Comparison of Bit and Word Level Algorithms for Evaluating Unstructured Functions over Finite Rings

Berk Sunar David Cyganski
sunar,cyganski@wpi.edu
http://crypto.wpi.edu

Worcester Polytechnic Institute
Department of Electrical & Computer Engineering
Worcester, Massachusetts 01609, USA

CHES 2005

Motivation

Need to implement unstructured functions defined over finite fields or rings:

- S-boxes in block and stream ciphers (DES, AES)
- Round functions in hash functions (MD5, SHA-1)
- Public key schemes defined over finite fields or rings

Implementation

- Common representation

$$f(x_1, x_2, x_3) = c_0 + c_1x_1 + c_2x_2 + c_3x_3 + c_4x_1x_2 + c_5x_1x_3 + c_6x_2x_3 + c_7x_1x_2x_3$$

  where $c_i, x_i \in R$.
- Typically implemented as parallel circuit *as given in the description*
- Components of the circuit are isolated blocks implementing operations in R.

A Question

- Idea: We can view the entire function as being defined over $GF(2)$
- Which approach is more efficient?
  - implement the circuit in two levels first as a circuit over R, and then implement operations in R as boolean circuits
  - implement the whole circuit as a boolean circuit, i.e. over $GF(2)$.

Horner's Method

In the univariate case a polynomial of degree $r-1$ over Z_m is represented as

$$u(x) = u_0 + u_1 x + u_2 x^2 + \ldots + u_{r-1} x^{r-1} \quad , \quad u_i \in Z_m \ .$$

Applying Horner's method

$$u(x) = u_0 + x(u_1 + x(u_2 + x(u_3 + \ldots + x(u_{r-2} + x u_{r-1})) \ldots)$$

is evaluated by computing only $r-1$ additions and $r-1$ multiplications with delay $T = (r-1)T_A + (r-1)T_M$

The Multivariate Version of Horner's Method

Level	#Coefficient Polynomials	#Mult or #Add
1	r	$(r-1)$
2	r^2	$(r-1)r$
3	r^3	$(r-1)r^2$
$\vdots$	$\vdots$	$\vdots$
n	r^n	$(r-1)r^{n-1}$

Table: Number of coefficient polynomials introduced in each level

The Multivariate Version of Horner's Method

- The evaluation of an n-variate polynomial over Z_m of maximum degree $(r-1)$ in all variables requires at most $r^n - 1$ additions and $r^n - 1$ multiplications in Z_m.
- The delay of a parallel circuit (of n levels) is at most $T = n(r-1)T_A + n(r-1)T_M$.

An Example

Let $Z_m = Z_2$ and $f = f(x_1, x_2, x_3, x_4)$ represent a multivariate polynomial $f : (Z_2)^4 \mapsto Z_2$ explicitly given as

$$\begin{aligned} f &= x_1x_2x_3x_4 + x_1x_2x_3 + x_1x_2x_4 + x_2x_3x_4 + x_1x_3 + x_3x_4 \\ &+ x_2x_4 + x_3x_4 + x_3 + x_2 + x_1 + 1 \ . \end{aligned}$$

Applying Horner's algorithm we convert the polynomial into the following representation

$$\begin{aligned} f &= 1x_1\left[1x_2\{1x_3(1x_4+1)+(1x_4+0)\}+\{1x_3(0x_4+1)+(1x_4+1)\}\right] \\ &+ \left[1x_2\{1x_3(1x_4+0)+(1x_4+1)\}+\{1x_3(1x_4+1)+(0x_4+1)\}\right] \end{aligned}$$

An Observation

- In the last level we have 8 polynomial evaluations of the form $ax_4 + b$ where $a, b \in Z_2$.
- However, there can be only 2^2 such polynomials.
- Multivariate version of Horner's algorithm is redundant!
- Same argument can be repeated for lower levels as well.
- Need to find the level where redundancy vanishes.

The Optimization Strategy

Level	#Coefficient Polynomials	#Mult or #Add	#Unique Polynomials	#Mult or #Add
1	r	$(r-1)$	m^{nr}	$(r-1)m^{r^n}$
2	r^2	$(r-1)r$	$m^{(n-1)r}$	$(r-1)m^{r^{n-1}}$
3	r^3	$(r-1)r^2$	$m^{(n-2)r}$	$(r-1)m^{r^{n-2}}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$n-2$	r^{n-2}	$(r-1)r^{n-3}$	m^{3r}	$(r-1)m^{r^3}$
$n-1$	r^{n-1}	$(r-1)r^{n-2}$	m^{2r}	$(r-1)m^{r^2}$
n	r^n	$(r-1)r^{n-1}$	m^r	$(r-1)m^r$

Table: Number of coefficient polnomials and unique polynomials at each level

Finding the Sweetspot

- Find the level k in which the number of coefficients exceeds the number of unique polynomials
- Find the smallest value of k satisfying

$$r^k \geq m^{r^{n-k+1}}$$

- Take the logarithm of both sides

$$kr^k \geq r^{n+1} \log_r m \ .$$

- Define $c = r^{n+1} \log_r m$ and take the log of both sides w.r.t base r

$$k \geq \log_r c - \log_r k \ .$$

Finding the Sweetspot

- Keep substituting value of k

$$k = \log_r c - \log_r(\log_r c - \log_r k(\log_r c - \log_r k(\log_r c - \log_r(\ldots)\ldots)\ldots) .$$

- The exact solution is defined in terms of the Lambert-W function [2]

$$k \geq W(\log r \frac{r^{n+1}}{\log_m r}) / \log r$$

where $W(x)$ is defined as the inverse of the map $x \rightarrow xe^x$.

- Approximate k by neglecting terms after two levels of substitution

$$k \approx \log_r c - \log_r(\log_r c) .$$

The Circuit Complexity

- Derive complexity in terms of Z_m additions and multiplications

$$
\begin{aligned}
C &= \sum_{i=1}^{k}(r-1)r^{i-1} + \sum_{i=1}^{n-k}(r-1)m^{r^i} \\
&= (r^k - 1) + (r-1)(m^r + m^{r^2} + m^{r^3} + \ldots + m^{r^{n-k}}) \\
&\approx r^k + rm^{r^{n-k}}
\end{aligned}
$$

- Substitute values derived from other identities[1]

$$
\begin{aligned}
C &= \frac{c}{\log_r c} + rm^{\frac{n \log_m r}{r}} \\
&= \frac{r^{n+1}\log_r m}{(n+1) + \log_r(\log_r m)} + r^{\frac{n}{r}+1}
\end{aligned}
$$

- Addition and multiplication complexities grow by $O(\frac{r^n}{n})$.

[1] See paper for details

Modified Horner over Prime Fields $GF(p)$

- Given $n > p$ the evaluation of an n-variate polynomial over $GF(p)$ requires at most $O(\frac{p^n}{n})$ additions and multiplications in $GF(p)$ with a delay of $O((p-1)(n-\log_p n))$.
- Muller [5] gives a construction gives a method for evaluating arbitrary n-variate polynomials over $GF(2)$ with $O(\frac{2^{n+1}}{n+1})$ complexity
- For $p = 2$ our construction is equivalent to Muller's construction.

Comparison of Circuit Area

- The bit-level algorithm implementing a polynomial evaluation over $GF(p)$ has bit-complexity

$$C_B = O\left((\log_2 p)\frac{2^{n\log_2 p+1}}{n\log_2 p + 1}\right) = O\left(\frac{2p^n}{n}\right) .$$

- Assuming a $GF(p)$ multiplication operation takes $(\log_2 p)^2$ bit operations we obtain the bit complexity of word level evaluation as follows

$$C_W = O\left(\frac{p^{n+1}}{n+1}(\log_2 p)^2\right) .$$

- The bit-level algorithm is $\frac{p}{2}(\log_2 p)^2$ times more area efficient

Comparison of Time Complexities

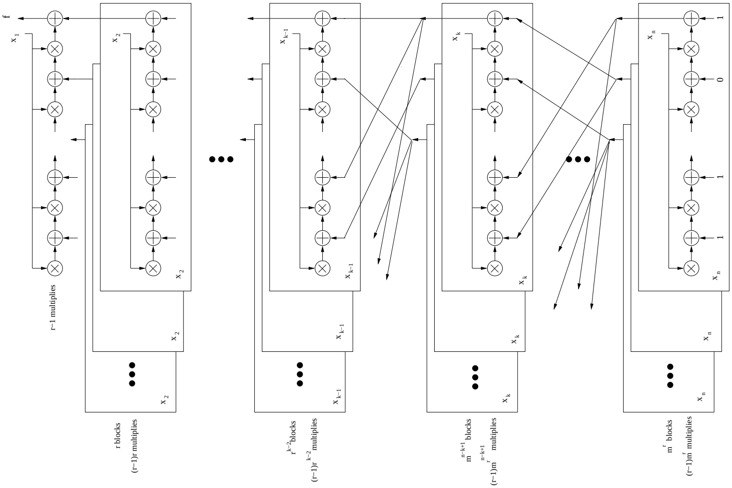
- The bit-level approach yields a time complexity of

$$T_B = O(n \log_2 p - \log_2(n \log_2 p)).$$

- Ignoring the constant operations the overall computation takes

$$T_W = O((p-1)(\log_2 \log_2 p)(n - \log_p n)).$$

  gate delays in the word-level approach.
- The bit-level algorithm is roughly $\frac{(p-1)(\log_2 \log_2 p)}{\log_2 p}$ times faster


f
r−1 multiplies
r blocks
(r−1)r multiplies
r^{k−2} blocks
(r−1)r^{k−2} multiplies
m^{n−k+1} blocks
(r−1)m^{n−k+1} multiplies
m^r blocks
(r−1)m^r multiplies
0
1

Conclusion

- We have develop a generic technique for *optimally* implements multivariate functions defined over finite rings.
- We have shown that implementing arbitrary (or generic) circuits over $GF(2)$ is more efficient
- The bit-level algorithm is $\frac{p}{2}(\log_2 p)^2$ times more area efficient
- The bit-level algorithm is roughly $\frac{(p-1)(\log_2 \log_2 p)}{\log_2 p}$ times faster
- Fan-out may be a problem for the bit-level algorithm!

Bibliography

1. A. Borodin. Horners Rule is Uniquely Optimal. In Z. Kohavi and A. Paz, editors, *Proceedings of an International Symposium on the Theory of Machines and Computations*, pages 45–57. Academic Press, 1971.
2. R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert W Function. *Advances in Computational Mathematics*, 5:329–359, 1996.
3. W. G. Horner. A new method of solving numerical equations of all orders by continuous approximation. *Philos. Trans. Roy. Soc. London*, 109:308–335, 1819.
4. D. E. Knuth. *The Art of Computer Programming. Volume 2: Seminumerical Algorithms*. Addison-Wesley, Reading, Massachusetts, USA, 2nd edition, 1981.
5. D. E. Muller. Complexity in Electronic Switching Circuits. *IRE Transactions on Electronic Circuits*, (5):15–19, 1956.
6. NIST FIPS PUB 180-1. *Secure Hash Standard*. Federal Information Processing Standards, National Bureau of Standards, U.S. Department of Commerce, April 1995.
7. NIST FIPS PUB 46-3. *Data Encryption Standard*. Federal Information Processing Standards, National Bureau of Standards, U.S. Department of Commerce, 1977.
8. U.S. Department of Commerce/National Institute of Standard and Technology. *Advanced Encryption Standard (AES)*, November 2001.
9. A. M. Ostrowski. On two problems in abstract algebra connected with Horner's rule. pages 40–48. Academic Press, 1954. presented to Richard von Mises.
10. V. Ya. Pan. Methods for Computing Values of Polynomials. *Russian Mathematical Surveys*, 21(1):105–136, 1966.
11. R.L. Rivest. *RFC 1321: The MD5 Message-Digest Algorithm*. Corporation for National Research Initiatives, Internet Engineering Task Force, Network Working Group, April 1992.
12. C. E. Shannon. The Synthesis of Two-terminal Switching Circuits. *Bell System Technical Journal*, 28(1):59–98, 1949.
13. ETSI/SAGE Specification. Specification of the 3GPP confidentiality and integrity algorithms; part 2: KASUMI specification. 3GPP TS 35.202, European Telecommunications Standards Institute, Sophia-Antipolis Cedex, France, November 1999. Draft.