta_{i+1}\cdots\beta_n \qquad \gamma_1\gamma_2\cdots\gamma_{i-1}\ \mathbf{b}\ \gamma_{i+1}\cdots\gamma_n}{\gamma_1\gamma_2\cdots\gamma_{i-1}\ \mathbf{a}\ \delta_{i+1}\cdots\delta_n}$$



Maltsev:

$$\varphi(a,a,b)=\varphi(b,a,a)=b$$

(7)



$$Sig(R) = \{(i,a,b) \in [n] \times A^2 \mid \exists x,y : (x,y) \text{ witnesses } (i,a,b)\}$$

$$R' = \bigcup_{(i,a,b) \in Sig(R)} \{x,y \mid (x,y) \text{ witnesses } (i,a,b)\}$$

Generator set $\leq 2 \cdot n \cdot |A|^2$

(Even when set of solutions has exp. size)

Theorem [Bulatov]: Let φ be a Maltsev operation. Then $CSP[Inv(\varphi)]$ is solvable in polynomial time.

Proof: Let $R_{C_1}, R_{C_2}, \ldots, R_{C_m}$ be the solution sets for constraints $C_1, C_2, \ldots, C_m$. (All R_{C_i} are inv. under φ)

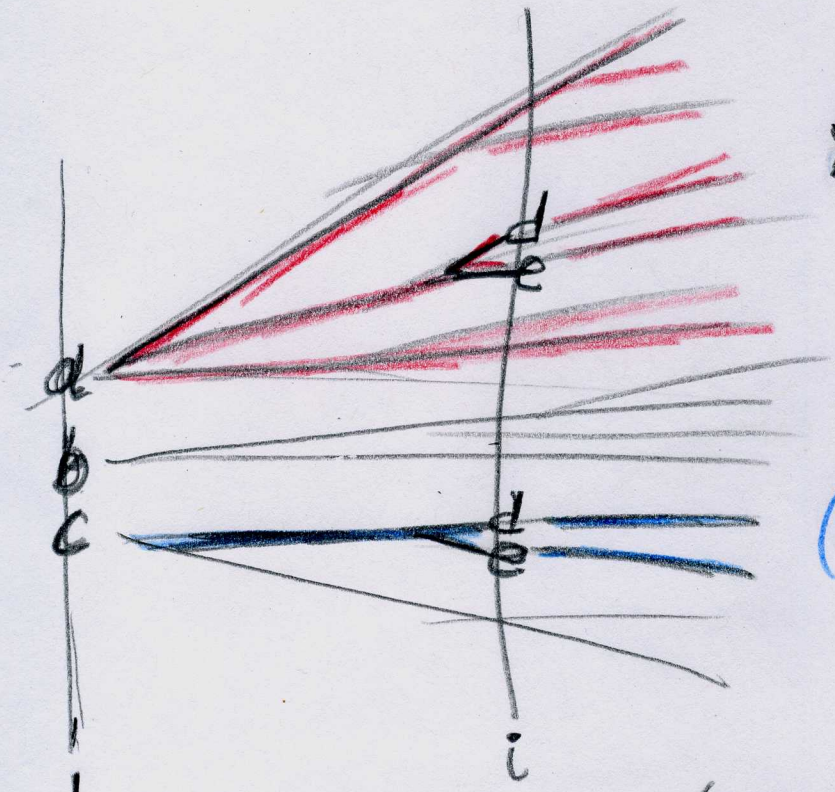
Compute

$Sig(A^n)$, $Sig(R_{C_1})$, $Sig(R_{C_1} \cap R_{C_2})$, ... $Sig(R_{C_1} \cap \cdots \cap R_{C_i})$ ....

and associated witnesses iteratively using the Add_constraint subroutine.

Add_constraint (illustration):

Assume, new constraint is "$x_1 = a$".



$x \in R,\ x_1 = a\ x_i = d$

$\Rightarrow (i,d,e) \in Sig(R)$

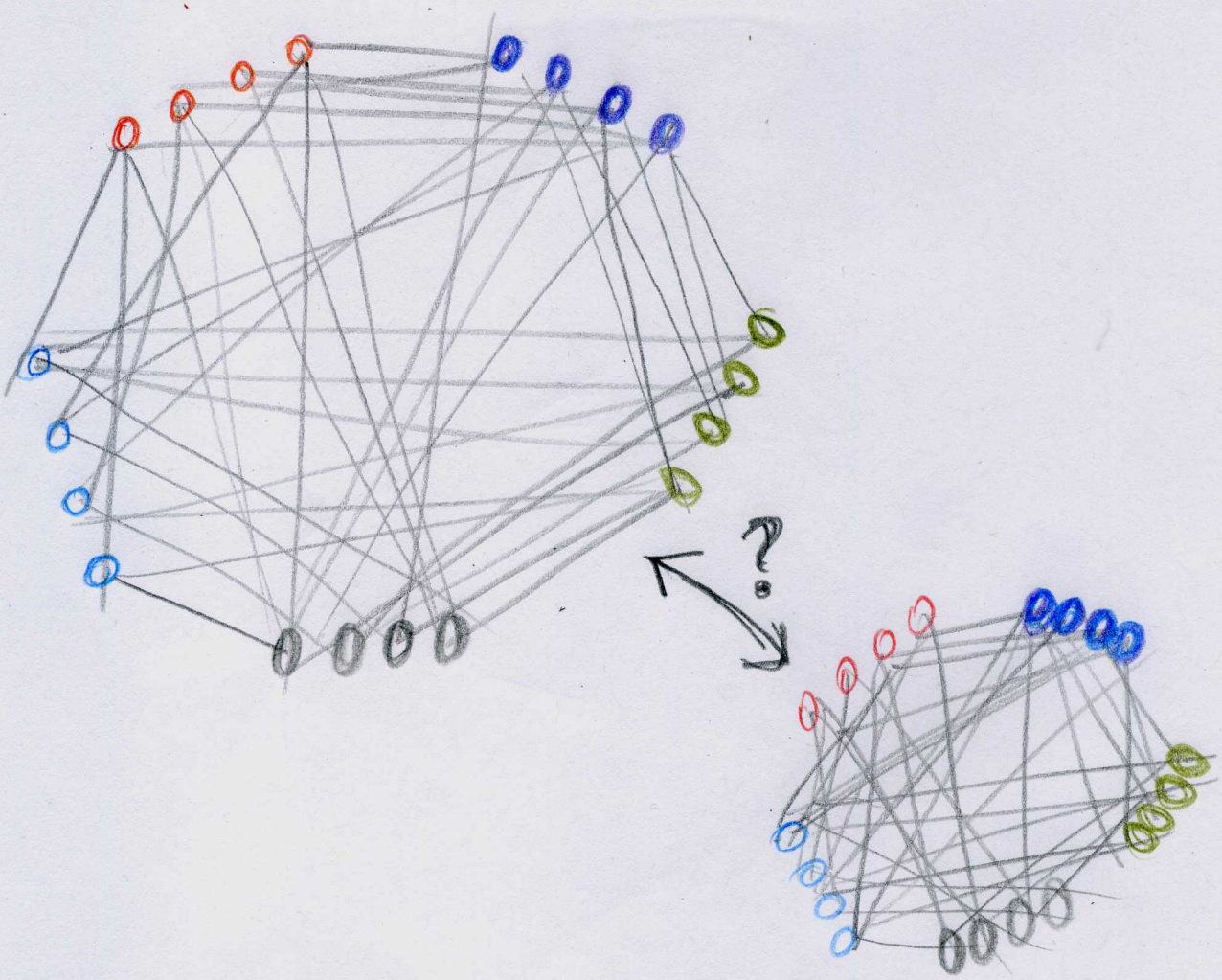
$(i,d,e) \in Sig(R \cap "x_1 = a")$

$Sig(R) \longrightarrow Sig(R \cap "x_1 = a")$

$$Sig(R \cap ("x_1 = a"))_i = Sig(R)_i \cap \left\{ (i,d,e) \;\middle|\; \exists x \in R : \begin{array}{l} x_1 = a \\ x_i = d \end{array} \right\}$$

Restrict all generators of R to 1st & i^{th} coordinates and by exhaustive search try to generate (d,d) on these two coordinates.

GRAPH ISOMORPHISM



Each color class has size k

$A = S_k$ ($\pi \in A$ corresponds to a 1-1 map btwn. nodes of the same color class)

Mal'tsev: $\varphi(\pi, \rho, \tau) = \pi\rho^{-1}\tau$