A rank conjecture

October 22, 2009

Conjecture. Suppose that $f_1, ..., f_k$ and $g_1, ..., g_k$ are polynomials in $\mathbb{F}_2[x]$, having $r_1, ..., r_k < k$ and $d_1, ..., s_k < k$ non-zero terms, respectively; and, suppose that $g(x)$ is an irreducible polynomial such that the order of x mod $(2, g(x))$ is greater than twice the maximal degree of the f_i's and g_i's. Then, so long as

$$M \ > \ (r_1 + \cdots + r_k + s_1 + \cdots + s_k)k^{o(1)},$$

and so long as

$$f_1(X)g_1(X),\ f_2(X)g_2(X),\ ...,\ f_k(X)g_k(X)$$

are linearly independent over $\mathbb{F}_2$, we have that the following matrix has full rank (i.e. rank k) in the residue field $\mathbb{F}_2[x]/(g(x))$:

$$\begin{bmatrix} f_1(1)g_1(1) & f_2(1)g_2(1) & \cdots & f_k(1)g_k(1) \\ f_1(x)g_1(x) & f_2(x)g_2(x) & \cdots & f_k(x)g_k(x) \\ \vdots & \vdots & \ddots & \vdots \\ f_1(x^M)g_1(x^M) & f_2(x^M)g_2(x^M) & \cdots & f_k(x^M)g_k(x^M) \end{bmatrix}$$

Remark. If in place of products of polynomials, we just had that the rows of the matrix have entries $f_1(x^j), f_2(x^j), ..., f_k(x^j)$, then by taking linear combinations of the columns in a certain Vandermonde matrix, it is quite easy to show that if $M = r_1 + \cdots r_k$ then this f_i matrix has full rank.