Karlsruhe Institute of Technology

Generalised Test Tables

Discussion at AIS, TU München
20 July 2017

Dr. Mattias Ulbrich

Project: IMPROVE APS

Institut für Theoretische Informatik
Anwendungsorientierte Formale Verifikation
Prof. Dr. B. Beckert

DFG SPP 1593

Purpose of this meeting

Scientists

propose a novel formal verification notation and engine.
Design goal: comprehensibility and usability

meet

Engineers from automation industry

- know industrial practice
- know industrial requirements for validation processes

$\Rightarrow$ can value usability of the proposal

Questions we would like to ask . . .

- If you use test tables today:
  - What feature do you miss in your table technique?
  - Which presented generalisation feature do you like (and which not . . .)?
- Would validation using generalised test tables be a valuable extension to your validation processes?
- What are the requirements to use a formal verification tool like the presented?
  (e.g., tradeoff specification effort vs. more coverage)

Industrial Practice: Testing

- Automated production systems must be validated

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases

Sequence of signals in clock cycles

	$\mathbf{In}_1$	$\mathbf{In}_2$	$\mathbf{Out}_1$	$\mathbf{Out}_2$
1	1	0	FALSE	FALSE
2	3	1	FALSE	TRUE
3	3	5	FALSE	TRUE
4	2	1	TRUE	TRUE
5	9	4	TRUE	TRUE
6	3	4	TRUE	FALSE
7	3	5	TRUE	FALSE
8	9	4	TRUE	FALSE

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.
  - Test tables describe behaviour examples, not concepts.

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.
  - Test tables describe behaviour examples, not concepts.
  - Higher coverage means more tables

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.
  - Test tables describe behaviour examples, not concepts.
  - Higher coverage means more tables

Goals of project:

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.
  - Test tables describe behaviour examples, not concepts.
  - Higher coverage means more tables

Goals of project:

→ **Increase test coverage!**

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.
  - Test tables describe behaviour examples, not concepts.
  - Higher coverage means more tables

Goals of project:

→ **Increase test coverage!**

→ **Keep Comprehensibility!**

Industrial Practice: Testing

- Automated production systems must be validated
- Practice today: **Test tables** describe individual test cases
- Test coverage is not optimal:
  - Unexpected rare corner cases may be overlooked.
  - Test tables describe behaviour examples, not concepts.
  - Higher coverage means more tables

Goals of project:

→ **Increase test coverage!**

→ **Keep Comprehensibility!**

→ **Increase Expressiveness!**

Generalised Test Tables

Generalise known concept: Test tables ($\rightsquigarrow$ Excel sheets)

Generalised Test Tables

Generalise known concept: Test tables ($\leadsto$ Excel sheets)

Generalisation Concepts:

Generalised Test Tables

Generalise known concept: Test tables ($\rightsquigarrow$ Excel sheets)

Generalisation Concepts:

1. *Abstraction*: Not concrete values, but constraints

   –, [4,8], > 10 OR ≤ 2

Generalised Test Tables

Generalise known concept: Test tables ($\rightsquigarrow$ Excel sheets)

Generalisation Concepts:

1. *Abstraction*: Not concrete values, but constraints
   –, [4,8], > 10 OR ≤ 2
2. *References*:
   "same value as value of X two cycles earlier"

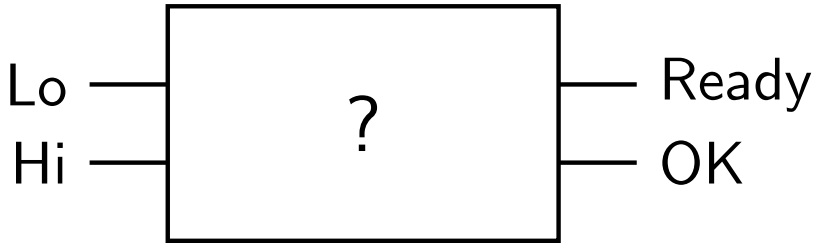
Generalised Test Tables

Generalise known concept: Test tables ($\rightsquigarrow$ Excel sheets)

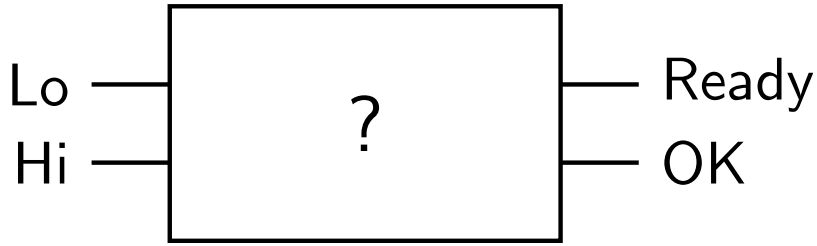
Generalisation Concepts:

1. *Abstraction*: Not concrete values, but constraints
   –, [4,8], > 10 OR ≤ 2
2. *References*:
   "same value as value of X two cycles earlier"
3. *Variable durations*:
   "must hold for 5-10 cycles", "... for at least 20 cycles"

Example



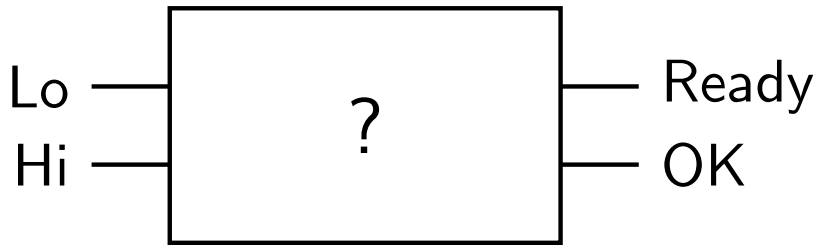
Example



	Lo	Hi	Ready	OK
1	1	0	FALSE	FALSE
2	3	1	FALSE	TRUE
3	3	5	FALSE	TRUE
4	2	1	TRUE	TRUE
5	9	4	TRUE	TRUE
6	3	4	TRUE	FALSE
7	3	5	TRUE	FALSE
8	9	4	TRUE	FALSE

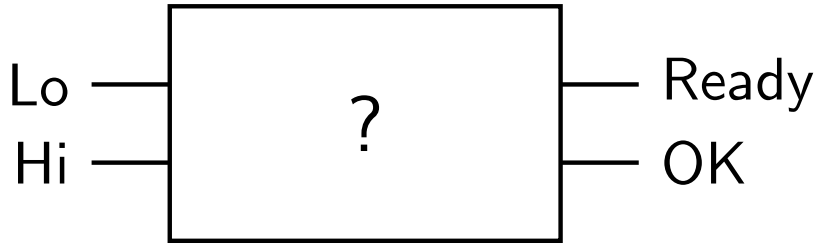
Concrete table – difficult to recognize concept

Example



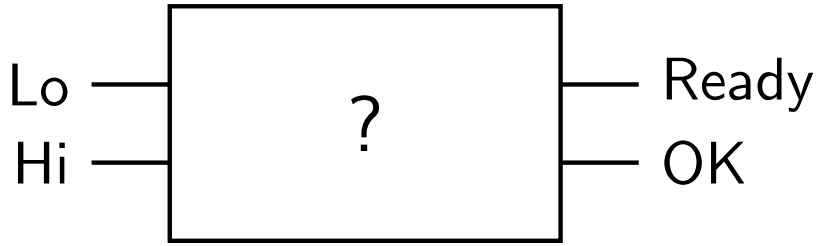
Lo	Hi	Ready	OK	Dur

Example



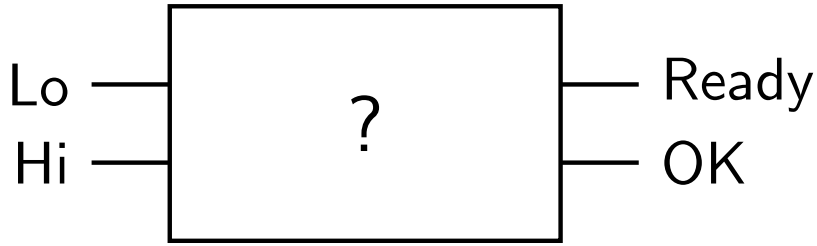
	Lo	Hi	Ready	OK	Dur
1	–	–	FALSE	–	$[0, 10]$

Example



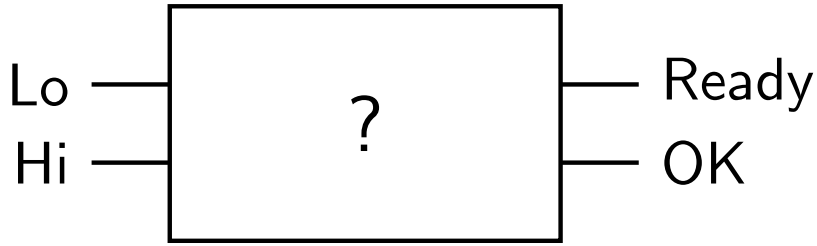
	Lo	Hi	Ready	OK	Dur
1	–	–	FALSE	–	$[0, 10]$
2	–	$> Lo$	TRUE	TRUE	–

Example



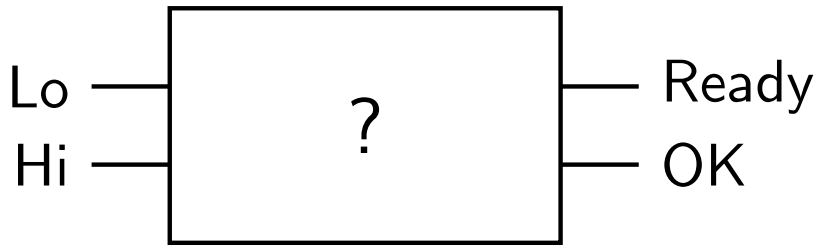
	Lo	Hi	Ready	OK	Dur
1	–	–	FALSE	–	$[0, 10]$
2	–	$> Lo$	TRUE	TRUE	–
3	–	$\leq Lo$	TRUE	FALSE	1

Example



	Lo	Hi	Ready	OK	Dur
1	–	–	FALSE	–	$[0, 10]$
2	–	$> Lo$	TRUE	TRUE	–
3	–	$\leq Lo$	TRUE	FALSE	1
4	–	–	TRUE	FALSE	–

Example



	Lo	Hi	Ready	OK	Dur
1	–	–	FALSE	–	$[0, 10]$
2	–	$> Lo$	TRUE	TRUE	–
3	–	$\leq Lo$	TRUE	FALSE	1
4	–	–	TRUE	FALSE	–

Generalised table:

- better coverage (*many* test cases covered by this table)
- still comprehensible
- documents the idea of the block

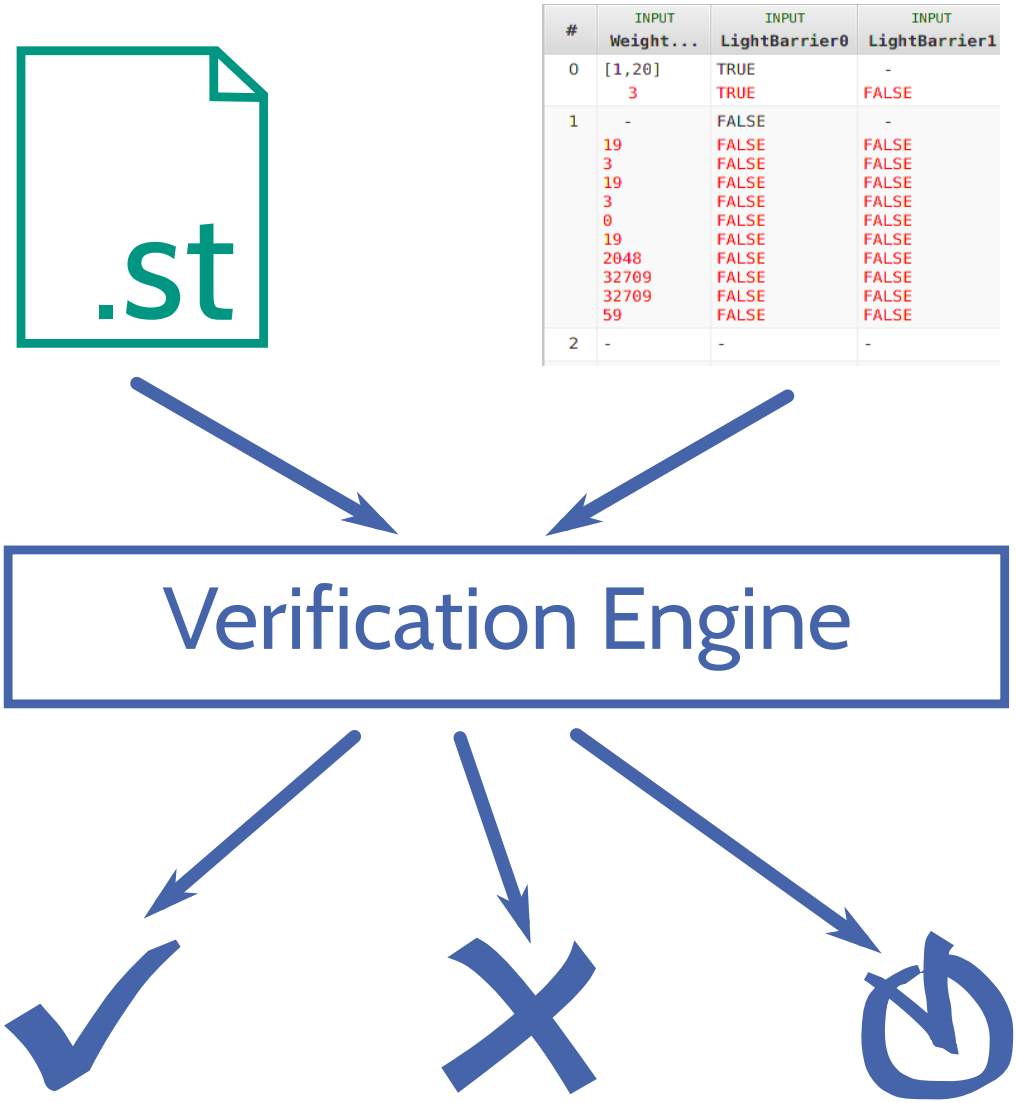
Tool

ST Verification Studio

`http://formal.iti.kit.edu/stvs`

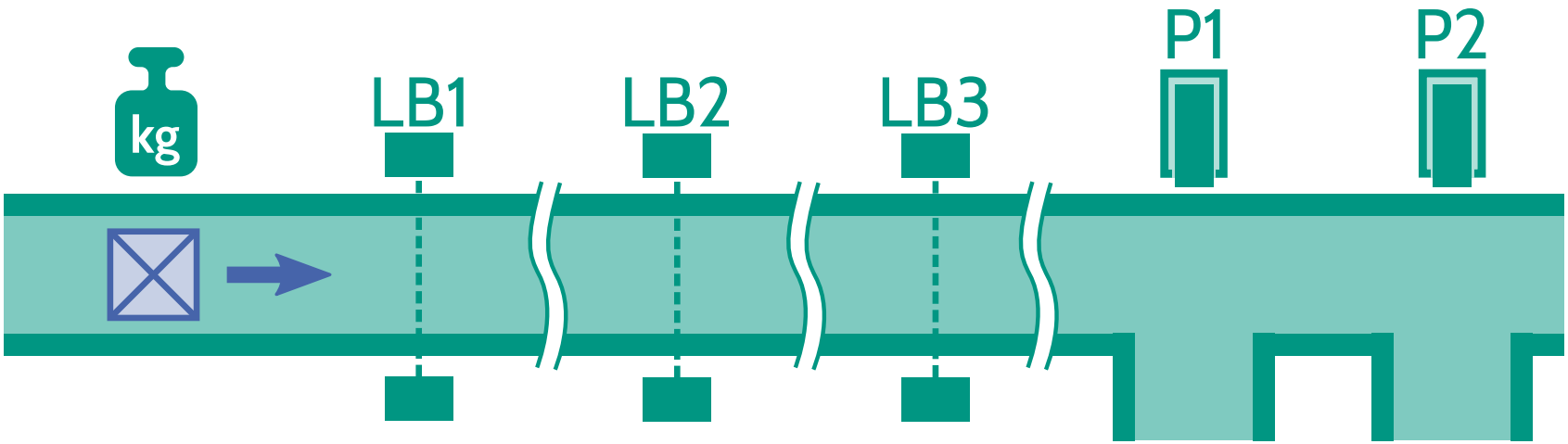
- Concepts for Interactive Table Exploration
- “Table-driven debugging”
- Prototypical implementation is there – extension on the way

Verification



#	INPUT Weight...	INPUT LightBarrier0	INPUT LightBarrier1
0	[1,20]	TRUE	-
	3	TRUE	FALSE
1	-	FALSE	-
	19	FALSE	FALSE
	3	FALSE	FALSE
	19	FALSE	FALSE
	3	FALSE	FALSE
	0	FALSE	FALSE
	19	FALSE	FALSE
	2048	FALSE	FALSE
	32709	FALSE	FALSE
	32709	FALSE	FALSE
	59	FALSE	FALSE
2	-	-	-

Example Production System



Exploring the Counterexample

Specification Table

#	INPUT Weight...	INPUT LightBarrier0	INPUT LightBarrier1	INPUT LightBarrier2	INPUT LightBarrier3	INPUT Workpi...	OUTPUT MoveBelt	OUTPUT Push1	OUTPUT Push2	OUTPUT ERROR	Duration
0	[1,20]	TRUE	-	-	-	EXPRESS	-	-	-	NO_ERROR	1
	3	TRUE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	1
1	-	FALSE	-	-	-	-	-	-	-	NO_ERROR	[4,19]
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	10
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	0	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	2048	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	32709	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	32709	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	59	FALSE	FALSE	FALSE	FALSE	EXPRESS	FALSE	FALSE	FALSE	MISS_LIGHTBARRIER_1	
2	-	-	-	-	TRUE	-	-	TRUE	-	NO_ERROR	1

Exploring the Counterexample

Specification Table

#	INPUT Weight...	INPUT LightBarrier0	INPUT LightBarrier1	INPUT LightBarrier2	INPUT LightBarrier3	INPUT Workpi...	OUTPUT MoveBelt	OUTPUT Push1	OUTPUT Push2	OUTPUT ERROR	Duration
0	[1,20]	TRUE	-	-	-	EXPRESS	-	-	-	NO_ERROR	1
	3	TRUE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	1
1	-	FALSE	-	-	-	-	-	-	-	NO_ERROR	[4,19]
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	0	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	2048	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	32709	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	32709	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	59	FALSE	TRUE	FALSE	FALSE	EXPRESS	FALSE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	0	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	2048	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	MISS_LIGHTBARRIER_2,	
2	-	-	-	-	TRUE	-	-	TRUE	-	NO_ERROR	1

Exploring the Counterexample

Specification Table

#	INPUT Weight...	INPUT LightBarrier0	INPUT LightBarrier1	INPUT LightBarrier2	INPUT LightBarrier3	INPUT Workpi...	OUTPUT MoveBelt	OUTPUT Push1	OUTPUT Push2	OUTPUT ERROR	Duration
0	[1,20]	TRUE	-	-	-	EXPRESS	-	-	-	NO_ERROR	1
	3	TRUE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	1
1	-	FALSE	-	-	-	-	-	-	-	NO_ERROR	[4,19]
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	0	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	2048	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	32709	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	32709	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
	59	FALSE	TRUE	FALSE	FALSE	EXPRESS	FALSE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	3	FALSE	FALSE	TRUE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	0	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	19	FALSE	FALSE	FALSE	FALSE	EXPRESS	TRUE	FALSE	FALSE	NO_ERROR	
	2048	FALSE	FALSE	TRUE	FALSE	NORMAL	TRUE	FALSE	FALSE	NO_ERROR	
2	-	-	-	-	TRUE	-	-	TRUE	-	NO_ERROR	1