VDM over PSP: A Pilot Course for VDM Beginners to Confirm its Suitability for Their Development

Hisayuki Suzumori,

Haruhiko Kaiya and **Kenji Kaijiri**

Shinshu University, JAPAN

Contents

- Background and Motivation
- Goal of this Research
- Fundamental Techniques for VDM over PSP (VoP)
  - The PSP: monitoring tech's
  - VDM: evaluated design method in VoP
- VDM over PSP (VoP)
  - Goal and Process
  - Extended Process and Metrics
- Conclusion and Future Works

Background

- Software Development Methods will help software engineers develop software.
  - Especially, Formal Methods will do so.
- How to encourage engineers to use new and/or unfamiliar method?
  - Text books or reports
  - Advertisements or rumors
  - Command or order from the boss

Our Wishes

- Each engineer should try new or unfamiliar methods, and improve his ability.
- He should be able to confirm the suitability of a method for him
  - by himself
  - by using measured data (his own process & products)
  - by focusing on changes of their works, that are carried by the method.

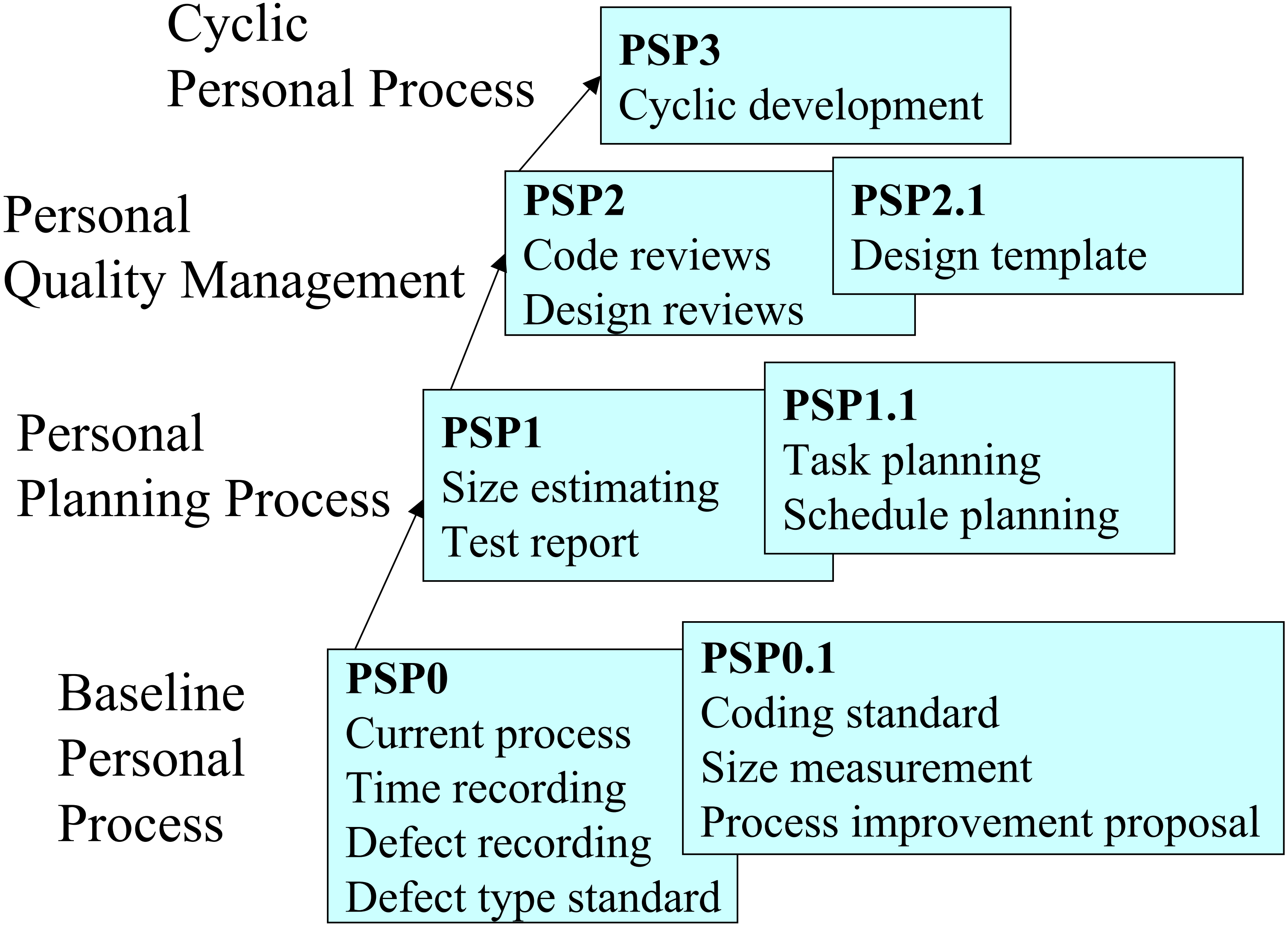
Our Solution

- Providing a (meta-)method for confirming suitability of a method using empirical data.
- **VDM over PSP(VoP)** - A first instance for confirming suitability of a method.
  - Engineers = Students for engineering courses
  - Measurement and Evaluation = based on the PSP
  - Development Method = the VDM

The PSP

- Personal Software Process^{SM} proposed by W. Humphrey
  - ‘a self-improvement process designed to help you control, manage and improve the way you work.’
- Tools and Materials
  - Process scripts and forms for measuring time, defects and products for one’s work.
  - Metrics for evaluating the work.
  - Concrete 10 exercises for practicing the PSP

The PSP Evolution



Cyclic
Personal Process

PSP3
Cyclic development

Personal
Quality Management

PSP2
Code reviews
Design reviews

PSP2.1
Design template

Personal
Planning Process

PSP1
Size estimating
Test report

PSP1.1
Task planning
Schedule planning

Baseline
Personal
Process

PSP0
Current process
Time recording
Defect recording
Defect type standard

PSP0.1
Coding standard
Size measurement
Process improvement proposal

Contents of the PSP

PSP level	measuring method	design method	exercies	
0	time, defects	water fall development	1A	calculate the mean and standard deviation of a set of data
0.1	LOC count	code standard	2A	LOC counter
			3A	LOC counter for each function
1	size, effort estimation	explicit design	4A	Linear regression parameters
1.1	task schedule estimation		5A	numerical integration
			6A	4A + the prediction interval
2	quality measurement	review	7A	correlation
2.1		semi-formal design notations	8A	sorting a linked list
			9A	x2 test for a normal distribution
3			10A	3 parameter multiple regression parameters and the prediction interval

Process Scripts and Forms

- Process Scripts
  - Define pre-conditions, outputs and the ordering of tasks in each development phases.
    - design, coding, compiling, testing ….
  - Basis for measurement
- Forms
  - Define recording schema for efforts(time), defects.
  - Size of products(LOC) is also recorded.

VDM

- Vienna Development Method
- Old and typical formal method
- Formal Specification Language (VDM-SL)
  - Abstract data representation based on sets
  - Invariants for data structures
  - Pre/Post spec. for functions
- Tool Support (provided by IFAD)
  - Syntax checker
  - Type checker
  - Interpreter and Debugger

Examples of VDM spec’s

```
Latitude = real
inv lat == lat >= 0 and lat < 360

AircraftPosition:: lat : Latitude
                   long : Longitude
                   alt : Altitude
```

```
SelectForLanding(radar: radarInfo) aircraft: AircraftId
pre dom radar <> {}
post aircraft in set dom radar
```

Merits and Demerits of VDM

- Merits
  - Rigorous Design
  - Systematic or automatic check for spec’s.
  - Validation of design against requirements by tools.
- Demerits or Obstacles
  - Unfamiliar notations for ordinarily engineers.
    - sets, predicate logics….
    - denotational (not operational) representations.
  - readability

VoP vs. the PSP

- Main goal: Checking suitability of VDM both
  - for each student and
  - for a problem domain.
- No estimation tasks.
- Techniques of VDM are gradually introduced.
- Exercises are designed for a domain where the student will engage.

Role of VDM in VoP

- Quality Management
  - Defect prevention
    - Review guideline and check lists (same as the PSP)
  - Defect elimination
    - Review, syntax/type check and validation of VDM specifications.
- Quality Indexes are based on defects
  - in source codes and
  - in VDM-SL spec’s.

Process Levels in VoP

- VoP0

  baseline of VoP

  PSP2.1 minus estimation tasks.

- VoP1

  + data def’s with invariants and pre/post function def’s using VDM

- VoP2

  + internal spec. for each functions

- VoP3

  +validation of VDM spec’s using tools

VoP3 Process Overview

	phases	
design	planning	
	design	VoP 1 & 2
	design review	
	VDM syntax review	VoP 1 & 2
	Syntax check with Tool	VoP3
	Type check with Tool	
	Validation with Tool	
implementation	coding	
	code review	
	test	
	postmortem	

VDM related phases

Metrics in VoP: Role and Usage

- Role: monitoring the changes (improvement) along with the introduction of VDM techniques.
  - during the continuous exercises.
- Usage: calculating the metrics in each VoP level, observing the changes of its value.
  - Each student can decide whether VDM is suited for him and his problem or not, by referring the changes.

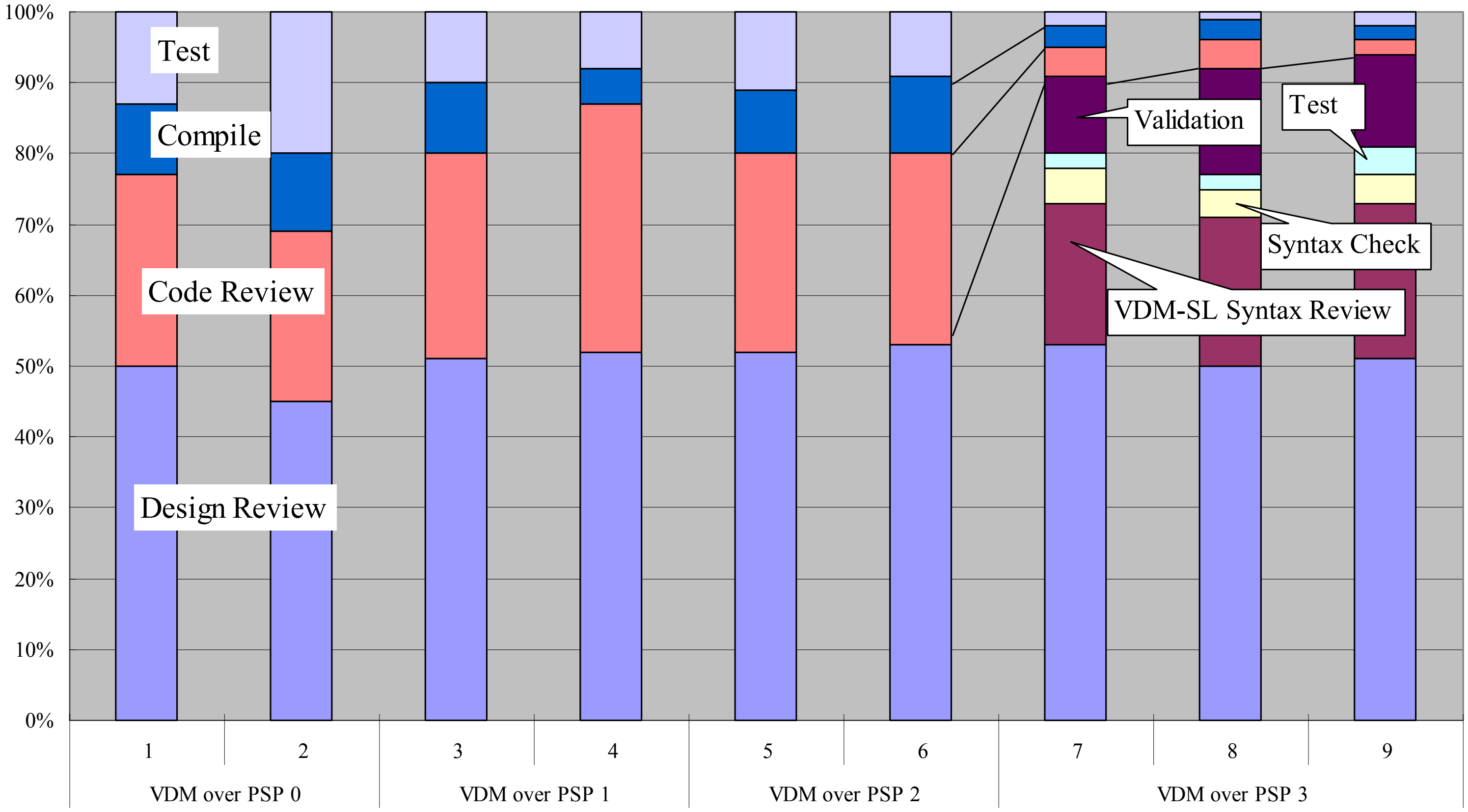
Metrics 1: DDR(design)

- Ratio of design defects removed in a phase to all defects.
- DDR(phase$_i$)

$$= \frac{\#\_of\_design\_defects\_removed\_in\_phase_i}{\#\_of\_all\_design\_defects} \times 100$$

- Typical Evaluation of DDR(VDM related phases)
  - Increase: VDM contributes to eliminate design defects in early phase.
  - Decline: VDM is harmful or useless for design defects elimination.

Example of DDR changes



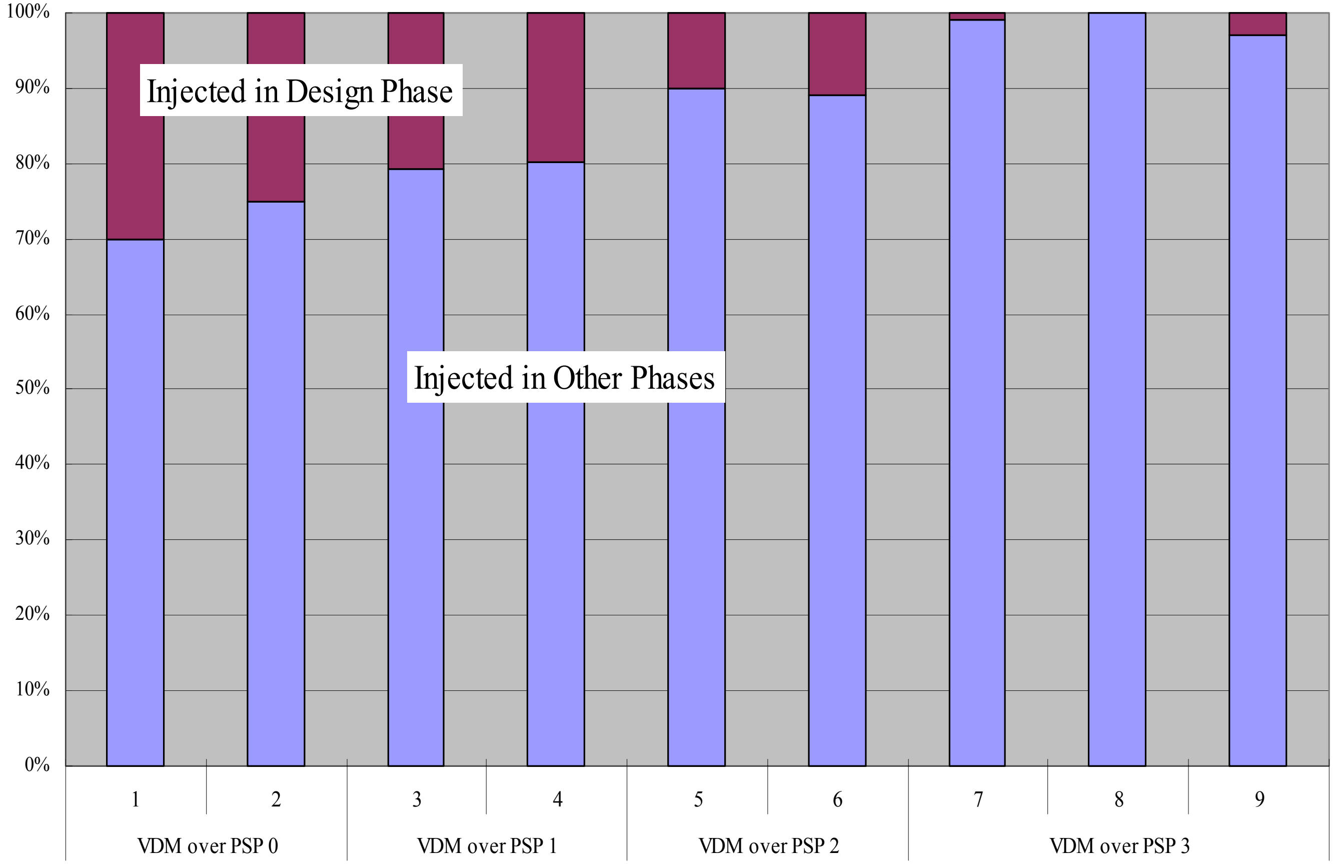
Metrics 2: DDI(design)

- Ratio of design defects injected in a phase to all injected defects.
- DDI(phase_i)

$$= \frac{\#\_of\_design\_defects\_injected\_in\_phase_i}{\#\_of\_all\_design\_defects} \times 100$$

- Typical Evaluation of DDI(VDM related phases)
  - Decline: VDM contributes to prevent design defects in design phase, but VDM may hinder the student deciding design issues in design phase.

Example of DDI changes



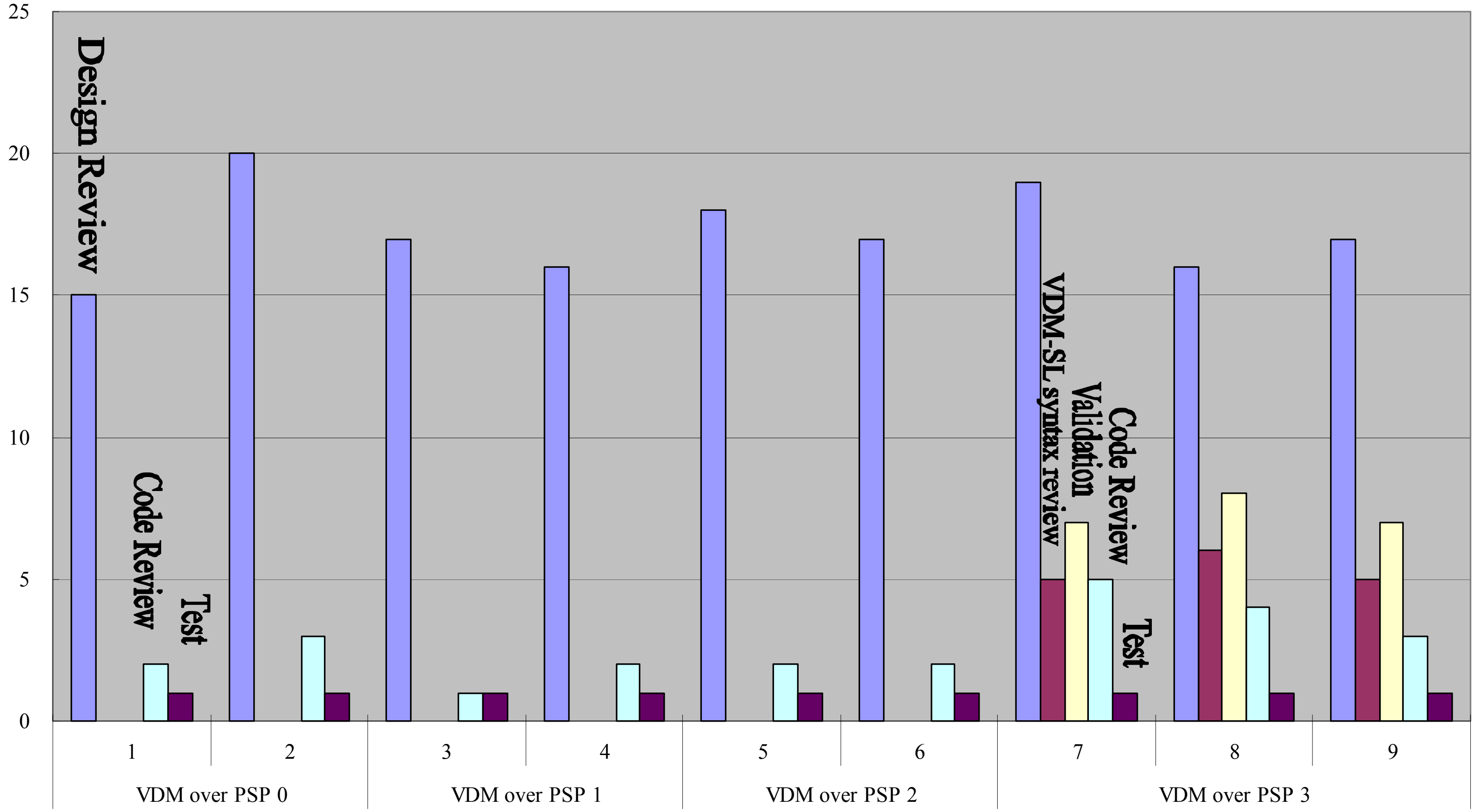
Metrics 3: DDRL(design)

- Design defect removal leverage for a phase.
  - – How efficiently one can remove defects in a phase?
- DDRL(phase$_i$)

$$= \frac{\#\_of\_removed\_defect(phase_i)/hour(phase_i)}{\#\_of\_removed\_defect(unit\_test)/hour(unit\_test)}$$

- Typical Evaluation of DDRL(VDM related phases)
  - – Increase: VDM contributes to improve efficiency of design defect removal.

Example of DDRL changes



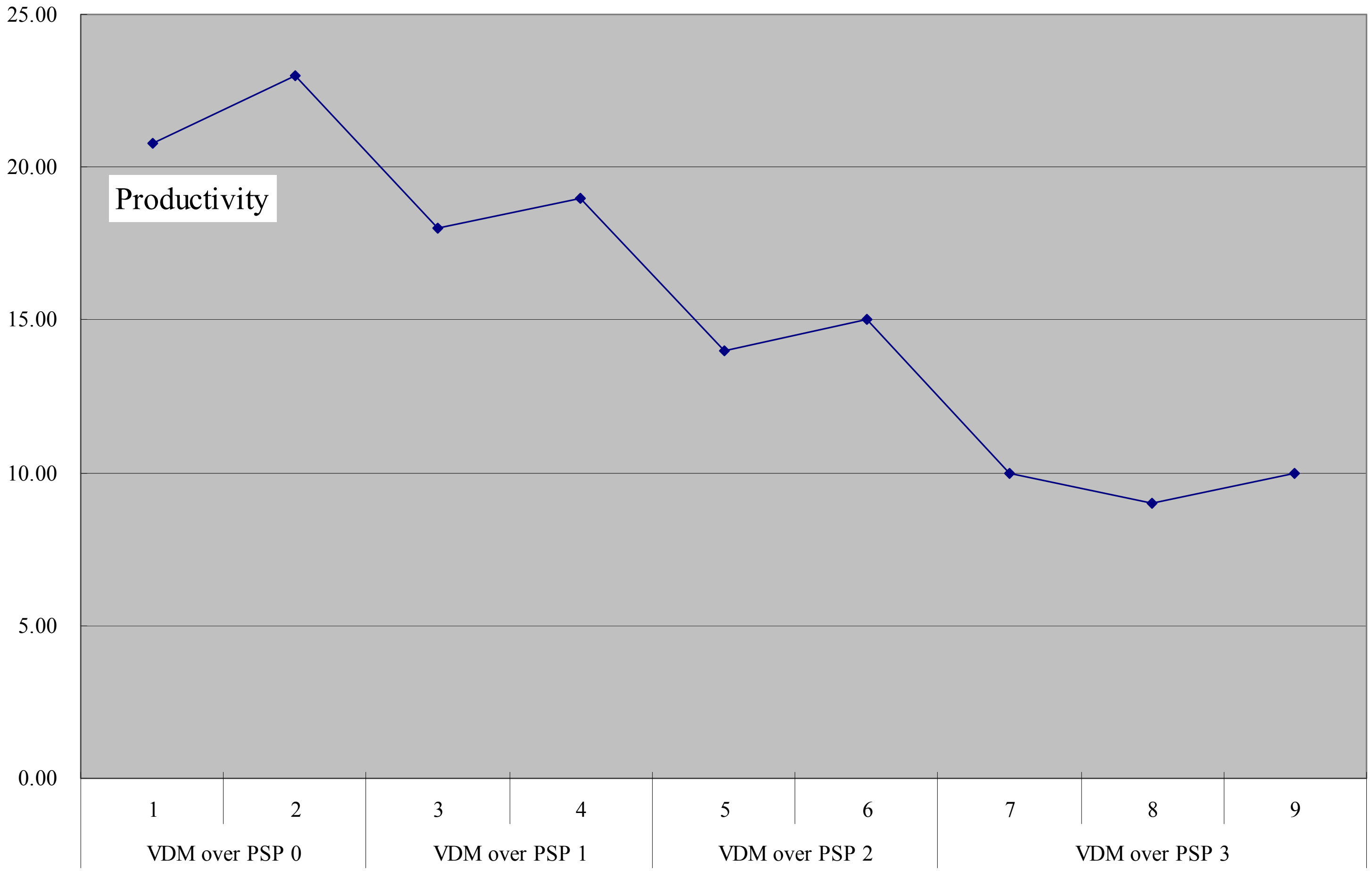
Metrics 4: Productivity

- We only focus on size of source codes(LOC) now.
- Productivity

$$= \frac{Lines\_of\_Codes}{total\_development\_hour}$$

- Typical Evaluation of Productivity
  – Increase: VDM is useful for cost saving.

Example of Productivity changes



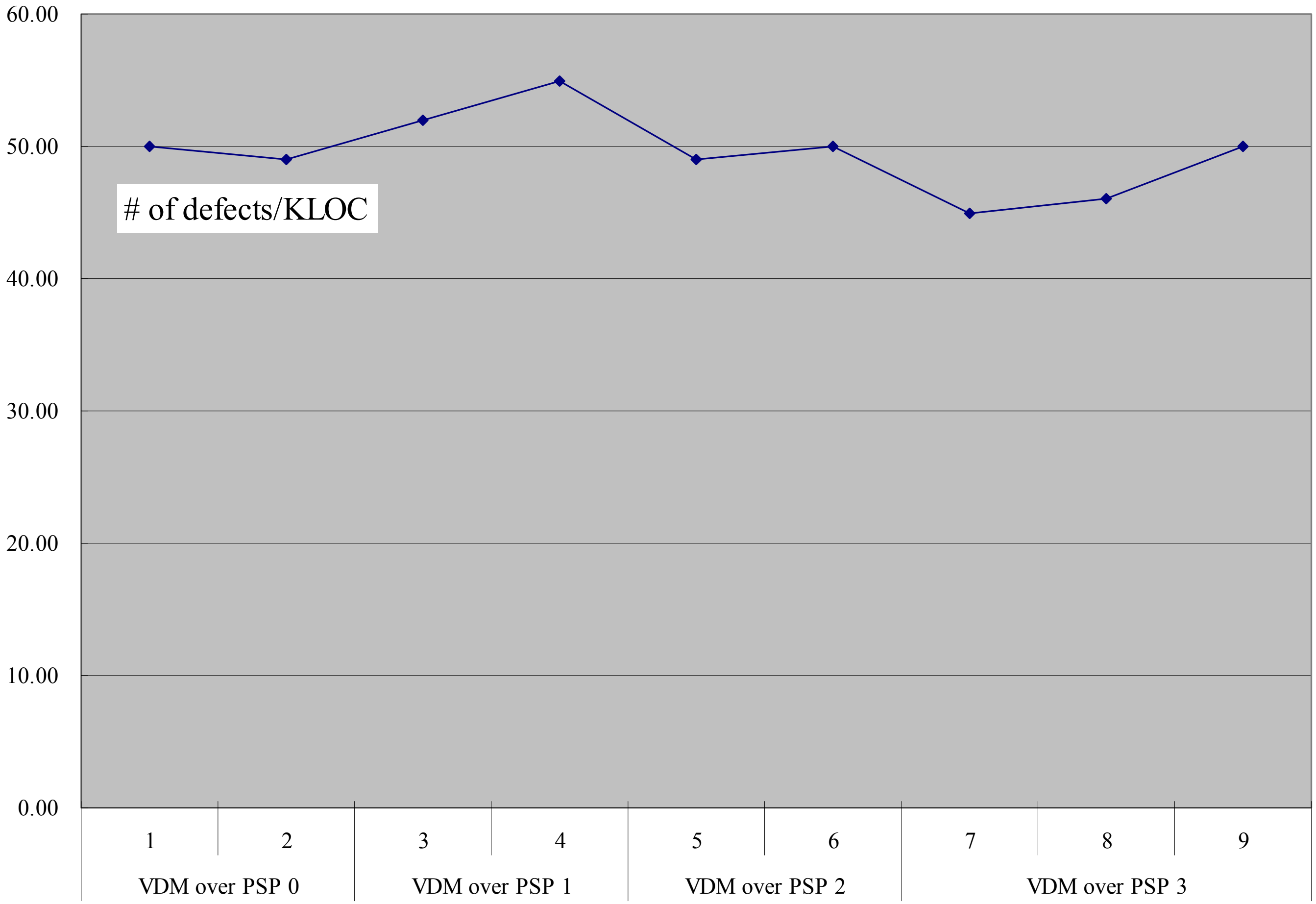
Metrics 5: NDDK

- Number of design defects per KLOC
- NDDK

$$= \frac{all\_design\_defects}{Kilo\_Lines\_of\_Codes}$$

- Typical Evaluation of NDDK
  - – Decline: VDM contributes to improve the design quality.

Example of NDDK



Notes

- All examples does not come from real experiences of VoP, but an imaginary cases based on the normal PSP experiences.
- Any notations could be OK for these metrics, currently we use normal graph notation.

Conclusion

- We present an instance for confirming the suitability of an method, VDM over PSP.
- VDM over PSP
  - specifies what and when techniques in VDM are introduced in a sequence of exercises.
  - specifies what and how data are evaluated so as to decide VDM suitability.

Future Works

- Applying VoP in an academic course.
  - The course will start from Nov. 13! (next week)
- Preparing exercise sets for each problem domain.
- Applying our approach to the other methods
  - e.g. Petri-nets, model checking tech. etc.
  - Using Method Base by exploring suitable method.