CAOS

FPGAの説明とデモ

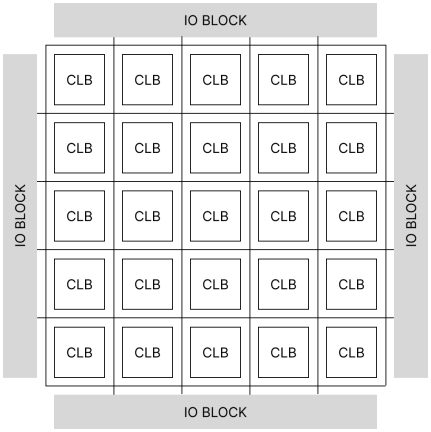
s1300040 東 大智

ASICとは

- ASIC (Application Specific Integrated Circuit) は半導体集積回路の一種
- シリコンから切り出したウエハに，いくつもの工程を踏んであらかじめ設計した回路を焼き付けることで，任意の動作を決定する．つまり，一度回路を決定すると，それ以降動作を変更することができない．

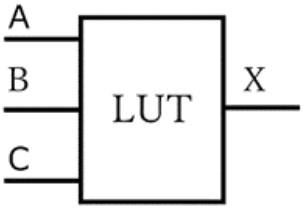
FPGAとは

- FPGA (Field Programmable Gate Array) とは，現場 (Field) で論理回路の構成をプログラムできる (Programmable) 論理回路 (Gate) を集積したデバイス
- 多数のCLB {設定可能 (Configurable) な論理 (Logic) ブロック(Block) }が集まって構成される
- ロジックブロックはLook-Up Table，FF，MUXで構成され，それぞれがIO-busや内部配線に繋がれる



Look-Up Tableとは

- 任意の論理関数を実装することができる素子であり，FPGAの中核をなす要素．
- 入力の組み合わせに対する出力値をメモリテーブルとして保持するので，メモリを書き換えるだけで任意の動作を決定することができる．
  例えば，3入力のLUTなら2^3=8通りの入出力の組み合わせを格納する．e.g.

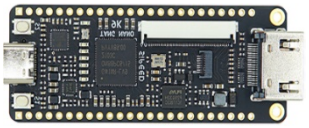


majority vote

a	b	c	x
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

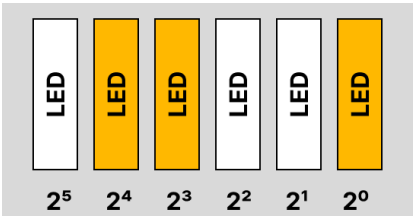
Tang Nano 9kとは

- Sipeed社製のFPGAボード。HDMI，RGBスクリーン，SPIスクリーン，32Mbit SPI flash，6つのLEDを備えている
- 4入力1出力のLUTが8640個実装されている (9K)



デモンストレーション

- FPGAに搭載されているLEDの点灯を制御
  FPGAにハードウェア記述言語でプログラムした論理回路を実装する．今回実装したものは，スイッチを押す度に2進数表記されたLEDが1ずつ加算されて点灯する論理回路．
  e.g. 25回ボタンを押したときのLEDの図



- FPGA上で実装したCPU(RISC-V)でC言語のプログラムの実行
  ハードウェア記述言語で実装されたCPU(RISC-V)をFPGAに書き込み，C言語のプログラムをFPGA上で動作させる．今回実行するプログラムは，任意の文字列からsha256アルゴリズムを用いてハッシュ値を算出し出力する．

※sha256アルゴリズムとは暗号学的ハッシュ関数の一つで，入力値に対して固定長のデータを出力する，同じ入力に対して同じ出力をする，出力値から入力値を求めるのが(事実上)困難，入力値を少しでも変えると，出力値は大幅に変わり，相関がないように見える，などの特徴がある．

参考文献

1. Sipeed wiki Tang Nano 9k (https://wiki.sipeed.com/hardware/en/tang/Tang-Nano-9K/Nano-9K.html)
2. Clifford wolf picorv32 (https://github.com/YosysHQ/picorv32)
3. sha256 hash function(https://wikipedia.org/wiki/SHA-2)

Computer Architecture & Operating Systems Group, The University of Aizu
Daichi Higashi and Dr. Hitoshi Oi (supervisor)