M1 Informatique
Premiers pas en NachOS

Vincent Danjean, Guillaume Huard, Arnaud Legrand,
Vania Marangozova-Martin, Jean-François Méhaut

Année 2010/2011

Résumé

Les objectifs de cette première étape sont la découverte du simulateur NachOS à travers la lecture du code source, le tracage d'éxécution grâce aux options de débogage et à gdb. En plus du démarrage du simulateur, nous observerons l'exécution d'un programme utilisateur qui donnera un exemple d'appel système, puis la commutation et l'ordonnancement des threads noyaux.

1 Machine de travail

Si vous travaillez sur les machines de l'UFR IMAG, vous devez impérativement vous connecter sur le serveur **mandelbrot.e.ujf-grenoble.fr**. Sur cette machine ont été installés le cross-compilateur et les différents outils nécessaires pour le travail sur NachOS.

Si vous disposez de votre machine personnelle (portable ou fixe) sous Linux, vous devez générer et installer le cross-compilateur gcc pour le processeur MIPS. Pour cela, récupérer le fichier **cross.tar.gz** disponible dans le Moodle ou sous /u/m/marangov/PUBLIC/NACHOS/. Cette archive contient un fichier vous expliquant comment installer le cross-compilateur. Vous devez également vérifier que le compilateur gcc en version 3.3 ou 3.4 est installée. Si vous utilisez une installation Debian ou Ubuntu), vous pouvez le récupérer avec la commande apt-get install gcc-3.3.

En cas de probléme, vous pouvez contacter les enseignants par mail pour expliquer précisément les difficultés que vous rencontrez.

2 Test de NachOS

Vous pouvez récupérer le code source de NachOS dans le Moodle ou dans /u/m/marangov/PUBLIC/NACHOS.

Positionnez-vous ensuite sous `nachos/code` et construisez les différents exécutables NachOS :

```
cd nachos/code

make clean      # Pour se remettre dans un état standard (prudent!)

make            # Pour produire les fichiers de dépendances
```

```
# et lancer la compilation (cela peut être long...)
```

Normalement, tout doit bien se passer... Pendant cette compilation vous pouvez lire les conseils ci-dessous et commencer la partie suivante qui debute par une lecture du code.

Il vous suffit maintenant de lancer les tests. Nous reviendrons sur la signification de ces tests plus tard, rassurez-vous. Il s'agit juste de voir si tout est en ordre...

```
cd threads
./nachos
```

pour le premier, et pour le second

```
cd userprog
./nachos -x ../test/halt
```

Si les affichages produits par ces deux tests ne comportent rien de suspect, alors tout devrait être valide.

3 Lecture du code source de NachOS

3.1 Principes de la simulation

Dans un systéme réel monoprocesseur, il existe au moins deux modes d'utilisation du processeur :

- le **mode utilisateur** (*user mode*) dans lequel il exécute les instructions d'un programme utilisateur ;
- le **mode noyau** (*kernel mode*) dans lequel il organise les différentes têches systémes qui lui sont demandées : communication avec les périphériques (disque-dur, clavier, carte graphique ...), gestion des ressources (mémoire (swap, allocation), processeur (ordonnancement des processus)), ...

Dans la réalité le systéme exécute alternativement du mode noyau et le mode utilisateur de la même façon sur un processeur.

Dans le cas du simulateur NachOS le fonctionnement est différent : il vous faut bien distinguer ce qui est simulé de ce qui est réellement exécuté. Compilé en assembleur x86, le mode systéme est exécuté sur le processeur réel (i386 et affidés).

En revanche, les programmes de niveau utilisateur sont compilés en assembleur MIPS et émulés par un simulateur de processeur MIPS. Ce simulateur étant un programme comme un autre, il est donc exécuté sur le processeur réel (i386) de la machine sur laquelle vous travaillez.

Le programme NachOS est un exécutable comme les autres sur votre machine réelle qui dispose de temps ê autre du processeur réel (i386) pour exécuter des instructions en mode noyau ou bien pour simuler divers éléments matériels comme un processeur MIPS (pour l'exécution des programmes utilisateur en mode utilisateur), une console pour les entrée/sorties clavier ou écran, un disque-dur ...

Pour les distinguer rapidement on appelle *mémoire réelle* la mémoire du processus (espace d'adressage) dans lequel est exécuté NachOS et *mémoire MIPS* la mémoire simulée associée au processeur MIPS simulé. On fera la même chose pour le processeur réel et le processeur MIPS qui est simulé.

Pour rattacher ce discours général ê la réalité, on se propose de lire dans le code source, l'exécution de la commande

```
nachos -x ../test/halt
```

`nachos` ayant été compilé avec le seul "drapeau" (flag) `USER_PROG`.
Le comportement de cette commande est d'initialiser le systéme `nachos` et d'exécuter le programme utilisateur MIPS `../test/halt` qui demande l'arrêt du systéme.

Avant de lire le code vous pouvez (devez) consulter l'annexe sur l'utilisation des tags qui peut vous faciliter grandement la vie !

3.2 Initialisation du systéme

Comme tout processus, l'exécutable NachOS dispose de mémoire réelle (espace d'adressage) subdivisée en zones de code, tas et pile. Le point d'entrée de ce programme est naturellement la fonction `main` du fichier `threads/main.cc`. Le premier objectif de cette partie est d'observer commment un exécutable usuel se "transforme " en un systéme d'exploitation sur lequel il existe un unique thread noyau.
Le second objectif (plus délicat) est de distinguer ce qui correspond ê une exécution réelle en mode systéme de ce qui correspond ê unesimulation de matériel (le processeur MIPS, le disque dur ...).

Allocation du simulateur Le schéma suivant représente les ressources du processus NachOS et les éléments du systéme qui sont initialisés ê la fin de la fonction `Initialize()`. Ces éléments sont créés par l'opérateur C++ `new` qui est l'"équivalent" du `malloc` en C.
Indiquez sur le schéma le nom des classes C++ qui codent ces éléments. Précisez dans quelle mesure ces éléments appartiennent au mode noyau ou à la simulation de matériel.

Le premier thread noyau On s'intéresse à la création du premier thread noyau. Pour répondre aux questions, nous vous conseillons aussi la lecture des fichiers `threads/thread.h` et `threads/thread.cc`. Comment est créé ce premier thread noyau ê C'est ê dire d'oê viennent sa pile et ses registres ê Quel est le rôle (futur) de la structure de données allouée par

```
currentThread = new Thread("main");
```

Les prochains threads noyaux pourront-ils être créés de la même façon ê

3.3 Exécution d'un programme utilisateur

Le processeur MIPS Repérez dans le code de la fonction `Initialize()` l'allocation du processeur MIPS et lisez le code d'initialisation de cet objet pour répondre aux questions suivantes : Comment sont initialisés les registres de ce processeur ? Quelle variable représente la mémoire MIPS ?

Revenez ê la fonction `main()` et vérifiez que la fonction `StartProcess()` est appelée avec le nom du fichier `../test/halt`. Survolez le code de cette fonction pour y reconnaitre le chargement du programme en mémoire (simulée ou réelle ê), l'initialisation des registres du processeur MIPS et surtout le lancement de l'exécution du processeur MIPS par la fonction `Machine::Run`.

Lisez le code de la fonction `Machine::Run`, repérez la fonction qui exécute une instruction MIPS. L'observation de cette fonction vous permet de connaitre le nom de l'exception levée lorsqu'une addition (instruction assembleur `OP_ADD`) déborde (même si cela ne s'avére pas crucial

pour la suite). Observez la fin de cette fonction pour trouver le registre contenant le compteur de programme.

L'appel systéme Halt Une fois dans la fonction `Machine::Run` la simulation d'un programme utilisateur ne peut être interrompue que de deux façons : soit une interruption est déclenchée (cf la fonction `Interrupt::OneTick()`), soit le programme utilisateur fait un appel systéme.

On se propose d'observer la fin du déroulement de l'appel systéme `Halt()` présent ê la fin du programme `../test/halt.c`. L'instruction assembleur codant un appel systéme dans `OneInstruction()` est `OP_SYSCALL`. Observer le traitement de cette instruction, notamment le moment oê le systéme reprend la main et le passage du numero de l'appel systéme (ici `SC_Halt`) par un registre (lequel ê) du processeur MIPS. Suivre le code jusqu'ê l'exécution de la fonction `CleanUp()` dont le rôle est de désallouer tout le simulateur.

4 Utilisation du systéme NachOS

4.1 Observation de l'exécution d'un programme utilisateur

Déplacez-vous sous le répertoire `test`, et regardez le programme `halt.c`. Faire `make halt` pour le compiler.

Placez-vous ensuite sous `userprog`. Lancez

```
./nachos -x ../test/halt
```

Les programmes utilisateurs sont écrits en `C`, compilés en binaires MIPS qui sont chargés et exécutés par la machine Nachos, instruction par instruction.

Tracer pour comprendre Essayez de tracer l'exécution du programme `halt` :

```
./nachos -d m -x ../test/halt
./nachos -rs 0 -d m -x ../test/halt
```

Vous pouvez en plus exécuter le simulateur MIPS pas ê pas :

```
./nachos -s -d m -x ../test/halt
```

Modifiez le programme `halt.c` pour y introduire un peu de calcul, par exemple en faisant quelques opérations sur une variable entiére. Tracez pas ê pas pour bien voir que cela change quelque chose...

N'oubliez pas que dans ce monde MIPS, vous n'avez ê votre disposition que les fonctions du langage `C` et les appels systémes de NachOS. Aucune fonction de bibliothéque (`printf`, ...) n'est disponible !

Il est aussi possible de générer facilement la version assembleur d'un programme MIPS. Commencez par détruire le fichiers `halt.o` et faites `make`. Récupérez la ligne de commande produite par copier-coller, qui doit ressembler ê :

```
/opt/NACHOS/nachos_gcc/cross/decstation-ultrix/bin/gcc -c \
-I../userprog -I../threads -G 0 -c halt.c
```

Changez le `-c` final en `-S`. Cela va produire le code assembleur MIPS de `halt` dans le fichier `halt.s`. Exécutez de nouveau `halt` pas ê pas en suivant maintenant les instructions code assembleur !

Repérez les instructions assembleur codant les calculs et l'appel ê la fonction `Halt`. On peut trouver le code de cette fonction `Halt` dans le fichier `test/start.c` ce qui permet de faire le lien avec l'étude de la fin de l'appel systéme dans le partie précédente.

(Question facultative) Pourquoi la premiere instruction MIPS est elle éxécutée au dixiéme *tick* d'horloge ê (cf la fonction `Interrupt::OneTick()` et l'initialisation du systéme)

4.2 Observation des threads noyau

Nous allons tester le systéme NachOS "seul", c'est-ê-dire en configuration d'auto-test. En l'occurrence, ce test consiste ê lancer deux threads internes au noyau qui affichent tour ê tour une ligne ê l'écran pendant 5 itérations. Placez-vous dans le répertoire `threads`. Lancez NachOS :

```
./nachos
```

Les options de compilation de ce répertoire font que NachOS lance la fonction `ThreadTest` dans `main.cc` (allez jeter un œil !) Cette fonction est définie dans `threadtest.cc`. Examinez attentivement sa définition.

NachOS dispose d'options de déboggage. Essayez par exemple

```
./nachos -d +   # + = all possible options
```

Vous pouvez voir les *ticks* de l'horloge interne de NachOS, les commutation entre threads, la gestion des interruptions, etc. Il est possible de n'afficher qu'une partie de ces informations.

Au lieu du `+`, on peut mettre :

`t` pour ce qui a trait aux threads systeme NachOS,

`a` pour ce qui a trait ê la mémoire MIPS,

`m` pour ce qui a trait ê la machine NachOS,

`t` pour ce qui a trait ê la gestion des threads,

`i` pour ce qui a trait aux interruptions,

`n` pour ce qui a trait au réseau NachOS,

`f` pour ce qui a trait au filesystem NachOS,

`d` pour ce qui a trait aux disques NachOS.

Certaines parties de NachOS (disques, ...) ne sont pas manipulées pour l'instant. Le flag correspondant n'affichera alors aucun message supplémentaire.

Allons maintenant éditer le fichier `threadtest.cc`. Compilez, lancez l'exécution en régle, observez attentivement...

Ajoutez le lancement d'un thread supplémentaire dans la fonction `ThreadTest()`. Il marche toujours ?

La sémantique de la méthode `fork` de l'objet `thread` n'a rien ê voir avec celle de la fonction Unix `fork`. Que fait la méthode `fork` dans NachOS ê À quel moment les threads nachos sont-ils créés (mémoire allouée, structures initialisées, ...) ê

Maintenant, commentez la ligne suivante :

```
currentThread->Yield();
```

Recompilez (`make`) et examinez ce qui se passe. Qu'en déduisez-vous pour la préemption des threads systémes par défautê

Restaurez cette ligne. On peut lancer NachOS en forçant un certain degré de préemption par l'option `-rs <n>`. De plus, la semence passée en paramétre rend aléatoire (mais *reproductible* !) l'entrelacement des threads (le nombre `n` n'a pas de signification particuliére, autre qu'être celui servant ê initialiser le générateur aléatoire).

```
./nachos -rs 0
./nachos -rs 1
./nachos -rs 7
```

Que se passe-t-ilê Couplez cela avec l'option `-d +`. Combien de ticks d'horloge maintenant ?

Ce point est assez difficile ê comprendre. Vérifiez votre intuition en commentant la ligne :

```
currentThread->Yield();
```

Vos conclusions ?

4.3 Découverte de l'ordonnanceur

L'objectif est maintenant de comprendre une partie du fonctionnement de l'ordonnanceur en s'appuyant sur l'expérience précédente.

Le changement de contexte explicite Que se passe-t-il exactement lors d'un appel ê la fonction `Yield()` ? Allez inspecter le source de cette fonction dans le fichier `code/thread/thread.cc`. A quel moment un thread ressort-il de cette fonction ?

La classe Scheduler Examinez les méthodes de la classe `Scheduler` appelées par la fonction `Yield()`. Quels sont les rêles respectifs des fonctions `ReadyToRun()`, `FindNextToRun()` et `Run()` ?

Au cœur du changement de contexte Dans quelle fonction de la classe `Scheduler` trouve-t-on la véritable instruction provoquant un changement de contexte (i.e. une commutation) entre deux processus ê Trouvez le source de la fonction de bas niveau correspondante. Que fait-elle ?

4.4 Exécution de NachOS pas ê pas

Dans les situations extrêmes, il vous sera toujours possible de suivre l'exécution de NachOS réellement pas ê pas, en utilisant un deboggeur tel que `gdb`. Par défaut, NachOS est d'ailleurs compilé avec l'option `-g` (voir les `Makefile`).

Retournez dans le répertoire `threads` et lancer NachOS sous le contrêle du deboggeur `gdb`.

```
gdb nachos
[...]
(gdb) break main
Breakpoint 1 at 0x804d6fa: file main.cc, line 84.
(gdb) run
Starting program: nachos  [...]
Breakpoint 1, main (argc=1, argv=0x8046db0) at main.cc:84
84          DEBUG('t', "Entering main");
(gdb)
```

Vous pouvez progresser avec les commandes `s` (atomic *step*), `n` (*next* instruction in the current fonction), `c` (*continue* jusqu'au prochain *breakpoint*), `r` (*run* : (re)démarre l'exécution du progamme), etc.

Essayez surtout :

```
(gdb) break ThreadTest
[...]
(gdb) cont
[...]
```

Ceci place un point d'arrêt sur la fonction `ThreadTest`, puis dit à NachOS de continuer son exécution jusqu'ê ce qu'il arrive sur un point d'arrêt.

Modifiez la fonction `SimpleThread()`, recompilez, relancez, réfléchissez, etc.

Exécutez `SimpleThread()` pas ê pas. Que se passe-t-il quand on appuie sur `n` (*next*) lorsque gdb est prêt ê exécuter la méthode `yield` ê Comment peut-on placer un point d'arrêt pour reprendre la main dans gdb chaque fois qu'un changement de contexte est exécuté par NachOS ê

4.5 Exercice

Modifiez la méthode `yield` pour qu'elle ne fasse de changement de contexte qu'une fois tous les deux appels.

Relancez le programmes NachOS dans le répertoire `thread` et observez le déroulement (avec l'option `-d` de NachOS et/ou avec `gdb`).

Nous allons maintenant tester les threads systémes NachOS, c'est-ê-dire les threads de niveau *noyau*. Placez-vous dans le répertoire `threads`. Lancez NachOS :

```
./nachos
```

Les options de compilation de ce répertoire font que maintenant NachOS lance la fonction `ThreadTest` dans `main.cc`. Cette fonction est définie dans `threadtest.cc`. Examinez attentivement sa définition.

Éditez maintenant le fichier `threadtest.cc`. Compilez, lancez l'exécution en régle, observez attentivement...

Ajoutez le lancement d'un autre thread dans la fonction `ThreadTest()`. Cela marche t-il toujours ê

Maintenant, "commentez-hors" la ligne

```
currentThread->Yield();
```

Recompilez (`make`) et examinez ce qui se passe. Qu'en déduisez-vous pour la préemption des threads systémes par défautê

Restaurez cette ligne. On peut lancer NachOS en forçant un certain degré de préemption par l'option `-rs <n>`. De plus, la semence passée en paramétre rend aléatoire (mais *reproductible* !) l'entrelacement des threads.

```
./nachos -rs 5
./nachos -rs 1
```

- que se passe-t-il ê
- couplez cela avec l'option `-d +`. Combien de ticks d'horloge dans chacun des cas ê

- quel matériel supplémentaire est utilisé ê
- vérifiez votre intuition en “commentant-hors” la ligne
  `currentThread->Yield();`
- vos conclusions ?

On peut aussi tracer NachOS au plus bas niveau en utilisant `gdb`. Par défaut, on compile avec l'option `-g` (voir les `Makefile`).

```
gdb nachos
[...]
(gdb) break main
Breakpoint 1 at 0x804d6fa: file main.cc, line 84.
(gdb) run
Starting program: nachos  [...]
Breakpoint 1, main (argc=1, argv=0x8046db0) at main.cc:84
84          DEBUG('t', "Entering main");
(gdb)
```

Vous pouvez progresser avec les commandes `s` (atomic *step*), `n` (*next* instruction in the current fonction), `c` (*continue*), etc.

Essayez aussi

```
break ThreadTest
```

Modifiez la fonction `SimpleThread()`, recompilez, relancez, réfléchissez, etc.

Annexe : Outils pour la lecture du code

Le code de NachOS est réparti dans de nombreux fichiers et lors de sa lecture on est amené ê sauter de fichier en fichier. Les *tags* (“étiquettes” en francais), permettent de trouver automatiquement la définition d'une fonction ê partir d'un endroit où elle est appelée.

Pour cela il faut dans un premier temps construire un dictionnaire référençant les définitions des fonctions. Ce dictionnaire différe selon l'éditeur utilisé. Ce sont les programmes `etags` pour emacs et `ctags` pour vim qui construisent un tel dictionnaire et le stockent dans un fichier (`TAGS` pour emacs et `tags` pour vim).

Ensuite l'éditeur que vous utilisez va lire dans ce fichier (quand il l'a trouvé) la position de la définition d'une fonction et saura ouvrir le fichier correspondant.

Mise en œuvre pratique pour l'éditeur `vim`

Construction du dictionnaire

Les premiéres versions de `ctags` traitaient principalement les fichiers C. Comme NachOS est écrit en C++ il faut une version relativement récente qui prenne en compte les classes. Une telle version est installée dans `/u/HOME/m/mehautj/ctags-5.7` sur mandelbrot, pour l'utiliser taper :

```
cat >> .bashrc
alias ctags='/u/HOME/m/mehautj/ctags-5.7/ctags'
C^D # Control-D  source .bashrc
```

Pour créer le dictionnaire des fonctions de NachOS taper :

```
cd Mon_Nachos/nachos/code
ctags */*.cc */*.c
```

et vous devez voir apparaêtre un fichier `tags` dans le répertoire courant (ici `Mon_Nachos/nachos/code`).

Lecture du code

On va utiliser ce dictionnaire pour lire le code de NachOS ê l'aide de l'éditeur `vim`. Pour éviter des écritures accidentelles on l'utilisera en lecture uniquement (cf l'option -R).

```
vim -R
```

Cet éditeur fonctionne selon deux modes : le mode insertion oê l'on peut modifier le contenu du fichier et le mode commande oê l'on réalise par exemple les ouvertures et fermetures de fichiers (á comparer á ce que l'on tape dans la barre de commande de `emacs`). La lecture des sources s'effectue dans le mode commande. Pour y basculer il suffit d'appuyer sur la touche **Echap**.

Commandes élémentaires

Commande	**Résultat**
`Echap`	Passe en mode commande (y reste si déjê en mode commande).
`:help` *sujet*	Donne l'aide sur le *sujet* (exemple `:help tags`).
`:q!`	Force la sortie de l'éditeur sans sauvegarde.
`:new` *un_fichier*	Ouvre *un_fichier*
`:ts` *une_fonction*	Propose la liste des fonctions de nom *une_fonction* et va ê la définition choisie.
`:ta` *une_fonction*	Va ê la définition de la premiére fonction dans le dictionnaire de noms *une_fonction*
`:tags`	Affiche la pile des tags courants (similaire ê la pile des appels de fonctions).
`:pop`	Dépile le premier tag de la pile.

Par défaut `vim` cherche le dictionnaire dans le répertoire courant. C'est pourquoi il est conseillé de lancer `vim` dans le répertoire oê se trouve le dictionnaire. Sinon on peut donner le nom du dictionnaire ê lire par la commande

`:set tags=`*`repertoire/le_fichier_dictionnaire`*

Comme `emacs`, `vim` propose des raccourcis claviers pour les commandes les plus usuelles. Ainsi au lieu de la commande `:ta` *`une_fonction`* on pourra préférer positionner le curseur sur l'occurrence de *une_fonction* dans le code et taper `Ctrl-]`. De même, `:pop` admet `Ctrl-t` comme abréviation.

Mise en œuvre pratique pour l'éditeur `emacs`

Pour contruire le dictionnaire taper :

```
cd Mon_Nachos/nachos/code

etags */*.cc */*.c
```

Pour l'utiliser lancer `emacs` dans le même répertoire.

Pour chercher la définition d'une fonction, placer le curseur sur son nom et taper `Meta-.` (“Méta - point”). Pour revenir ê la définition précédente taper `Meta-*`.

Lors de la premiére recherche d'un tag, emacs demande le nom du fichier du dictionnaire, ici c'est `Mon_Nachos/nachos/code/TAGS`.

La commande `grep`

Si on cherche autre chose que la définition d'une fonction (par exemple un appel de cette fonction ou un nom de variable) la commande `grep` est utile.

```
cd Mon_Nachos/nachos/code

grep -r ‘‘currentThread’’ */*.cc */*.h */*.c
```

Cela affiche les lignes contenant la variable `currentThread` dans tous les fichiers sources.