

第1章 FPGAの進歩に伴い実用価値が高まる高位合成

高位合成の必要性と技術的課題、そして今後

森岡 澄夫 Sumio Morioka

C言語などのソフトウェア・コードからRTLを自動生成する高位合成(動作合成とも呼ばれる)は、1980年代から研究開発が活発化し、1990～2000年代には本格的な市販ツールも登場しましたが、なかなか普及が進みませんでした。しかしここ数年のFPGAの進歩や用途の変化により、普及を阻害していた要因の一部は回避できるようになってきています。あらゆる回路を高位合成しようとするのではなく、適したアプリケーションを選び、合成の得意・不得意を見極めた使い方をすれば、十分に恩恵を得られます。


1. なぜ高位合成をしたいのか

● 複雑な動作をハード実装する方法はそれしかない
 そもそも高位合成を使いたい理由は、とても単純です。複雑な動きをする回路を、簡単に早く作成してテストもしたい、という点に尽きます(図1)。使い古された例えですが、マイコンなどのソフトウェアを作る際に、高級言語のコンパイラを使えるに越したことはなく、必要がない限りは低レベルのアセンブラを使いたくないのと同じことです。
 また、もし世の中の多くのデータ処理や制御処理を専用回路で行えるのであれば、似たようなプロセス・

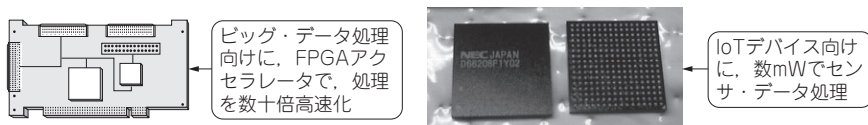
ルールやテクノロジーで作ったプロセッサと比べ、桁違いに高速化したり低電力化したりすることが可能です。しかし専用回路の置きどころは、設計やテストがソフトウェアと比べてずっと難しくて手間がかかり、エンジニアの数も限られていることです。

データ処理や制御処理はどんどん複雑化が進んでいますが、それに比べると回路設計環境の進歩は速いとはいえ、もどかしい状況です。IPコアが蓄積されたり、IPコア接続ツール(Altera社のQsysなど)が普及したりはしているのですが、スクラッチ設計環境(つまり高位合成)が進歩しないと、高度な処理はなかなか作れるようになりません。

最新のデータ処理やデバイス・通信制御処理を実装したい

データ圧縮や認識など	複雑な最新アルゴリズム
	<ol style="list-style-type: none"> 1. Choose $\rho_E \in \mathbb{Z}_q$, $(\rho_m, \rho_h) \in \{0,1\}^{n/2} \times \{0,1\}^{n/2}$, $\mu_x \in \{0,1\}^{n/2+\kappa+\sigma}$, $\mu_y \in \{0,1\}^{n/2+\kappa+\sigma}$, $\mu_z \in \{0,1\}^{n/2+\kappa+\sigma}$ and $\mu_E \in \mathbb{Z}_q$, randomly. 2. Compute $E = (E_0, E_1, E_2) = ((\rho_E/G, h_x + \rho_E/H_1, h_x + \rho_E/H_2))$ and $(\rho_{state}, \rho_{cipher}) = ((\mu_z/G, \mu_x/G + \mu_z/H_1, \mu_x/G + \mu_z/H_2))$. 3. Compute $(A_{COM}, B_{COM}) = (A_{COM}^{\rho_m} \bmod n, B_{COM}^{\rho_h} \bmod f)$ and $(\rho_{state}, \rho_{cipher}) = (A_{COM}^{\rho_m} \bmod n, B_{COM}^{\rho_h} \bmod f)$. 4. Compute $c = \text{Hash}(\kappa, \text{ipk}, \text{opk}, \text{rpk}, E, A_{COM}, B_{COM}, \rho_{state}, \rho_{cipher}, m)$. 5. Compute $\tau_x = c\tau_1 + \mu_x$, $\tau_y = c\tau_2 + \mu_y$, $\tau_z = c\tau_3 + \mu_z$, $\tau_r = c\tau_4 + \mu_r$ and $\tau_g = c\rho_E + \mu_E \bmod q$. 6. The output signature is $(E, A_{COM}, B_{COM}, c, \tau_x, \tau_y, \tau_z, \tau_r, \tau_g)$.

- (1) プロセッサでは遅過ぎるので、回路で並列処理したい
- (2) プロセッサでは消費電力が大き過ぎるので、回路化したい



回路化をHDLによるRTL設計で行うのは、抽象レベルが低く大変。テストにも時間がかかる

図1 高位合成が欲しくなる動機