

# 創造情報学専攻 専門科目 問4 対策

@SythonUK

2016 年 2 月 29 日

# 目次

1	既出問題	2
2	プログラミング	3
3	言語理論	3
4	データベース	4
5	ソフトウェア開発	4
6	多変量解析と人工知能	4
7	データ構造とアルゴリズム	5
8	コンピュータグラフィクス	5
9	コンピュータアーキテクチャ	6
10	暗号理論とセキュリティ	8
11	メカトロニクス	8
12	コンピュータネットワーク	9
13	情報通信理論	10
14	信号画像処理	10
15	制御工学	10

# 1 既出問題

- スーパースカラ
- 半加算器
- キャリー・ルック・ahead
- TLB
- パイプラインハザード
- マイクロプログラム制御
- スヌープキャッシュ
- アウトオブオーダー実行
- RISC と CISC
- プロセスとスレッド
- クロスサイトスクリプティング
- 公開鍵暗号
- PKI
- ユーザ認証 (個人識別) 法
- フィッシング
- 公開鍵のデジタル署名
- PWM 制御
- ステップ応答と伝達関数
- カルマンフィルタ
- フィードバック/フォワード制御
- $H^\infty$  制御
- サーボ系の位置とトルクフィードバック
- インパルス応答とステップ応答
- PID 制御
- 交流回路のインピーダンス
- 実行時コンパイラ
- クロージャ
- 有限オートマトン
- 末尾再帰
- LL(1) 構文解析
- 高階関数
- 関係データベースの正規化
- チューリングマシン
- リフレクション
- 参照透明性
- 正規文法と正規言語
- 関数型言語
- 自然言語の形態素
- 関係データベースの結合演算
- 文脈自由文法
- 論理型言語
- サポートベクターマシン
- tf-idf
- ベイジアンネットワーク
- ニューラルネットの学習
- 主成分分析
- ベイズの定理
- 決定木の学習
- 隠れマルコフモデル
- ベクトル量子化
- 意味ネットワーク
- 最尤推定法
- 中心極限定理
- ひずみゲージ
- 不確かさ
- 近接覚センサの原理
- 同時座標系
- グローシェーディング
- フォンシェーディング
- モンテカルロ法
- 分割統治法
- B 木
- 分枝限定法
- ヒープソート
- 分散ハッシュ
- DNS
- クライアントサーバシステム
- P2P システム
- AS 番号
- スペクトル拡散通信
- Unicode
- グリッドコンピューティング
- CGI
- TCP と UDP
- オプティカルフロー
- 離散コサイン変換
- 画像のエッジ検出法
- ナイキスト周波数
- サンプリング定理
- GIF と JPEG の符号化
- ハフ変換
- ラプラス変換

## 2 プログラミング

- プリプロセッサ
- コンパイラ
- アセンブラ
- アセンブリ言語
- ニーモニック
- リンカ (リンケージエディタ)
- インタプリタ
- デバッグ
- オブジェクト指向
- クラス変数とインスタンス変数
- 継承と継承
- オーバーライドとオーバーロード
- ポリモーフィズム
- イミュータブル
- ジェネリックプログラミング
- 命令型 (手続き型) プログラミング
- 宣言型プログラミング
- 構造化プログラミング
- メタプログラミング
- 論理プログラミング
- イベント駆動型プログラミング
- ドメイン固有言語
- スクリプト言語
- マクロ言語
- マークアップ言語
- HTML
- XML
- 動的型付けと静的型付け
- 動的スコープと静的スコープ
- 動的リンクと静的リンク
- ダックタイピング
- メモ化
- 自己書き換えコード
- シリアルライズ
- 評価戦略
- 多重ディスパッチ (マルチメソッド)
- 糖衣構文
- ラムダ計算
- 表明 (アサーション)
- モナド
- ガベージコレクション
- マークアンドスイープ
- 参照カウント
- 名前修飾
- 弱い参照
- ランタイムライブラリ
- リファクタリング
- API
- 第一級オブジェクト
- バイトコード
- プラグイン
- スレッドセーフ
- リエントラント
- メインループ (イベントループ)
- 呼び出し規約
- バッファオーバーラン
- 副作用
- スパゲティプログラム

## 3 言語理論

- チョムスキー階層
- バッカスナウア記法 (BNF)
- チョムスキー標準形
- グライバッハ標準形
- 形式文法と形式言語
- 字句解析
- lex と yacc
- 構文解析
- 曖昧な文法
- 抽象構文木
- LR 構文解析
- クロスコンパイラ
- プッシュダウンオートマトン
- CYK 法
- アーリー法
- マルコフアルゴリズム
- カリー化
- 機能的再帰関数 ( $\mu$  関数)

## 4 データベース

- 関係モデル
- データモデル
- E-R モデル
- 関係演算
- 論理表現と物理表現
- データベース言語
- データベース管理システム
- 3 層スキーマ
- トランザクション

- トランザクション分離レベル
- ACID 特性
- ロールフォワードとロールバック
- 再編成と再構築
- ジャーナルファイル
- データウェアハウス
- 一元管理とその利点
- NULL 値
- 更新時異常

## 5 ソフトウェア開発

- アジャイルソフトウェア開発
- ソフトウェアインスペクション
- 形式仕様記述
- UML
- Rapid Application Development
- オープンソースソフトウェア
- クロスプラットフォーム
- 動的プログラム解析
- 統合開発環境
- フロントエンドとバックエンド

- モジュール
- リバースエンジニアリング
- 契約プログラミング
- アンチパターン
- デザインパターン
- 凝集度 (コヒージョン)
- 結合度
- 粒度
- 移植性
- ブラックボックスとホワイトボックス

## 6 多変量解析と人工知能

- 傾向推定
- データクラスタリング
- エキスパートシステム
- データマイニング
- 因子分析
- 判別分析
- 正準相関分析
- オートエンコーダー
- ディープラーニング
- $k$  近傍法
- 過剰適合
- 交差検証
- ブースティング
- ロジスティック回帰
- パーセプトロン

- シグモイド関数
- Q 学習
- 自己組織化写像
- 集団的知性
- ベイズ誤り率
- 赤池情報量基準
- ブートストラップ法
- マハラノビス距離
- コーパス
- Neuroevolution
- ハイパーパラメータ
- 次元の呪い
- フレーム問題
- 人工無脳
- ソフトウェアエージェント

## 7 データ構造とアルゴリズム

- 逆ポーランド記法とポーランド記法
- 優先度付きキュー
- ハッシュ関数
- チャイティンの定数 (停止確率)
- クラス P とクラス NP
- $P \neq NP$  予想
- コルモゴロフ複雑性
- 充足可能性問題
- 停止性問題
- ソートの安定性
- 内部ソートと外部ソート
- マトロイド
- 反復深化深さ優先探索
- 深さ制限探索
- 最良優先探索
- 双方向探索
- 均一コスト探索
- $A^*$  アルゴリズム
- BM 法
- KMP 法
- ノーフリーランチ定理
- 線形計画法
- 整数計画問題
- シンプレックス法
- Nelder-Mead 法
- 最急降下法
- 共役勾配法
- 動的計画法
- 貪欲法
- ラグランジュの未定乗数法
- バックトラッキング
- ビタビアルゴリズム
- ヒューリスティクス
- 焼きなまし法
- タブーサーチ
- 粒子群最適化
- 蟻コロニー最適化
- 近似アルゴリズム
- 遺伝的アルゴリズム
- 最大フロー問題
- ギフト包装法
- ゲーム木
- ミニマックス法
- $\alpha\beta$  法
- ミラーラビン素数判定法
- テイラー展開
- 最小二乗法
- LU 分解
- 線形合同法
- メルセンヌツイスタ
- メトロポリス法
- 特異値分解

## 8 コンピュータグラフィクス

- フラクタル
- パーティクル
- メタボール
- レイトレーシング
- バンプマッピング
- 透視投影と平行投影
- AR と VR
- ブレゼンハムのアルゴリズム
- ダブルバッファ方式
- アフィン変換
- ワイヤフレームモデル
- サーフェスモデル
- CSG
- NURBS
- ポリゴン
- サブディビジョンサーフェス (細分割曲面)
- Z バッファ
- バイナリ空間分割
- 光モデル
- ラジオシティ
- マーチングキューブ法
- モーションブラー
- モーフィング
- GPU

## 9 コンピュータアーキテクチャ

- マイクロアーキテクチャ
- バイナリ変換
- コード密度
- オープンアーキテクチャ
- ノイマン型コンピュータ
- ノイマンボトルネック
- DNA コンピュータ
- 量子コンピュータ
- 設定ファイル
- ハードウェア記述言語
- メタデータ
- ウェアレベリング
- リアルタイムシステム
- ウォッチドッグタイマ
- 透過性
- フォールトトレラント
- GUI と CUI
- ムーアの法則
- アムダールの法則
- グロシュの法則
- ベンチマーク
- RFID
- シフトレジスタ
- 抽象化
- ステータスレジスタ
- メモリマップト I/O
- I/O マップト I/O (ポートマップト I/O)
- DMA
- コントロールストア
- ビジーウェイト (ポーリング)
- 割込み
- 割込みハンドラ
- デバイスドライバ
- カーネル
- シェル
- システムコール
- プロセス制御ブロック
- CPU モードとユーザモード
- 実行ファイル
- コンテキストスイッチ
- マルチタスク
- プリエンプション
- ラウンドロビンスケジューリング
- 排他制御
- 競合状態
- デッドロック
- 食事する哲学者の問題
- リソーススタベーション
- クリティカルセクション
- 不可分操作
- テストアンドセット
- コンペアアンドスワップ
- デッカーのアルゴリズム
- 互換性
- ロック
- スピンロック
- セマフォ
- モニタ
- ページ方式とセグメント方式
- アドレス空間
- MMU
- ページテーブル
- ページフォールト
- セグメンテーション違反
- 仮想記憶
- ページ置換アルゴリズム
- LRU
- 参照の局所性
- 補助記憶装置
- ファイルシステム
- フラグメンテーション
- メインフレーム
- フレームバッファ
- スループット
- MIPS
- FLOPS
- 命令セット
- テーブルジャンプ
- プログラムカウンタ
- コールスタック
- コアダンプ
- アドレッシングモード

- インライン展開
- アキュムレータ
- 2 進化 10 進数 (BCD)
- 符号付き数値表現
- 可変長数値表現
- 単精度と倍精度
- 丸め誤差
- 桁落ち誤差
- 算術シフトと論理シフト
- 非正規化数
- NaN
- 文字コード
- JIS コード
- ASCII
- バレルシフト
- ALU
- FPU
- ブースの乗算アルゴリズム
- キャリーセーブアダプター
- 演算子強度低減
- SRT 除算
- ステイッキービット
- コプロセッサ
- レジスタファイル
- 例外処理
- VLIW
- データ依存
- ワイヤードロジック
- ソフトウェアパイプラインニング
- ループ展開
- 投機的実行
- レベル適応型分岐予測
- 遅延スロット
- プリフェッチ
- リザベーションステーション
- メモリバリア
- レジスタリネーミング
- ファームウェア
- FPGA
- RAM と ROM
- SRAM と DRAM
- SDRAM

- キャッシュミスの 3C
- ダイレクトマップ方式
- セットアソシアティブ方式
- フルアソシアティブ方式
- スラッシング
- キャッシュコヒーレンシ
- ライトスルーとライトバック
- メモリインタリーブ
- L2 キャッシュ (2 次キャッシュ)
- プロセス識別子
- ノンブロッキングキャッシュ
- DIMM
- バックプレーン
- シンクロナイザ
- デファクトスタンダード
- SCSI
- PCI
- USB
- デイジーチェーン
- RAID
- ディスクアレイ
- 再構成可能コンピューティング
- 分散コンピューティング
- 分散共有記憶 (DSM)
- シンククライアント
- デスクトップ仮想化
- マルチプロセッサとマルチコア
- 対称型マルチプロセッシング
- ハードウェアマルチスレッディング
- NUMA
- コンピュータクラスタ
- メッセージ交換
- バリア同期
- MESI プロトコル
- 超並列マシン
- フリンの分類
- 性能解析 (プロファイラ)
- 仮想機械
- ハイパーバイザ
- エミュレータ
- 準仮想化
- GPGPU



## 10 暗号理論とセキュリティ

- 安全素数
- S ボックス
- ステガノグラフィー
- 一方向性関数
- 暗号学的ハッシュ関数
- ゼロ知識証明
- 電子署名
- S/MIME
- セキュリティの CIA
- サンドボックス
- 最小権限の原則
- ワンタイムパスワード
- 計算量的安全性
- 情報理論的安全性
- ケーパビリティ
- アクセス制御リスト
- ハードコア述語
- ワンタイムパッド
- 証明書失効リスト
- セキュリティホール
- 換字式暗号
- 転置式暗号
- DES
- ブロック暗号
- ストリーム暗号
- RSA 暗号
- 差分解読法
- 線形解読法
- 頻度分析
- 締め上げ暗号分析
- 辞書攻撃
- DoS 攻撃と DDoS 攻撃
- 総当たり攻撃
- 誕生日攻撃
- 反射攻撃
- 暗号文単独攻撃
- ゼロデイ攻撃
- Fork 爆弾
- SQL インジェクション
- DNS キャッシュポイズニング
- サイドチャネル攻撃
- ゾンビコンピュータ
- コンピュータウイルス
- ブートストラップウイルス
- マクロウイルス
- ワーム
- スパムメール
- ボットによる攻撃
- トロイの木馬
- スパイウェア
- ファーミング
- ワンクリックウェア
- ソーシャルエンジニアリング
- スキミング

## 11 メカトロニクス

- アクチュエータ
- ポテンショメータ
- ロータリエンコーダ
- サイリスタ
- サーミスタ
- マニピュレータ
- ステッピングモータ (パルスモータ)
- リーク電流
- チャタリング
- 能動回路と受動回路
- 分布定数回路
- 水晶振動子
- MEMS
- CMOS
- ECL
- LED
- PLL
- 分解能
- 測域センサ
- トレーサビリティ

## 12 コンピュータネットワーク

- LAN, WAN, PAN
- Ethernet
- MIMO
- ARPANET
- OSI 参照モデル
- エンドツーエンド原理
- オーバレイネットワーク
- 電力線搬送通信
- 回線交換
- 同期方式
- ガードインターバル
- 前方誤り訂正
- ADSL
- CSMA/CA と CSMA/CD
- ストリーミング
- 非同期転送モード
- フレームリレー
- FTTH
- 輻輳制御
- 自動再送要求
- 肯定要求 (ACK)
- VPN
- Ajax
- CIDR
- ネットワークアドレス変換
- クラウドコンピューティング
- プロキシサーバ
- リバースプロキシ
- イントラネット
- エクストラネット
- ルーティングプロトコル
- OSPF
- EIGRP
- RIP
- BGP
- モデム
- ISDN
- リピータ
- スイッチングハブ
- ネットワークカード (NIC)
- SIM カード
- TCP/IP
- 3 ウェイハンドシェイク
- DHCP
- FTP
- HTTP
- IMAP
- IRC
- LDAP
- MGCP
- NNTP
- NTP
- POP
- RPC
- RTP
- SIP
- SMTP
- SNMP
- SSH
- Telnet
- TFTP
- SSL
- XMPP
- SCTP
- RSVP
- IPv4 と IPv6
- IP フラグメンテーション
- ICMP
- IGMP
- IPSec
- VoIP
- Mobile IP
- RADIUS
- ARP と RARP
- トンネリング
- SPB
- PPP
- メディアアクセス制御
- ファイアウォール
- 非武装地帯 (DMZ)
- ホスト名
- ドメイン名とサブドメイン名
- サブネットマスク
- ラウンドトリップタイム
- ローミング
- ASP
- WWW
- URL
- ハイパーテキスト
- ハイパーリンク
- SNS
- コンテンツデリバリネットワーク
- VPS
- IaaS, PaaS, SaaS
- GPS
- GSM
- ACD
- Wi-Fi
- LTE
- WiMAX
- サービスセット識別子 (SSID)

## 13 情報通信理論

- 情報量 (エントロピー)
- 結合エントロピー
- 相互情報量
- マルコフ過程
- レイテンシ
- SN 比
- 符号誤り率
- スペクトル効率
- 通信路容量
- シャノン=ハートレーの定理
- 冗長性
- エンコードとデコード
- 巡回冗長検査
- 誤り訂正符号
- チェックサム
- パリティ検査符号
- ハフマン符号
- ハミング符号
- リードソロモン符号
- BCH 符号
- 畳み込み符号
- ターボ符号
- 8B/10B
- 振幅変調
- 周波数変調
- 位相変調
- 位相偏移変調
- パルス符号変調
- 空間分割多重
- 周波数分割多重
- 時間多重
- 符号多重
- 直交周波数分割多重 (OFDM)
- 符号分割多重接続 (CDMA)

## 14 信号画像処理

- ウェーブレット変換
- Z 変換
- 双一次変換
- 高速フーリエ変換
- アダマール変換
- 無限インパルス応答
- スペクトル密度
- ハイパス/ローパスフィルタ
- 連長圧縮
- 窓関数
- ホワイトノイズとピンクノイズ
- 解像度
- ダイナミックレンジ
- ピーク信号対雑音比
- アスペクト比
- YUV 色空間
- HSV 色空間
- テンプレートマッチング

## 15 制御工学

- ラウス・フルビッツの安定判別法
- ファジィ制御
- ボード線図
- ナイキスト線図
- ニコルズ線図
- 状態空間
- 可制御性と可観測性
- 有界入力有界出力安定性
- 状態観測器
- 時不変システム
- オンオフ制御
- ヒステリシス
- プログラマブルロジックコントローラ
- リアプノフ関数