セキュリティ情報学実験
～課題説明～

情報理工学域 Ⅱ類
渡邉洋平　阿波拓海　淺野京一

実験の進め方

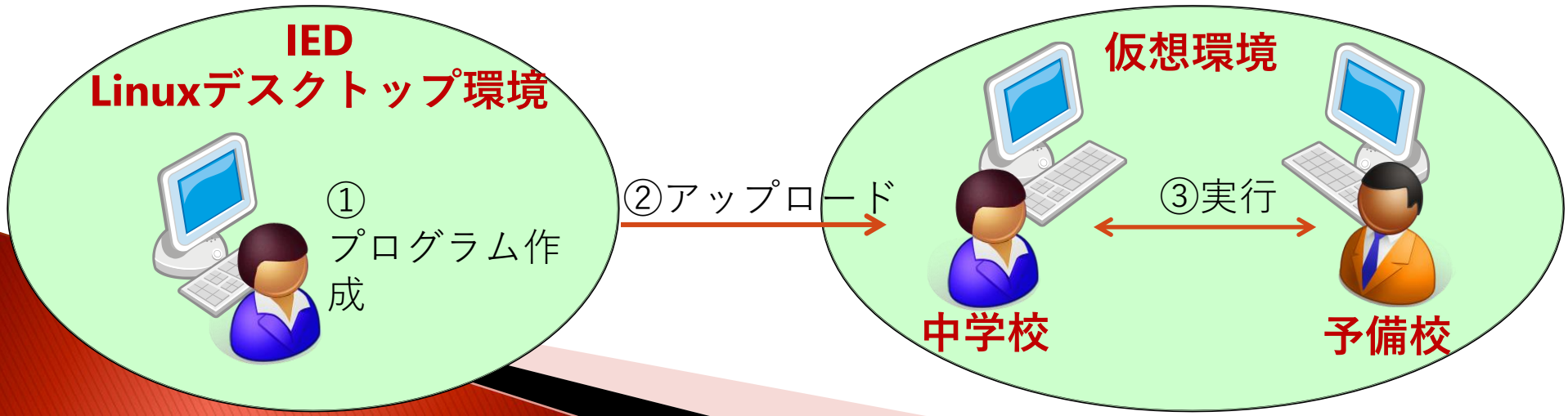
ペアリング

- ２人１組のペアをつくり，中学校の役と予備校の役に分かれて課題を行います．

  ※受講者数が奇数の場合は，３人の組を１つ作ります．

  　中学校の役が２人と予備校の役が１人

- Linux(Ubuntu)デスクトップ環境を用いて，中学校の役と予備校の役が各自のPCでプログラムを作成し，通信を含むPPDMプログラムを完成します．



作成するプログラム

- ２つのプログラムをJava言語で作成します．
  １つ目は各自で作成し，２つ目はペアで作成します．

1. プライバシーを考慮しない非PPDMプログラム（各自で作成）
   生徒の成績（成績行列）と予備校の裏情報（重み行列）を
   両方知っているという前提で，
   行列の積によって，適性行列と合否行列を直接計算
   これはペアではなく，各自が作成します．

2. PPDMプログラム（ペアで作成）
   前ページのPPDMプログラムをペアで作成
   計算結果の適性行列，合否行列が非PPDMプログラムと
   一致することを確認してください．

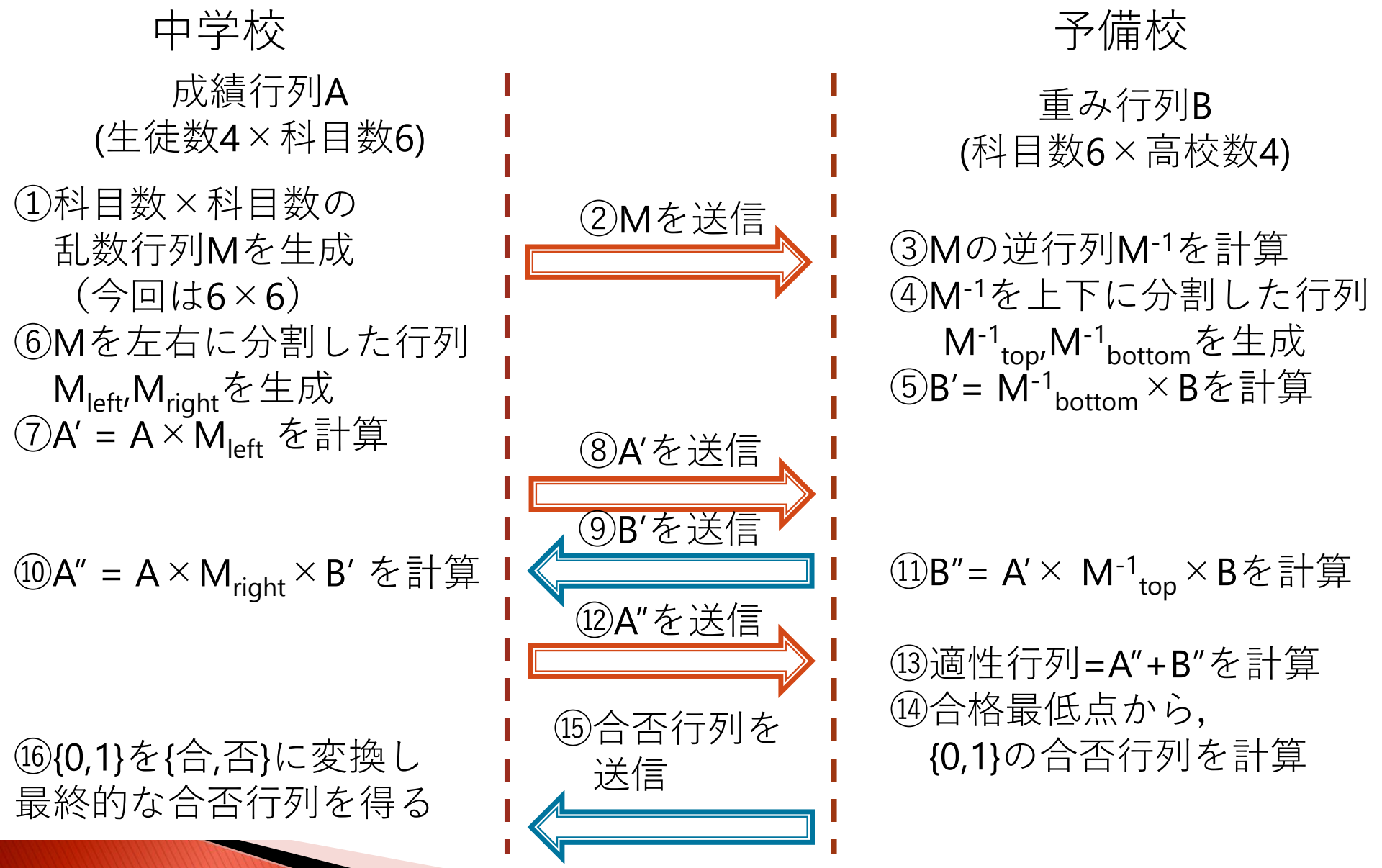
課題の提出と評価について

- 課題の提出
  - プログラム
  - レポート
    作成したプログラムの解説，ペアでの役割分担や考察
  - 詳細は３週目に説明します．
- 評価方法

出席点，プログラム，レポート

アルゴリズムの説明

アルゴリズムの流れ


中学校
予備校
成績行列A
(生徒数4×科目数6)
重み行列B
(科目数6×高校数4)
①科目数×科目数の
乱数行列Mを生成
（今回は6×6）
②Mを送信
③Mの逆行列M^{-1}を計算
④M^{-1}を上下に分割した行列
M^{-1}_{top},M^{-1}_{bottom}を生成
⑤B′= M^{-1}_{bottom}×Bを計算
⑥Mを左右に分割した行列
M_{left},M_{right}を生成
⑦A′ = A×M_{left} を計算
⑧A′を送信
⑨B′を送信
⑩A″ = A×M_{right}×B′ を計算
⑪B″= A′× M^{-1}_{top}×Bを計算
⑫A″を送信
⑬適性行列=A″+B″を計算
⑭合格最低点から,
{0,1}の合否行列を計算
⑮合否行列を
送信
⑯{0,1}を{合,否}に変換し
最終的な合否行列を得る

- 簡単な例として,

  中学校の成績行列が生徒数2と科目数2,
  予備校の重み行列が科目数2と高校数2

  の場合のアルゴリズムの流れを説明します.

中学校

80	70
60	40

成績行列A

予備校

0.8	1.2
1.1	0.9

重み行列B

中学校

80	70
60	40

成績行列A

2.0	1.0
5.0	3.0

乱数行列 M を生成

予備校

0.8	1.2
1.1	0.9

重み行列B

中学校

80	70
60	40

成績行列A

2.0	1.0
5.0	3.0

乱数行列 M を生成

Mを送信

予備校

3.0	-1.0
-5.0	2.0

逆行列 M^{-1} を計算

0.8	1.2
1.1	0.9

重み行列B

中学校

80	70
60	40

成績行列A

2.0	1.0
5.0	3.0

乱数行列 M を生成

Mを送信

予備校

3.0	-1.0
-5.0	2.0

逆行列 M^{-1} を計算

0.8	1.2
1.1	0.9

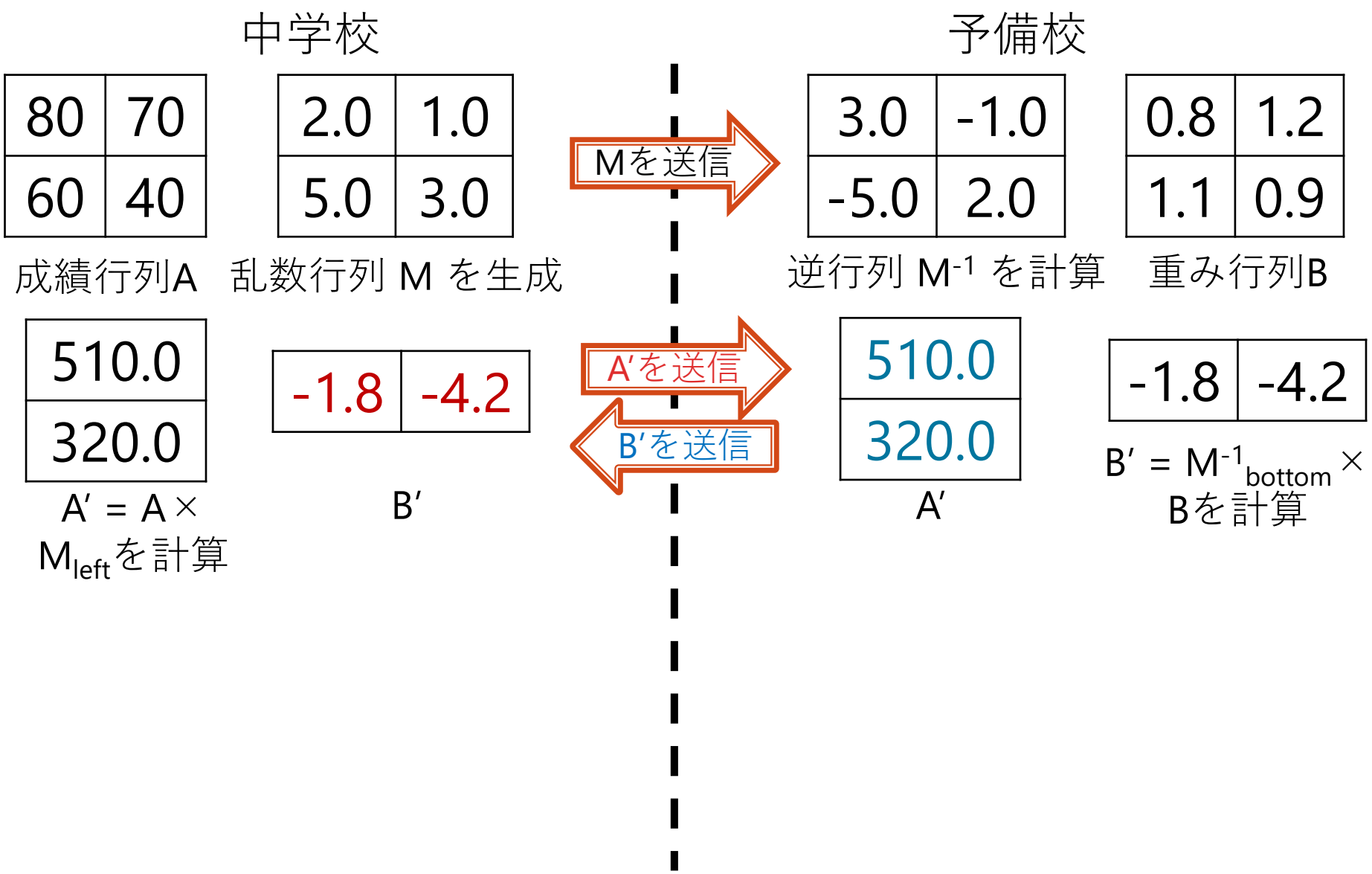
重み行列B

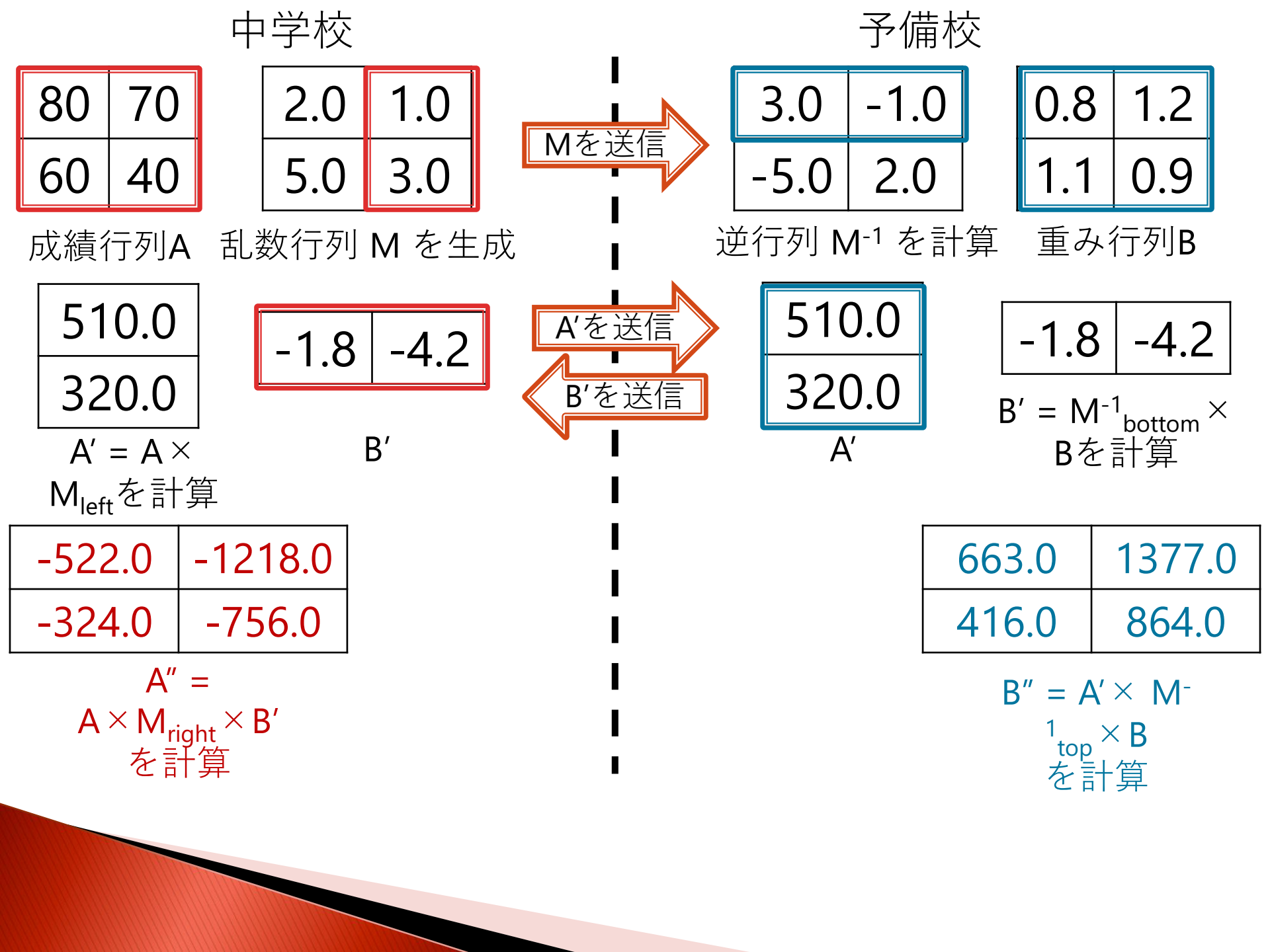
510.0
320.0

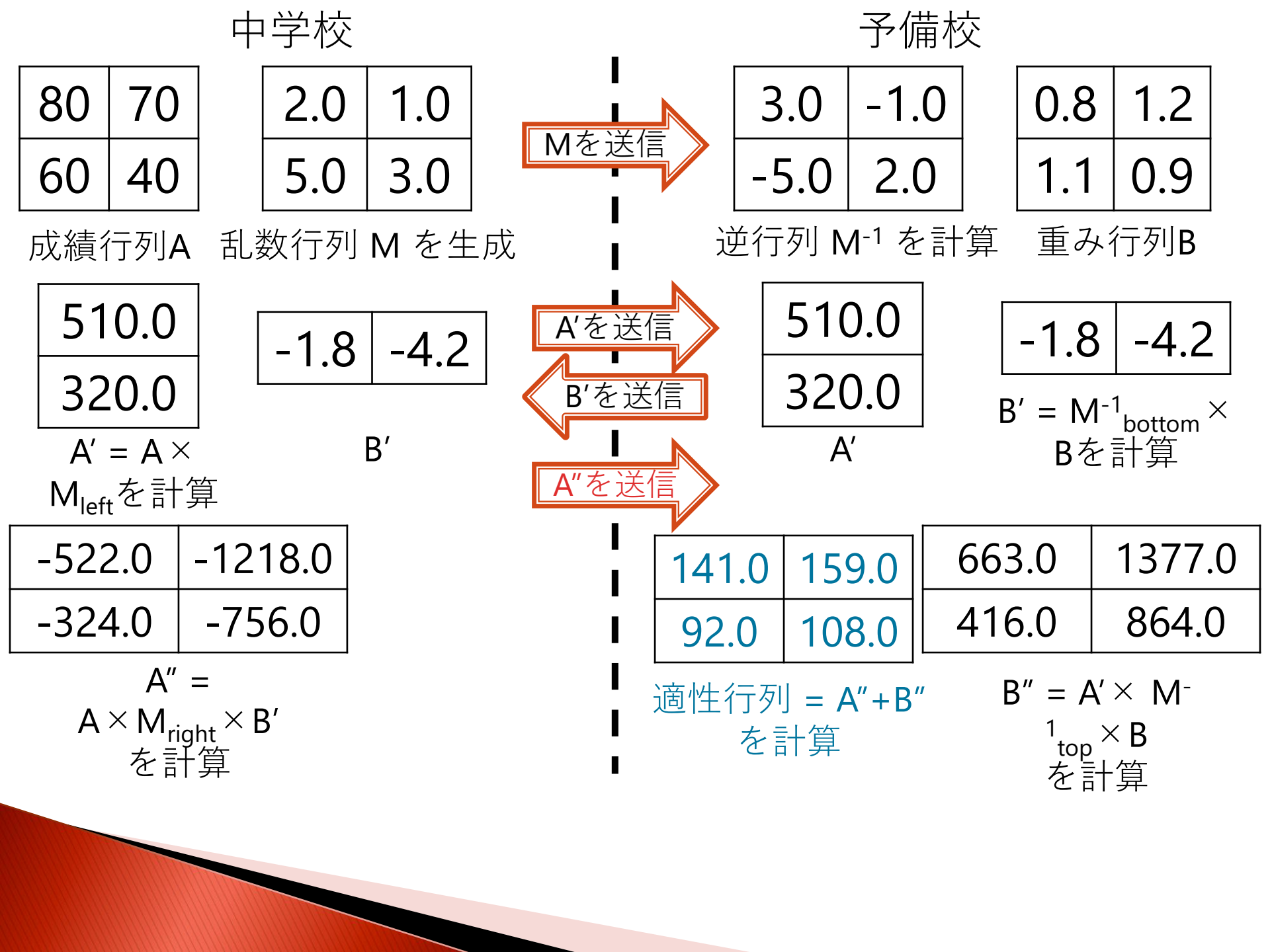
$A' = A \times M_{left}$を計算

-1.8	-4.2

$B' = M^{-1}_{bottom} \times$ Bを計算


中学校
予備校
80 70
60 40
成績行列A
2.0 1.0
5.0 3.0
乱数行列 M を生成
Mを送信
3.0 -1.0
-5.0 2.0
逆行列 M-1 を計算
0.8 1.2
1.1 0.9
重み行列B
510.0
320.0
A′ = A × Mleftを計算
-1.8 -4.2
B′
A′を送信
B′を送信
510.0
320.0
A′
-1.8 -4.2
B′ = M-1bottom × Bを計算


中学校
予備校
80 70
60 40
成績行列A
2.0 1.0
5.0 3.0
乱数行列 M を生成
Mを送信
3.0 -1.0
-5.0 2.0
逆行列 M-1 を計算
0.8 1.2
1.1 0.9
重み行列B
510.0
320.0
A′ = A × Mleftを計算
-1.8 -4.2
B′
A′を送信
B′を送信
510.0
320.0
A′
-1.8 -4.2
B′ = M-1bottom × Bを計算
-522.0 -1218.0
-324.0 -756.0
A″ = A × Mright × B′ を計算
663.0 1377.0
416.0 864.0
B″ = A′ × M-1top × B を計算


中学校
予備校
80 70
60 40
成績行列A
2.0 1.0
5.0 3.0
乱数行列 M を生成
Mを送信
3.0 -1.0
-5.0 2.0
逆行列 M-1 を計算
0.8 1.2
1.1 0.9
重み行列B
510.0
320.0
A′ = A × Mleftを計算
-1.8 -4.2
B′
A′を送信
B′を送信
510.0
320.0
A′
-1.8 -4.2
B′ = M-1bottom × Bを計算
A″を送信
-522.0 -1218.0
-324.0 -756.0
A″ = A × Mright × B′ を計算
141.0 159.0
92.0 108.0
適性行列 = A″+B″ を計算
663.0 1377.0
416.0 864.0
B″ = A′ × M-1top × B を計算

中学校

80	70
60	40

成績行列A

2.0	1.0
5.0	3.0

乱数行列 M を生成

Mを送信

予備校

3.0	-1.0
-5.0	2.0

逆行列 M^{-1} を計算

0.8	1.2
1.1	0.9

重み行列B

510.0
320.0

$A' = A \times M_{left}$ を計算

-1.8	-4.2

B′

A′を送信

B′を送信

510.0
320.0

A′

-1.8	-4.2

$B' = M^{-1}_{bottom} \times$ Bを計算

-522.0	-1218.0
-324.0	-756.0

$A'' = A \times M_{right} \times B'$ を計算

A″を送信

141.0	159.0
92.0	108.0

適性行列 = A″+B″ を計算

663.0	1377.0
416.0	864.0

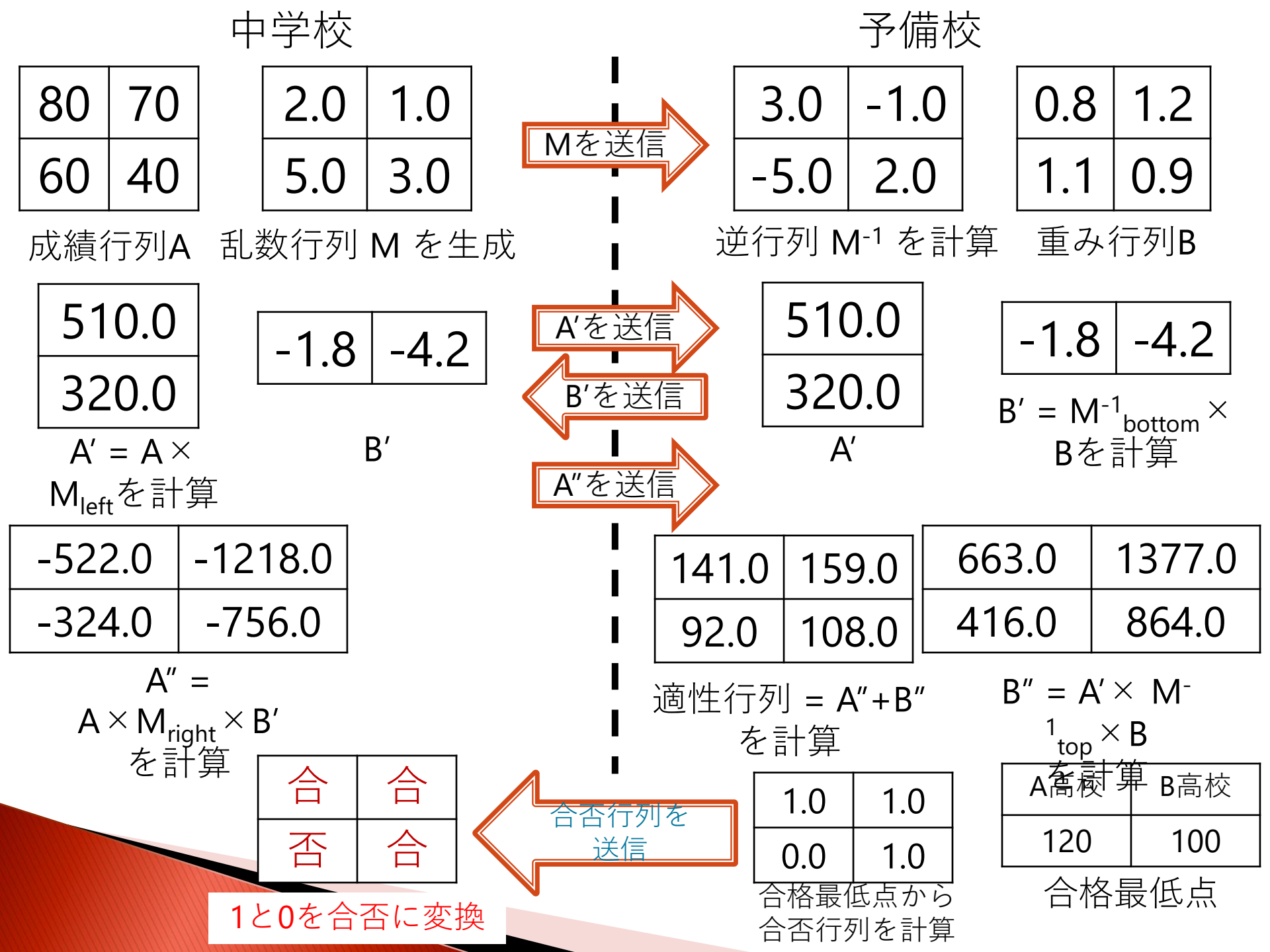
$B'' = A' \times M^{-1}_{top} \times B$ を計算

1.0	1.0
0.0	1.0

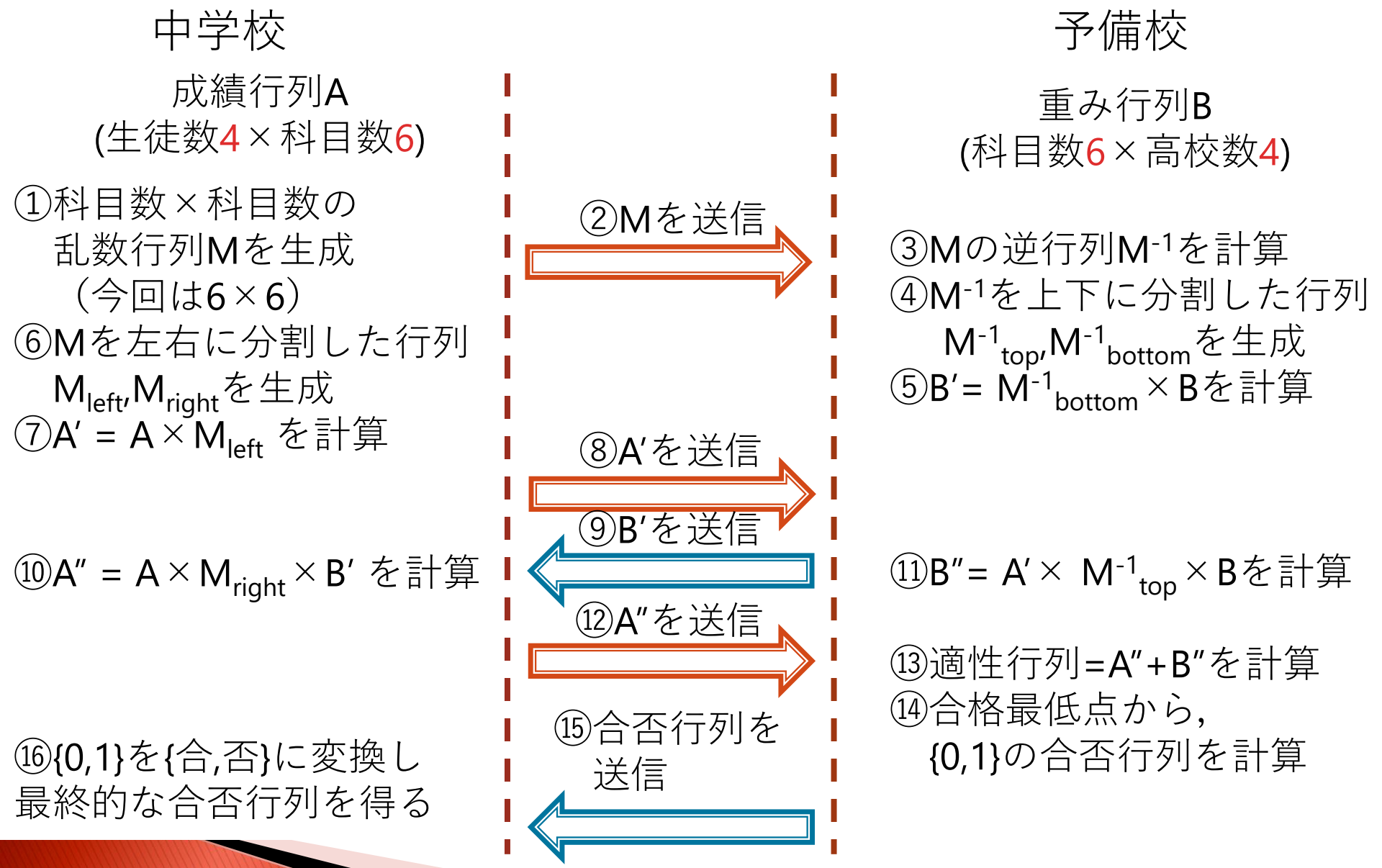
合格最低点から合否行列を計算

A高校	B高校
120	100

合格最低点


中学校
予備校
80 70
60 40
成績行列A
2.0 1.0
5.0 3.0
乱数行列 M を生成
Mを送信
3.0 -1.0
-5.0 2.0
逆行列 M-1 を計算
0.8 1.2
1.1 0.9
重み行列B
510.0
320.0
A′ = A × Mleftを計算
-1.8 -4.2
B′
A′を送信
B′を送信
510.0
320.0
A′
-1.8 -4.2
B′ = M-1bottom × Bを計算
A″を送信
-522.0 -1218.0
-324.0 -756.0
A″ = A × Mright × B′ を計算
141.0 159.0
92.0 108.0
適性行列 = A″+B″ を計算
663.0 1377.0
416.0 864.0
B″ = A′ × M-1top × Bを計算
合 合
否 合
1と0を合否に変換
合否行列を送信
1.0 1.0
0.0 1.0
合格最低点から合否行列を計算
A高校 B高校
120 100
合格最低点

アルゴリズムの流れ


中学校
予備校
成績行列A
(生徒数4×科目数6)
重み行列B
(科目数6×高校数4)
①科目数×科目数の
乱数行列Mを生成
（今回は6×6）
②Mを送信
③Mの逆行列M^{-1}を計算
④M^{-1}を上下に分割した行列
M^{-1}_{top},M^{-1}_{bottom}を生成
⑤B′= M^{-1}_{bottom}×Bを計算
⑥Mを左右に分割した行列
M_{left},M_{right}を生成
⑦A′ = A×M_{left} を計算
⑧A′を送信
⑨B′を送信
⑩A″ = A×M_{right}×B′ を計算
⑪B″= A′× M^{-1}_{top}×Bを計算
⑫A″を送信
⑬適性行列=A″+B″を計算
⑭合格最低点から,
{0,1}の合否行列を計算
⑮合否行列を
送信
⑯{0,1}を{合,否}に変換し
最終的な合否行列を得る

週毎の課題の説明

速い人は翌週の課題を進めてください

1週目

1．非PPDMプログラム

＜入出力＞

- 入力：成績行列，重み行列，合格最低点
- 出力：適性行列，合否行列

いずれもtxtファイル

＜処理＞

1. 成績行列，重み行列，合格最低点を読み込む
2. 成績行列と重み行列の積により，適性行列を計算
3. 合格最低点との比較により，合否行列を計算
4. 適性行列，合否行列を出力

＜注意＞

- 行列の値は，double型の二次元配列として定義してください.
- IEDのPC(Ubuntu)環境上で作成，実行してください.
- ※Windowsではなく，Ubuntuで作成してください

１週目（続き）

２．PPDMプログラム

- 非PPDMプログラムを再利用しながら，PPDMアルゴリズムを実装
- １週目，２週目は，中学校役と予備校役に分かれて
  通信以外の部品を作成してください．
- ３週目は，両方のプログラムを通信でつなぎます．

＜入出力＞

- 入力　　中学　　：成績行列
  予備校　：重み行列，合格最低点
- 出力　　中学　　：合否行列
  予備校　：適性行列　　いずれもtxtファイル

＜処理＞

非PPDMプログラムとPPDMアルゴリズムを参考に自分で考えること

＜注意＞

- 行列の値は，double型 の２次元配列を使用してください．

２週目

PPDMプログラム(余力のある人は先に着手して構いません)

- 非PPDMプログラムを再利用しながら，PPDMアルゴリズムを実装
- １週目，２週目は，中学校役と予備校役に分かれて通信以外の部品を作成してください.
- ３週目は，両方のプログラムを通信でつなぎます.

１週目に引き続いて，通信以外の部品を作成してください.

３週目

PPDMプログラム

- 非PPDMプログラムを再利用しながら，PPDMアルゴリズムを実装
- １週目，２週目は，中学校役と予備校役に分かれて通信以外の部品を作成してください.
- **３週目は，両方のプログラムを通信でつなぎます.**

通信プログラムは難しいので,
TAの作成したプログラムを利用してください.

参考情報

- Javaの基本的なコマンド
  - 実行
    パッケージ上位のディレクトリに移動し,
    java [パッケージ名]/[クラスファイル名]
    (例 java contentssecurity/Main)

  - コンパイル
    パッケージ上位のディレクトリに移動し,
    javac [パッケージ名]/[ソースファイル名].java
    (例 contentssecurityパッケージのMain.javaファイルを
    　　コンパイルする場合,
    javac contentssecurity/Main.java)

参考情報

- UNIXの基本的なコマンド
  - cd　　：ディレクトリの移動
  - scp –r　：ファイル・ディレクトリのコピー

  （例　scp –r programs root@linuxXX:[保存パス]
  - mkdir　：フォルダの新規作成
  - passwd　：パスワードの変更
  - ls　　：ファイルやディレクトリの情報を表示
  - pwd　　：現在のディレクトリの場所を絶対パスで表示

参考情報

- ファイル入力（一例）

FileInputStream fis = new FileInputStream(“FILEPATH”);

InputStreamReader isr = new InputStreamReader((fis),”UTF-8”);

BufferedReader br = new BufferedReader(isr);

と書き,

String input = br.readLine();

とするとinputに一行目のテキストが読み込まれるので,

“ , ”で区切り，double型に変換すれば良いです.

※）区切り方

Stringクラスの，splitメソッドを参照.

※）FILEPATHについて

(“./contentssecurity/seiseki.txt”)など.

参考情報

- 乱数生成：Javaのライブラリーを使用
- 逆行列の計算方法：掃き出し法以外にも，
  ヤコビ法，ガウス・ジョルダン法等があります．

- Javaの書き方やUNIXのコマンド，emacsについて……
  ：外部サイトを参照

  ※）岩本・渡邉研究室WEBサイトの
  コンテンツセキュリティ実験のページにも，
  外部サイトへのリンクがあります．

通信プログラムの説明（詳細は２日目以降に説明します）

package contentssecurity

Connector class

- double[][] getTable()
  引数：なし
  返値：double[][]
  テーブルを受け取るメソッド
- void sendTable(double[][])
  引数：double[][]
  返値：なし
  テーブルを送るメソッド

作成手順

1. 岩本・渡邉研究室WEBサイト※ > 講義関係 > コンテンツセキュリティ実験のページにアクセスし，ファイルをダウンロード
   ※「岩本・渡邉研究室」でWeb検索して下さい.
2. Main.javaファイルに記述
3. 各プログラムを作成した後，３日目にLinux仮想マシンにアップロードし実行.

注意事項

- Javaファイル(Main.java)のコンパイル・実行手順

1. Main.javaがある階層の上位の階層に移動
   例: kadai〇/contentssecurity/Main.javaの場合,
   kadai〇 に移動
2. Main.javaをコンパイル
   コマンド:　javac contentssecurity/Main.java
3. Main.javaを実行
   コマンド:　java contentssecurity/Main

Linux 参考情報

- 仮想環境へのログイン

1. スタートメニューから端末エミュレータを起動
2. ssh root@linux○○　と入力
   ※○○はマシン番号
3. パスワードを入力（初期パスワード：linux○○）

- 仮想環境にファイル・ディレクトリをコピー

1. スタートメニューから端末エミュレータを起動
2. scp –r [コピー元] root@linux○○:[コピー先]　と入力
   ※○○はマシン番号
3. パスワードを入力

- エディタやライブラリの使用，ペアの役割分担などは自由に行って下さい．
  - ただし，最終レポートにその旨を記載すること．

- 授業時間外で質問がある方は，下記のアドレスへ連絡を下さい．

  csec_exp2021@oslab.inf.uec.ac.jp