An Alternative Eager Encoding of the All-Different Constraint over Bit-Vectors

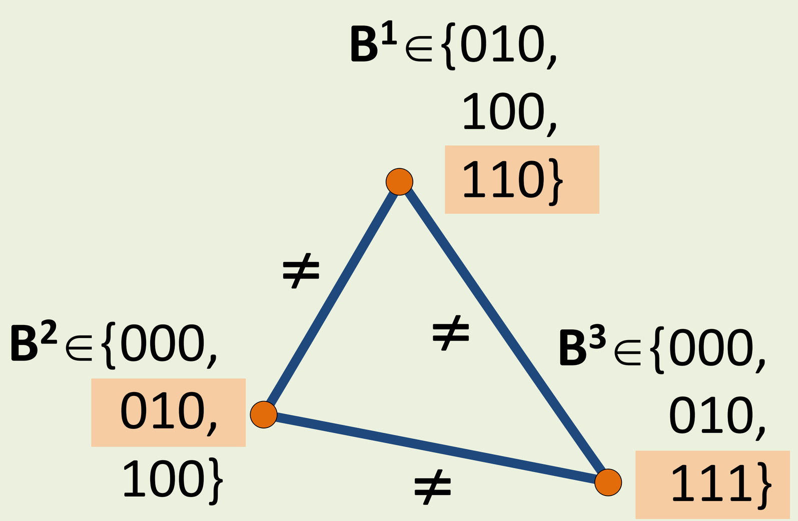
Pavel Surynek

Faculty of Mathematics and Physics, Charles University in Prague, Czech Republic

Graduate School of Maritime Sciences, Kobe University, Japan

All-Different over Bit-Vectors

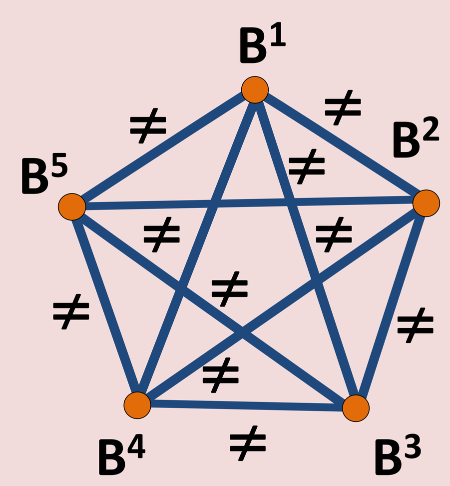
- **All-Different** constraint
  - a **finite** set of variables with **finite** domain
  - each variable should be **assigned** a value from its domain
  - all the assigned values should be **distinct**
- Special case with **bit-vectors**
  - the involved variables are bit-vectors of fixed length $l \in \mathbb{N}$
  - domains consist of subsets of possible bit assignments
- Example:
  - **All-Different(B^1,B^2,B^3)**
  - bit-vectors **B^1,B^2**, and **B^3**
    - length = 3
    - different domains



- Use in the **SAT solving** technology

The Standard Model

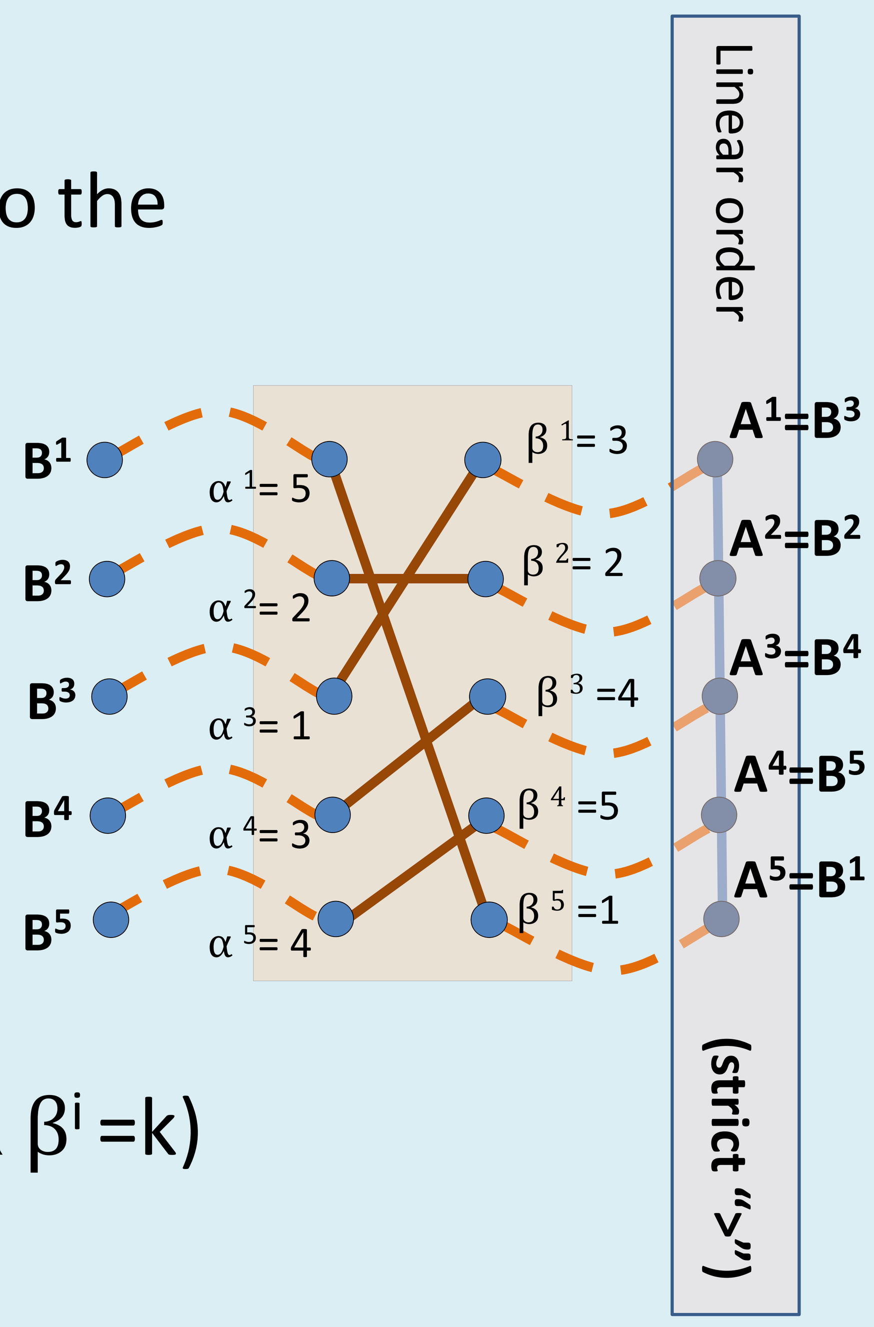
- **All-Different(B^1,B^2, …, B^n)** $\equiv \bigwedge^{n}_{i,j=1;i<j} B^i \neq B^j$
  - **pair-wise differences** are encoded
  - a single difference between two bit-vectors
    - $B^i \neq B^j \equiv \bigvee^{l}_{\mathbb{i}=1}(\neg B^i_{\mathbb{i}} \vee B^j_{\mathbb{i}}) \wedge (B^i_{\mathbb{i}} \vee \neg B^j_{\mathbb{i}})$



- **Auxiliary variables** are needed to translate the formula into CNF efficiently

A New Alternative Model

- Introduce certain kind of **anti-symmetry** into the model
  - allow a SAT solver to **quickly discover** unsatisfiability
- **Map** the original bit-vectors to a **linearly ordered** set of auxiliary bit-vectors
  - **A^1,A^2, …,A^n** linearly ordered bit-vectors of length l
  - **α^1, α^2, …, α^n** auxiliary bit-vectors of length $\lceil \log_2 n \rceil$
    - α^i determines what A^j the original B^i is mapped to
  - **β^1, β^2, …, β^n** auxiliary, length $\lceil \log_2 n \rceil$
    - ensure that at most one original bit-vector is mapped to a single ordered bit-vector
- **Bijection constraint** $\equiv \bigwedge^{n}_{i,k=1} \alpha^k = i \Rightarrow (B^k = A^i \wedge \beta^i = k)$
- **Linear order constraint** $\equiv \bigwedge^{n-1}_{i=1} A^i < A^{i+1}$



Theoretical Comparison

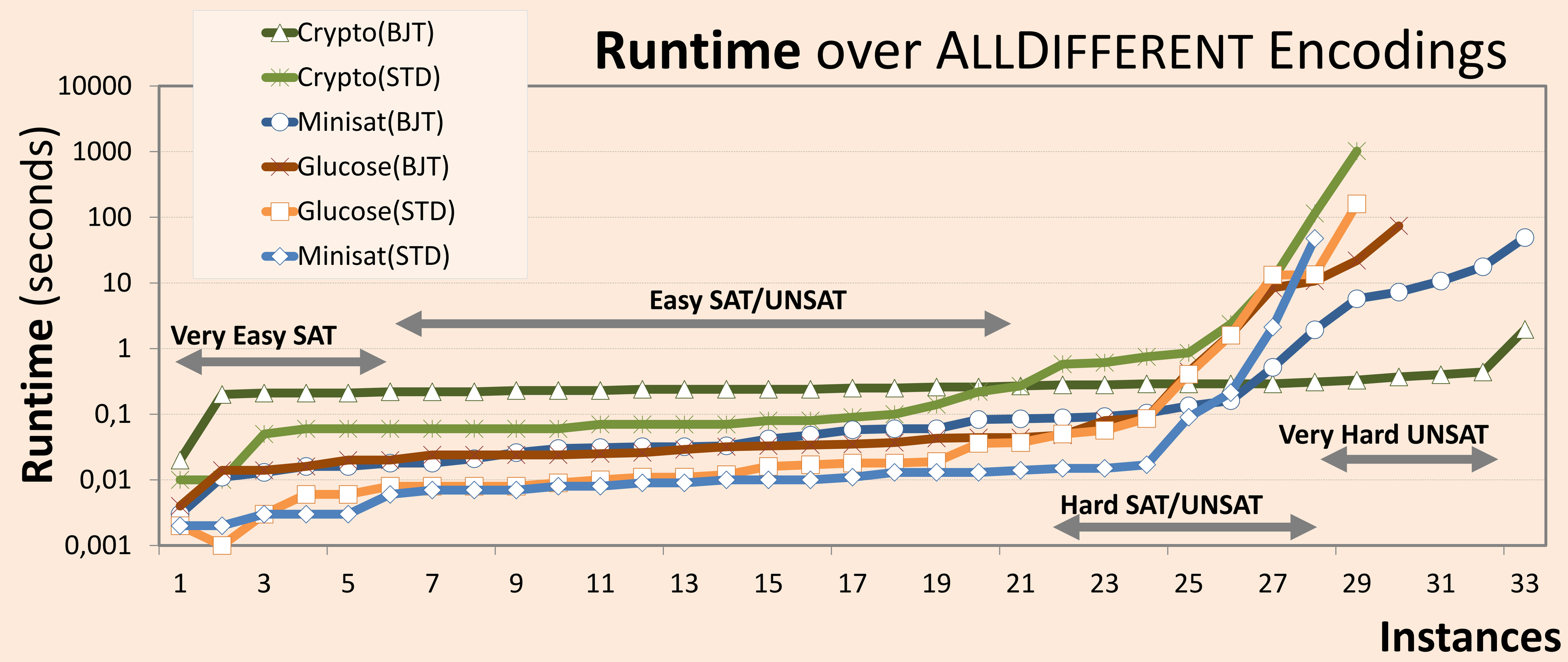
- **Standard** model
  - **$l \cdot n$** visible propositional variables, **$l \cdot n(n+1)/2$** auxiliary
  - **$1+l \cdot n(n+1)$** clauses
- **Alternative** model
  - **$2l \cdot n$** visible, **$2n\lceil \log_2 n \rceil$** bijection, **$n^2+l(n-1)$** auxiliary
  - **$n^2(1 + l + \lceil \log_2 n \rceil) + l \cdot (l + 1)(n - 1)$** clauses

Model Size Evaluation

#bit-vectors (16-bits)	Standard		Alternative	
	#Variables	#Clauses	#Variables	#Clauses
64	67584	133056	9968	176943
128	266240	536448	28400	690031
256	1056768	2154240	90096	2756591

Runtime Evaluation

- **Setup**
  - 32 bit-vectors of length l, domain random **interval** of size up to 34, single all-different constraint



Conclusions

- **Pros and cons** of the alternative model
  - **fewer** variables
  - **more** constraints
  - **better** for discovering unsatisfiability in the hard case
  - **big overhead** in the easy case
- **Observation**
  - prominent solver sensitivity
- **Future works**
  - lazy integration with the SMT solver
  - evaluation in applications

ECAI 2012 - the 20th European Conference on Artificial Intelligence, Montpellier, France