Boolean Decision Functions

Steven Finch

April 22, 2015

Let $f : \{0,1\}^n \to \{0,1\}$ be the Boolean function that decides whether a given $(n+1)$-bit odd integer is square-free. More precisely,

$$f(x_1, x_2, \ldots, x_n) = \begin{cases} 1 & \text{if } 2\xi + 1 \text{ is square-free,} \\ 0 & \text{otherwise} \end{cases}$$

where the string $x_1 x_2, \ldots x_n$ is the integer ξ written in binary (with leading zeroes added as necessary). Let x denote the vector $(x_1, x_2, \ldots, x_n)$. There are many ways of characterizing the computational complexity of f; we focus on a single combinatorial method related to what is called the *average sensitivity* of f. The **influence** of x_i on f, denoted by $I_i(f)$, is the probability that flipping the i^{th} component of the input vector, selected at random from $\{0,1\}^n$, will flip the output. That is,

$$I_i(f) = 2^{-n} \sum_{x \in \{0,1\}^n} \left| f(x) - f\left(x^{(i)}\right) \right|$$

where $x^{(i)} = (x_1, x_2, \ldots, x_i + 1, \ldots, x_n)$ modulo 2. Bernasconi, Damm & Shparlinski [1, 2] proved that

$$I_i(f) = 2\gamma_{\text{int}} + o(n)$$

as $n \to \infty$, where

$$\gamma_{\text{int}} = \frac{8}{\pi^2} - 2\prod_p \left(1 - \frac{2}{p^2}\right) = 0.1653012713... = \frac{0.3306025426...}{2}.$$

In words, an odd integer changes from square-free to square-full or vice versa with probability $\approx 33\%$ if one of its bits is flipped. The infinite product is familiar – called the Feller-Tornier constant in [3] – and its appearance here is quite interesting.

We turn attention from integers to polynomials with coefficients in the finite field $\mathbb{Z}_2$. Let $g : \{0,1\}^n \to \{0,1\}$ decide whether a given binary polynomial with constant coefficient unity

$$\eta(x) = y_n x^n + y_{n-1} x^{n-1} + \cdots + y_1 x + 1$$

is square-free. More precisely,

$$g(y_1, y_2, \ldots, y_n) = \begin{cases} 1 & \text{if } \eta(x) \text{ is square-free,} \\ 0 & \text{otherwise} \end{cases}$$

and we again abbreviate the vector as y. The influence $I_i(g)$ of y_i on g is defined similarly. Clearly the polynomial corresponding to the vector $y^{(i)}$ is $\eta(x)+x^i$ modulo 2. Allender, Bernasconi, Damm, von zur Gathen, Saks & Shparlinski [4] proved that

$$I_i(g) = 2\gamma_{\text{poly}} + O\left(2^{-n/4}\right)$$

as $n \to \infty$, where

$$\gamma_{\text{poly}} = \frac{2}{3} - 2\prod_{k=1}^{\infty}\left(1 - \frac{1}{2^{2k-1}}\right)^{a_k} = 0.2735795624... = \frac{0.5471591248...}{2}.$$

The sequence $\{a_k\}_{k=1}^{\infty} = \{2, 1, 2, 3, 6, 9, 18, 30, \ldots\}$ counts all irreducible polynomials over $\mathbb{Z}_2$ of degree k and satisfies [5]

$$2^k = \sum_{d\,|\,k} d\, a_k;$$

equivalently,

$$a_k = \frac{1}{k}\sum_{d\,|\,k}\mu\left(\frac{k}{d}\right)2^d$$

where μ is the Möbius mu function [6]. Note that the error term is tighter for $I_i(g)$ than that for for $I_i(f)$.

A fascinating unanswered question arises if we replace square-freeness by primality (for odd integers) and irreducibility (for binary polynomials). What are the influence I_i asymptotics in this new scenario? Formulas analogous to the preceding would be good to see someday.

With regard to integers, a positive proportion of primes become composite when *any* one of their bits is changed [7, 8, 9]. As a consequence, it is not possible to establish whether an arbitrary integer is prime without examining all of its bits. With regard to polynomials, it is curious that [10]

$$\prod_{k=1}^{\infty}\left(1 - \frac{1}{2^{2k}}\right)^{a_k} = \frac{1}{2}$$

is trivial while a slight modification yields the unrecognizable constant γ_{poly}.

References

[1] A. Bernasconi, C. Damm and I. Shparlinski, On the average sensitivity of testing square-free numbers, *Computing and Combinatorics (COCOON)*, Proc. 1999 Tokyo conf., ed. T. Asano, H. Imai, D. T. Lee, S.-I. Nakano and T. Tokuyama, Lect. Notes in Comp. Sci. 1627, Springer-Verlag, 1999, pp. 291–299; MR1730345 (2000i:11192).

[2] A. Bernasconi, C. Damm and I. Shparlinski, The average sensitivity of square-freeness, *Comput. Complexity* 9 (2000) 39–51; MR1791089 (2001k:11179).

[3] S. R. Finch, Meissel-Mertens constants, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 94–98.

[4] E. Allender, A. Bernasconi, C. Damm, J. von zur Gathen, M. Saks and I. Shparlinski, Complexity of some arithmetic problems for binary polynomials, *Comput. Complexity* 12 (2003) 23–47; MR2054893 (2005b:68119).

[5] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, A001037, A059966, and A060477.

[6] S. R. Finch, Artin's constant, *Mathematical Constants*, Cambridge Univ. Press, 2003, pp. 104–109.

[7] F. Cohen and J. L. Selfridge, Not every number is the sum or difference of two prime powers, *Math. Comp.* 29 (1975) 79–81; MR0376583 (51 #12758).

[8] Z.-W. Sun, On integers not of the form $\pm p^a \pm q^b$, *Proc. Amer. Math. Soc.* 128 (2000) 997–1002; MR1695111 (2000i:11157).

[9] T. Tao, A remark on primality testing and decimal expansions, *J. Aust. Math. Soc.* 91 (2011) 405–413; arXiv:0802.3361; MR2900615.

[10] E. R. Berlekamp, *Algebraic Coding Theory*, rev. ed., Aegean Park Press, 1984, pp. 70–86; MR0238597 (38 #6873).