A Note on a Theorem of Fried and MacRae

Josef Schicho
RISC Linz
Johannes Kepler University
A-4040 Linz
Austria

September 30, 1997

Abstract

A theorem of Fried and MacRae will be proved and generalized with categorical methods.

1 Introduction

Consider polynomial equations over some field k as a language, describing properties of some "magnitudes" $x_1, \ldots, x_n$. A sentence is of the form

$$l = r,$$

where l and r are polynomials in $x_1, \ldots, x_n$. The sentence $l_2 = r_2$ is a consequence of the sentence $l_1 = r_1$ iff the polynomial $l_1 - r_1$ divides the polynomial $l_2 - r_2$.

Starting with a sentence $l = r$, we may "polynomially derive" other sentences by applying the same univariate polynomial to both sides: $H(l) = H(r)$. This new sentence is always a consequence of the former.

Fried and MacRaes theorem ([6],[7]) and its generalizations (Theorem 2 and Theorem 3 in section 3) state that under some assumption that essentially forbids correlations between left hand side and right hand side, any such consequence relation has a polynomial proof in the above sense.

The theorem turned out to be quite useful in the theory of decompositions. It allows to find common left factors of two polynomial functions F and G with respect to composition. It reduces the problem to the usual factorization of one bivariate polynomial. One can also take $F = G$ and find all left factors of F.

Alonso, Gutierrez and Recio found useful generalizations to the case of rational functions (cf [1],[2]). Binder [4] and Aichinger [5] generalized to the the multivariate case.

However, it is interesting to notice that all those FMR-like theorems are easy consequences of a category theoretical statement: The pushout diagram of stable monos is also a pullback diagram. In **Sets**, where every mono is stable, the statement is easily seen to be true. More generally, the same holds for topoi (cd [7]).

For **Rings**, the statement can easily be proved under additional assumptions (which are fulfilled in all applications). As a consequence of this observation, we obtain a proof for the previously open case of rational functions in several variables.

I am indepted to E. Aichinger, C. Alonso and F. Binder for their enlightening discussions about the FMR theorem. This paper is influenced by their work. The discussion was made possible by an integrated action between Austrian and Spanish universities.

I also thank J. Pfalzgraf for helpful remarks.

2 Pushouts that are pullbacks

In **Sets**, the pullback of monos $A \hookrightarrow G$ and $B \hookrightarrow G$ is the intersection $A \cap B \hookrightarrow G$.

Proposition 1 *Let $C \hookrightarrow A$ and $C \hookrightarrow B$ be monos in* **Sets**. *Then all four arrows in the pushout diagram*

$$\begin{tikzcd} & C \arrow[dl] \arrow[dr] & \\ A \arrow[dr] & & B \arrow[dl] \\ & D & \end{tikzcd}$$

are mono, and the diagram is also a pullback diagram.

The proof is easy. It is rather instructive to try to generalize the proposition to other categories. In [7], the proposition is proved for topoi.

If we have a diagram of monos

$$\begin{tikzcd} & C \arrow[dl] \arrow[dr] & \\ A & & B \end{tikzcd}$$

in **Rings**, then the arrow $A \rightarrow A \otimes_C B$ is in general not mono, because the functor $\_ \otimes_C B$ from C-**Mod** to C-**Mod** is not left exact. But $\_ \otimes_C B$ is left exact if B is flat over C (flat implies stable mono). In the following theorem, the assumption is even stronger.

Theorem 1 *Let A and B be two C-algebras that are free as C-modules. Assume that the bases of A and B contain 1. Then all four arrows in the pushout diagram*

$$\begin{tikzcd} & C \arrow[dl] \arrow[dr] & \\ A \arrow[dr] & & B \arrow[dl] \\ & A \otimes_C B & \end{tikzcd}$$

are mono, and the diagram is also a pullback.

Proof: Let

$$A = \bigoplus_i a_i \cdot C, a_0 = 1,$$

$$B = \bigoplus_j b_j \cdot C, b_0 = 1.$$

Then

$$A \otimes_C B = \bigoplus_{i,j} a_i \otimes b_j \cdot C,$$

and the (obviously injective) images of A and B in $A \otimes_C B$ are

$$\bigoplus_i a_i \otimes 1 \cdot C \text{ and } \bigoplus_j 1 \otimes b_j \cdot C.$$

The set-theoretic pullback is the intersection, namely

$$1 \otimes 1 \cdot C = C.$$

This shows that the diagram is a pullback in **Sets**.

Now, **Rings** is a finitary algebraic category (cf [4],[8]). Hence pullbacks exist and coincide with the pullbacks of underlying sets (forgetting the algebraic structure). The functions $0, 1, +, -, \cdot$ are the restrictions of the corresponding functions in the superset A, hence they are also the same as in the original ring structure in C.

It would be more satisfactory (from a category theoretic point of view) if the assumption could be weakened to $C \to A$ and $C \to B$ being stable mono. But for all applications that follow, this weaker form is sufficient. Since we are not earning more, it is not worth to pay the price of a more complicated proof, even if the stronger version were true.

The theorem has some relevance in computational algebra, because pullbacks are - in contrary to pushouts - not very reliable to explicit computation. In general, it is rather hard to check the pullback property of a diagram. The above theorem answers at least a special case.

3 Applications

The generalized FMR-theorem reads as follows.

Corollary 1 *Let $f : C \to A$ and $g : C \to B$ be two C-algebras that are free as C-modules. Assume that the bases of A and B contain 1. Let $a \in A$ and $b \in B$. The following are equivalent:*
a) There exists $h \in C$ such that $f(h) = a$ and $g(h) = b$.
b) $a \otimes 1 = 1 \otimes b$ in $A \otimes_C B$.

Proof: This is nothing else than the statement that the pushout diagram is a pullback in **Sets**. The set-theoretic pullback is

$$A \times_{A \otimes_C B} B = \{(a, b) \in A \times B \mid a \otimes 1 = 1 \otimes b\}.$$

By uniqueness of the pullback up to isomorphism, there is a 1-1 correspondence

$$C \to A \times_{A \otimes_C B} B, h \mapsto (f(h), g(h)).$$

This is the only morphism that fits into the diagram.

The corollary turns out to be particularily nice if the tensor product is a quotient of a UFD, which is in some sense independent of the morphisms f and g, by a principal ideal.

Theorem 2 (Multivariate FMR) *Let $f, F \in k[x_1, \ldots, x_m]$ and $g, G \in k[y_1, \ldots, y_n]$ be non-constant multivariate polynomials over a field k. The following are equivalent:*
a) There exists $h \in k[t]$ such that $F = h(f)$ and $G = h(g)$.
b) $f - g$ divides $F - G$ in $k[x_1, \ldots, x_m, y_1, \ldots, y_n]$.

Proof: Let $C := k[t]$, $A := k[x_1, \ldots, x_m]$ and $B = k[y_1, \ldots, y_n]$. Let f and g be the k-morphisms

$$f : C \to A, t \mapsto f,$$

$$g : C \to B, t \mapsto g.$$

Choose a term order in $k[x_1, \ldots, x_m, t]$, where t is the smallest variable. Then the leading terms of a Groebner base of $(f(x_1, \ldots, x_m) - t)$ do not contain t, hence A is free over C with a base containing 1 (the reduced monomials). The same holds for B, hence our corollary applies.

With $a = F$ and $b = G$, (a) is the same as (a) in the corollary. (b) is also the same as (b) in the corollary, because

$$A \otimes_C B = k[x_1, \ldots, x_m, y_1, \ldots, y_n]/(f - g).$$

The result of Fried and MacRae ([6],[7]) is the case where $m = n = 1$.

Since $k[x_1,\ldots,x_m,y_1,\ldots,y_n]$ is a UFD, this theorem allows to find common left factors of F and G by factoring $F-G$.

The following application was proved recently by C. Alonso, J. Gutierrez and T. Recio([2]), for the case $m=n=1$.

Theorem 3 (Multivariate FMR for the rational case) *Let $A=k(x_1,\ldots,x_m)$ and $B=k(y_1,\ldots,y_n)$ be function fields over a field k. Let $f,F\in A$ and $g,G\in B$ be non-constant rational functions. The following are equivalent:*

a) There exists a rational function $h\in k(t)$ such that $F=h(f)$ and $G=h(g)$.

b) $f-g$ divides $F-G$ in $A\otimes_k B$.

Proof: Let $C:=k(t)$ and let f and g be the k-morphisms

$$f: C \to A, t \mapsto f,$$

$$g: C \to B, t \mapsto g.$$

Since C is a field, A and B are free over C, and bases containing 1 exist. Hence, our corollary applies.

With $a=F$ and $b=G$, (a) is the same as (a) in the corollary. (b) is also the same as (b) in the corollary, because

$$A\otimes_C B = A\otimes_k B/(f-g).$$

Note that again $A\otimes_k B$ is a UFD: It is the ring of all fractions $\frac{p(x_1,\ldots,x_m,y_1,\ldots,y_m)}{r(x_1,\ldots,x_m)s(y_1,\ldots,y_m)}$. To factor such a fraction, just factor the polynomial in the numerator. All monomials only depending on $x_1,\ldots,x_m$ or $y_1,\ldots,y_m$ are units. Hence we again see that the theorem can be applied to find common left factors of two given functions F and G.

Other applications seem also promising. One could try to choose some function field in several variables as C, or consider rings of algebraic functions.

References

[1] Alonso C.,

Desarrollo análisis e implementación de algoritmos para la manipulación de variedades parametricas,

Thesis, Universidad de Cantabria, 1994.

[2] Alonso C., Gutierrez J., and Recio T.,

Work on Fried and MacRae's theorem,

Oral communication, 1994.

[3] Binder F.,
Work on polynomial decomposition,
Oral communication, 1994.

[4] Burris S., and Sankappanavar H.P.,
A Course in Universal Algebra,
Springer, New York 1981.

[5] Aichinger E.,
Work on Fried and MacRae's theorem,
Oral communication, 1994.

[6] Fried M. D., and MacRae R. E.,
On the invariance of chains of fields,
Ill. J. Math. 13, 1969,
pp 165-171.

[7] Fried M. D., and MacRae R. E.,
On curves with separated Variables,
Math. Ann. 180, 1969,
pp 220-226.

[8] Johnstone P.T.,
Topos Theory,
Academic Press, London 1977.

[9] Johnstone P.T.,
Stone Spaces,
Cambridge Univ. Press, Cambridge 1982.