MLL proof nets as error-correcting codes

Satoshi Matsuoka

AIST

The structure of the talk

1. Introduction to error-correcting codes
2. Introduction to MLL proof nets
3. How to analyze MLL proof nets using coding theory
4. Our results so far

Hamming <7,4> code

- A subset of {0,1}^{7} called **code words**
- Satisfying

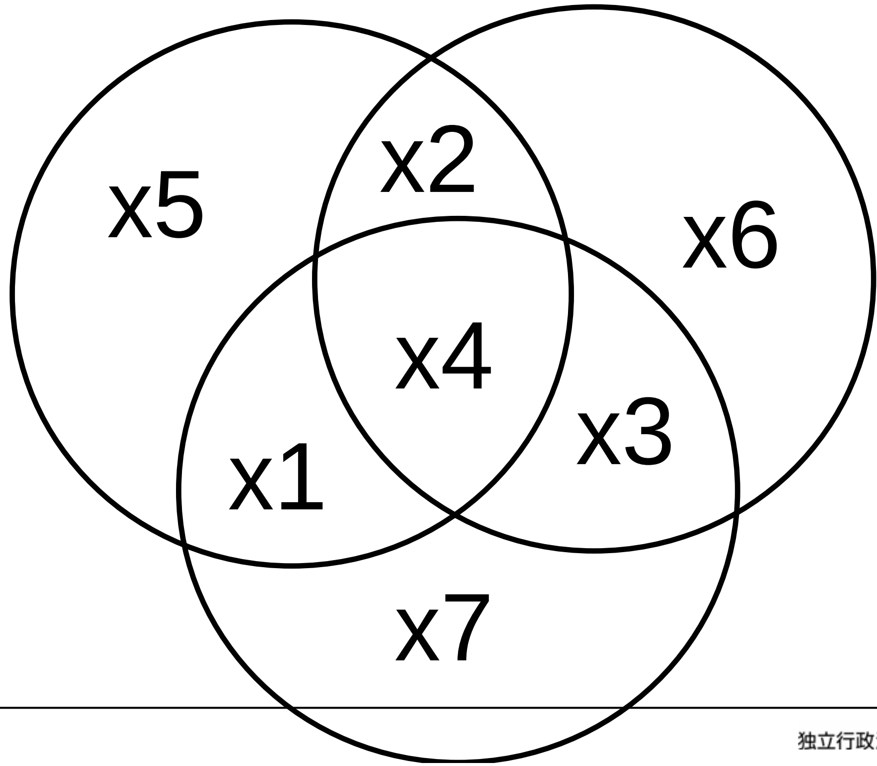
1. x1 + x2 + x4 + x5 = 0
2. x2 + x3 + x4 + x6 = 0
3. x1 + x3 + x4 + x7 = 0

where xi ¥in {0,1}

+ is exclusive or (or parity check)

Hamming <7,4> code (cont.)

1. $x1 + x2 + x4 + x5 = 0$
2. $x2 + x3 + x4 + x6 = 0$
3. $x1 + x3 + x4 + x7 = 0$



Hamming <7,4> code (cont.)

x1	x2	x3	x4	x5	x6	x7
0	0	0	0			
1	0	0	0			
0	1	0	0			
0	0	1	0			
0	0	0	1			
1	0	0	0			
0	1	0	1			
0	0	1	1			

Hamming <7,4> code (cont.)

x1	x2	x3	x4	x5	x6	x7
0	0	0	0	0	0	0
1	0	0	0	1	0	1
0	1	0	0	1	1	0
0	0	1	0	0	0	1
0	0	0	1	1	1	1
1	0	0	1	0	1	0
0	1	0	1	0	0	1
0	0	1	1	1	0	0

Hamming <7,4> code (cont.)

x1	x2	x3	x4	x5	x6	x7
1	1	0	0			
1	0	1	0			
0	1	1	0			
1	1	0	1			
1	0	1	1			
0	1	1	1			
1	1	1	0			
1	1	1	1			

Hamming <7,4> code (cont.)

x1	x2	x3	x4	x5	x6	x7
1	1	0	0	0	1	1
1	0	1	0	1	1	0
0	1	1	0	1	0	1
1	1	0	1	1	0	0
1	0	1	1	0	0	1
0	1	1	1	0	1	0
1	1	1	0	0	0	0
1	1	1	1	1	1	1

Hamming <7,4> code (cont.)

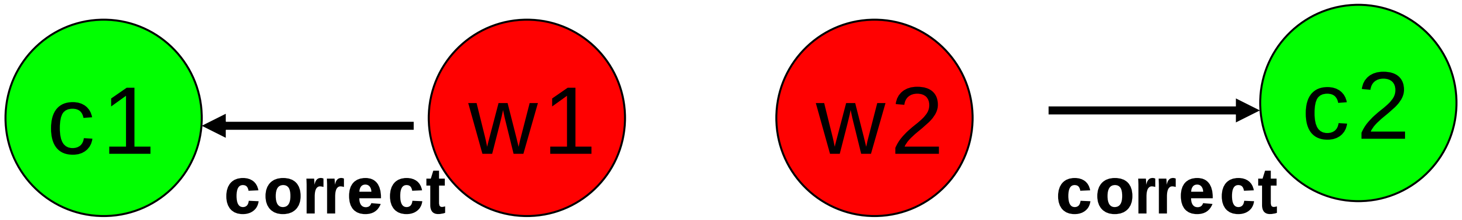
- 2^4 = 16 words are (legitimate) codewords
- Other words (2^7-2^4 = 112) are not

Hamming <7,4> code (cont.)

- distance of w1, w2 ¥in {0,1}^{7}
  d(w1, w2) = | { i | w1(i) ¥neq w2(i)} |
- Example
  d(0101000, 00110011)=4
- The distance of code C, d(C):
  the minimum distance of different codewords
- Hamming <7,4> code C has d(C)=3

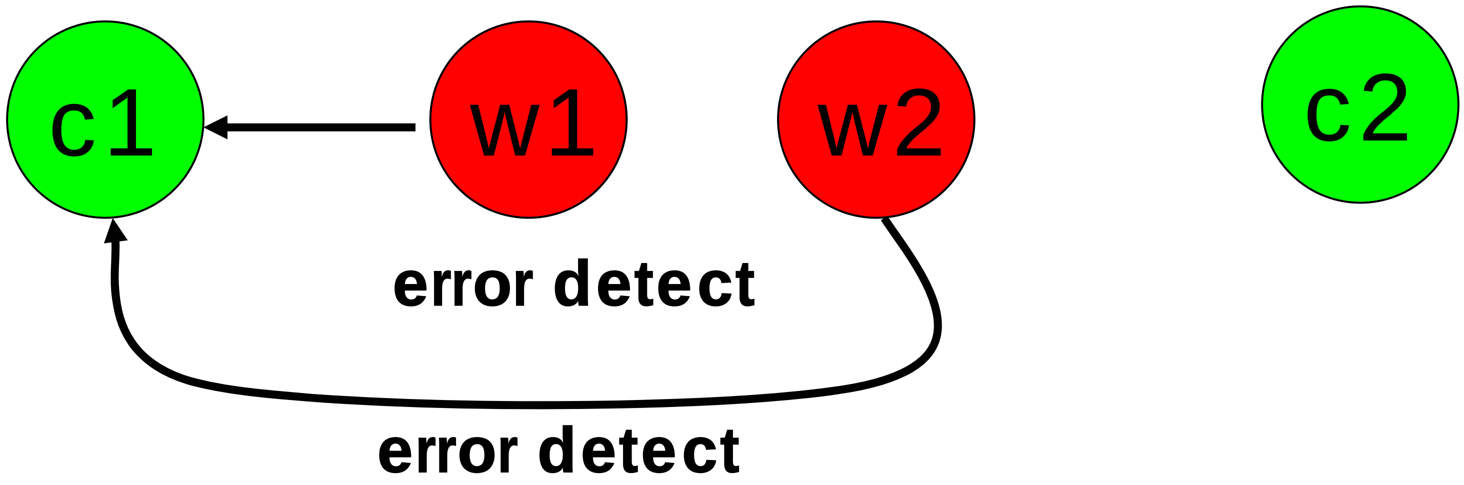
Hamming <7,4> code (cont.)

- So, Hamming <7,4> code is
  1-error correcting



Hamming <7,4> code (cont.)

- On the other hand, Hamming <7,4> code is **2-error detecting**

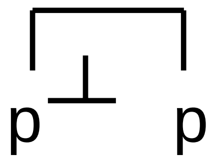


- But, **1-error correcting** and **2-error detecting** are not compatible

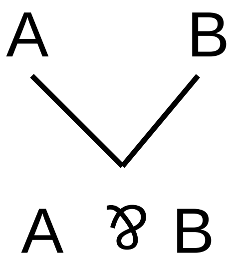
The structure of the talk

1. Introduction to error-correcting codes
2. Introduction to MLL proof nets
3. How to analyze MLL proof nets using coding theory
4. Our results so far

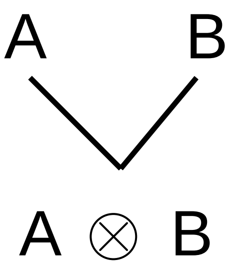
Links



ID-links



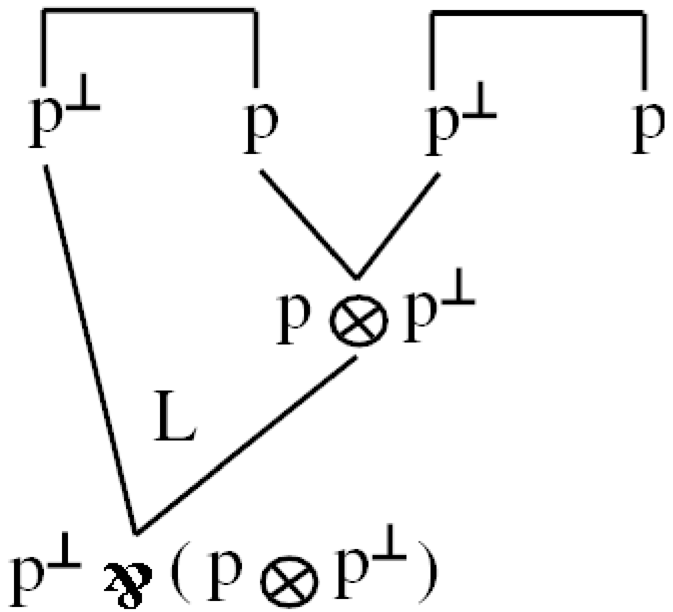
par-links



tensor-links

MLL proof structure (also MLL proof net)

$\Theta 1=$



Graph-theoretic characterization theorem

- Theorem (Girard, Danos-Regnier)

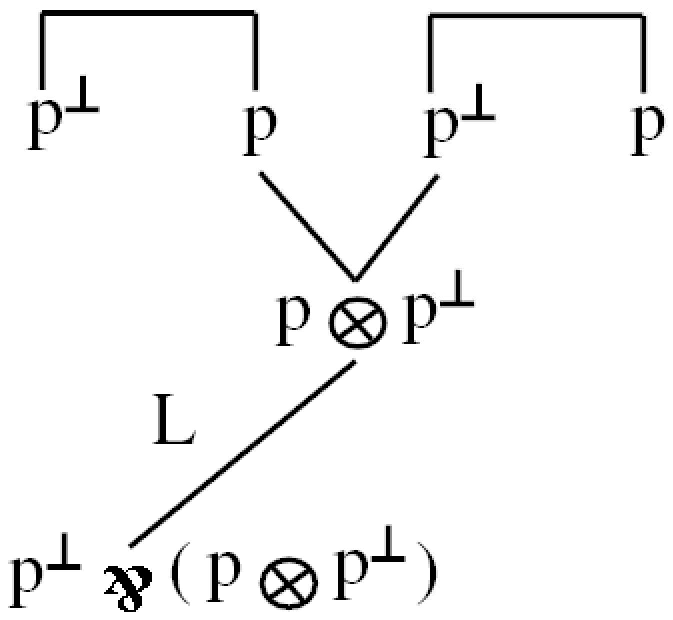
  Θ is MLL proof net

  iff

  for any DR-switching S, the DR-graph Θ_S is acyclic and connected

DR-graph 1 for Θ1

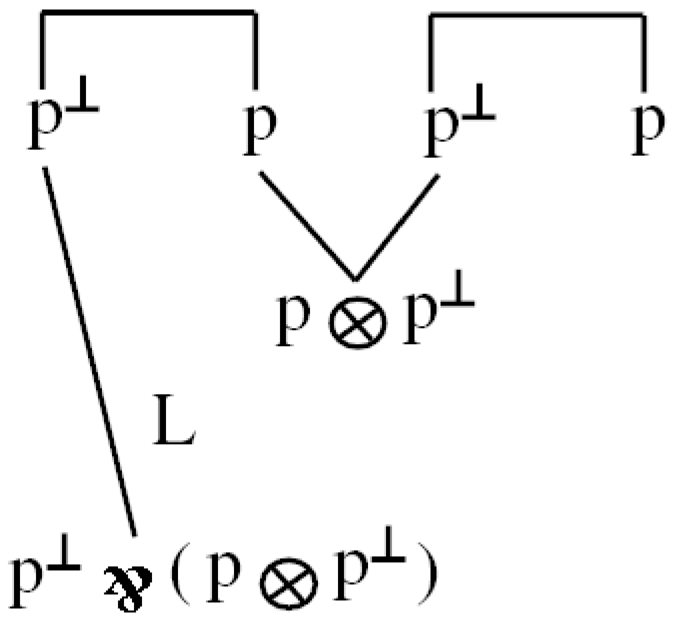
S(L)=Right



acyclic and connected(tree)

DR-graph 2 for Θ1

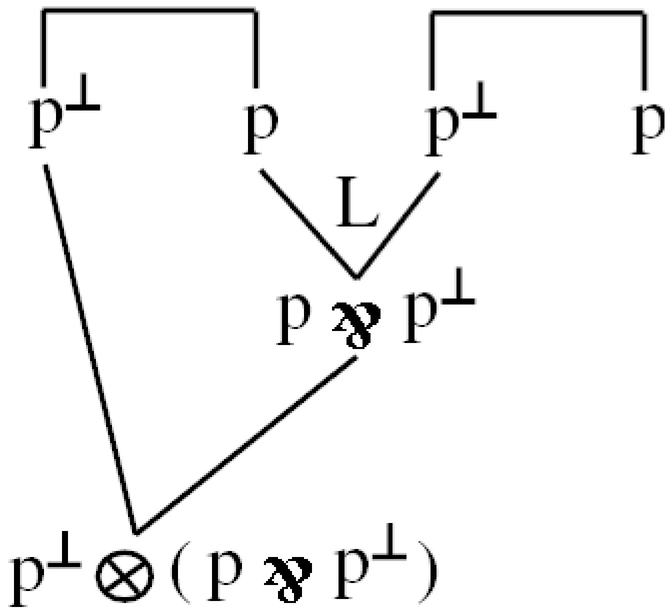
S(L)=Left



acyclic and connected(tree)

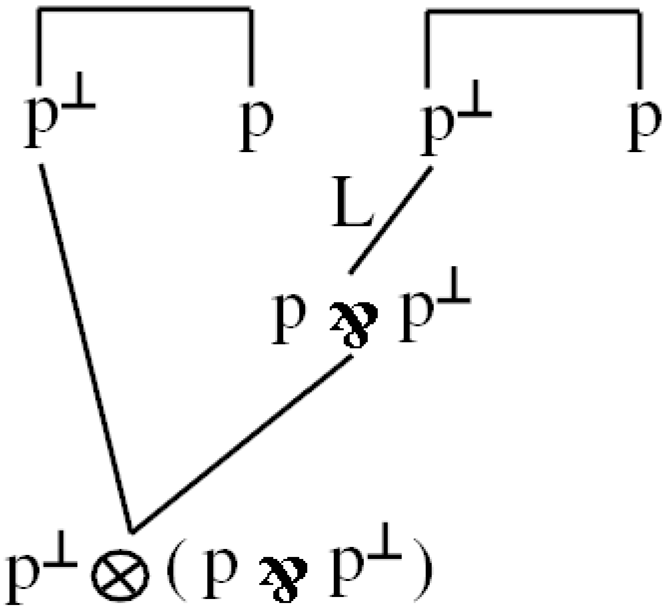
MLL proof structure (but not MLL proof net)

Θ2=



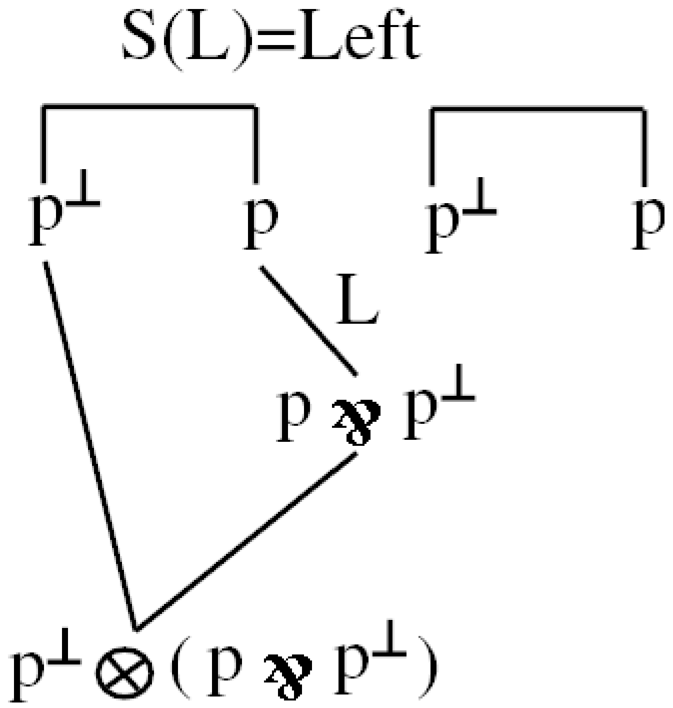
DR-graph 1 for Θ2

S(L)=Right



acyclic and connected(tree)

DR-graph 2 for Θ2



has a cycle

The structure of the talk

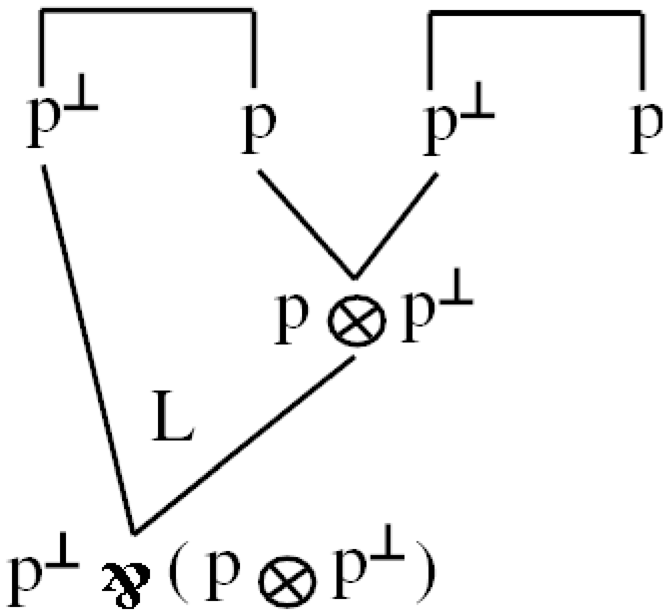
1. Introduction to error-correcting codes
2. Introduction to MLL proof nets
3. How to analyze MLL proof nets using coding theory
4. Our results so far

The Basic Idea

- **PS-family**: a set of MLL proof structures such that each member is reachable from the other members by **several tensor-par exchanges**
- Partition MLL proof structures into PS-families
- Regard each PS-family as a code

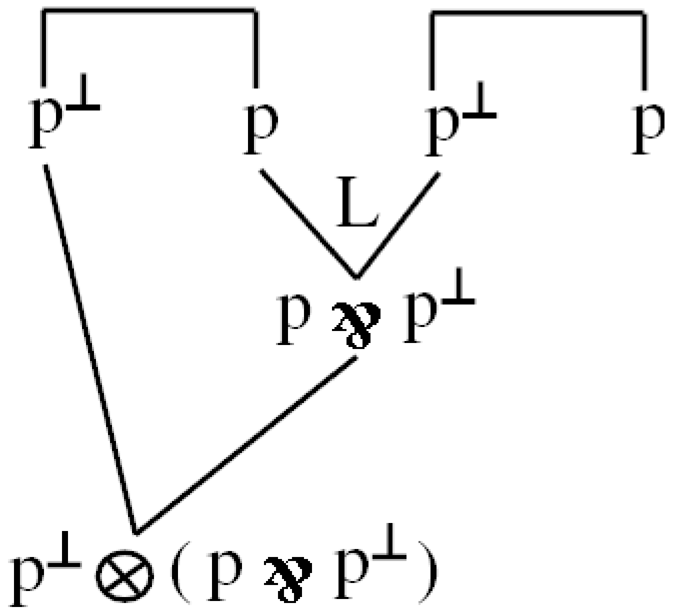
One of four members of a PS-family

Θ1=



One of four members of a PS-family

$\Theta 2=$

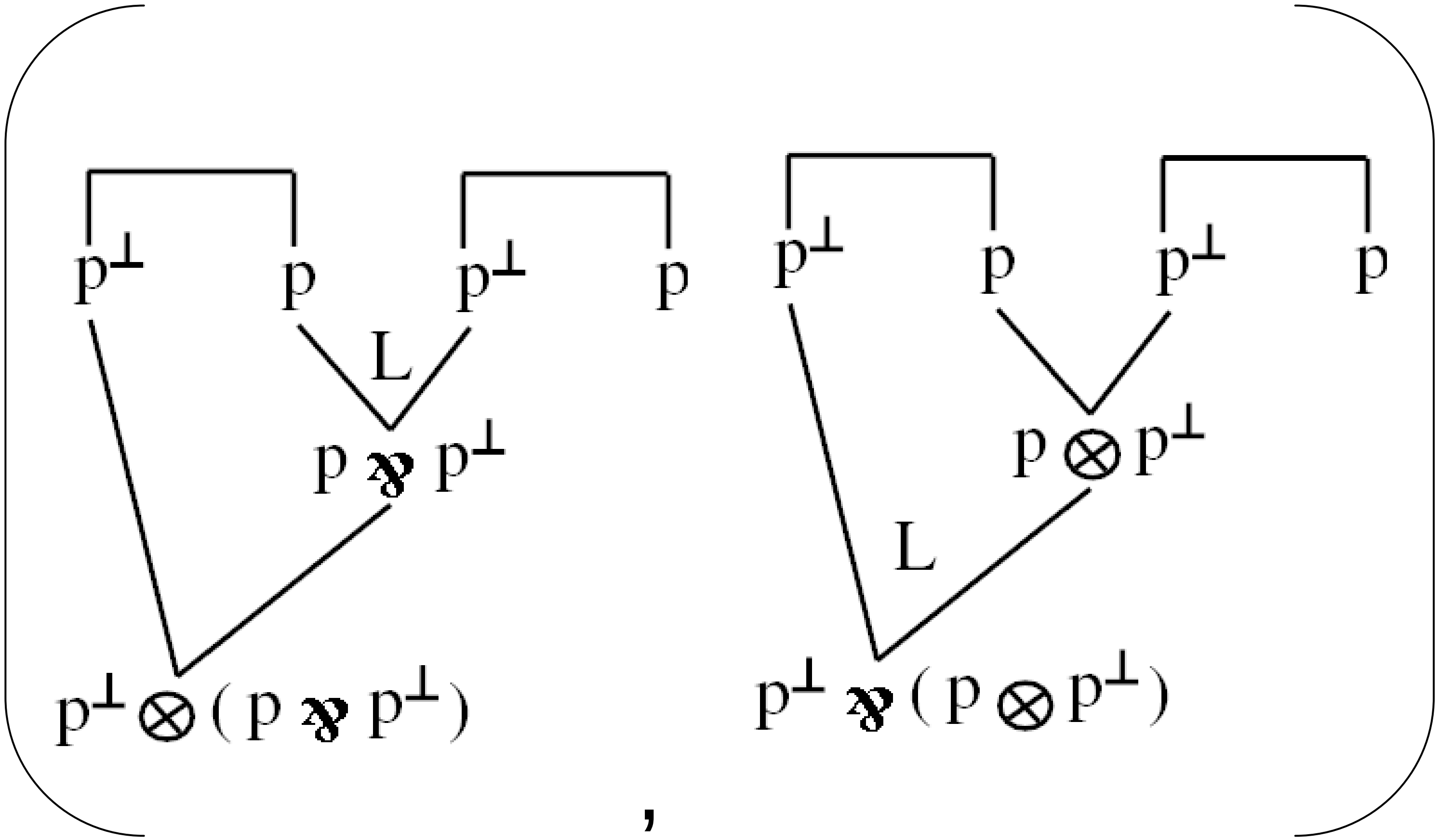


Hamming distance on a PS-family

- distance of Θ1, Θ2 ¥in PS-family F
  d(Θ1, Θ2)
  = the number of "locations" where
  multiplicative links are different
- For each PS-family F,
  d(F) is the minimum distance of
  different MLL proof nets in F

Example

d



= 2

The structure of the talk

1. Introduction to error-correcting codes
2. Introduction to MLL proof nets
3. How to analyze MLL proof nets using coding theory
4. Our results so far

First Question

- How do we have properties about d(F)?

Proposition

- Let F be a PS-family.

  If Θ_1 and Θ_2 are MLL proof nets and both belong to F, then the number of ID-links (tensor-links, and par-links) of Θ_1 is the same as that of Θ_2.

Theorem

If PS-family F has more than two MLL proof nets, then d(F)=2.

So, such a PS-family is just **one-error detecting**.

Idea of Proof

If Θ, Θ' ¥in F, then we can have a sequence

$\Theta \Rightarrow \Theta 1 \Rightarrow \cdots \Rightarrow \Theta n \Rightarrow \Theta'$

such that Θ1,...,Θn are MLL proof nets

where Θa ⇒ Θb if Θb is obtained from Θa by replacing a tensor-link by a par-link and a par-link by a tensor-link exactly two times

Using graph-theoretic characterization theorem, nontrivial (at least for me)

Using reduction to absurdity

Summary

- We can incorporate the notion of Hamming distance into MLL proof nets naturally
- Got an elementary result
- But it's ongoing work
- Need to get more results (composition of two PS-families, characterization of PS-families with n MLL proof nets,….)
- The manuscript can be found in

  http://arxiv.org/abs/cs/0703018