A NOTE ON ORTHOGONALITY AND STABLE EMBEDDEDNESS

GREGORY CHERLIN, MARKO DJORDJEVIC, EHUD HRUSHOVSKI

Abstract. Orthogonality between two stably embedded definable sets is preserved under the addition of constants.

[1]

Introduction

Let T be a first order theory, with two distinguished sorts P, Q, taking variables x, y. P, Q are said to be *orthogonal* if any formula $\phi(x, y) = \phi(x_1, \ldots, x_n, y_1, \ldots, y_m)$ is equivalent to a Boolean combination of formulas $\psi_i(x), \theta_j(y)$, possibly involving parameters. (Their canonical parameters will always be at worst algebraic.)

Orthogonality would perhaps be better referred to as model-theoretic "almost disjointness" of P and Q; (strict) disjointness would then be the same notion, without allowing algebraic parameters. Considering P,Q and $P \cup Q$ as structures in their own right, with the structure induced from T, disjointness is just the categorical notion of direct sum, in the category of structures (or theories) and interpretations. The term "orthogonality" arises from a considerably more sophisticated and more restricted situation encountered initially in stability theory ([8]); out of habit, we will stick with this terminology in our general setting.

A collection $\mathfrak{P}$ of sorts is called *stably embedded* if every relation on sorts $P_1, \ldots, P_m$ defined with parameters in a model M of T can also be defined with parameters from elements of the sorts in $\mathfrak{P}$. Any collection of sorts extends canonically to a stably embedded one; it suffices to add those (possibly imaginary) sorts that code subsets of existing $P_1 \times \ldots \times P_n$, and to close $\mathfrak{P}$ under this operation. (We will speak of single sorts below; but the results apply equally to families.)

We show that if P, Q are orthogonal and stably embedded, then they remain orthogonal in any expansion by constants of T. Equivalently, $P \cup Q$ is also stably embedded. As a corollary, if Q is orthogonal to P_1 and to P_2, all three being stably embedded, then Q is orthogonal to $P_1 \cup P_2$. A similar result holds for the union of more than two P_i. This corrects lemma 2.4.8 of [2], where stable embeddedness was not assumed; Example 2.7 below shows the assumption is necessary. For further remarks associated with [2], please see also: `http://www.rci.rutgers.edu/~cherlin/Notes`

The proof of this rather basic model-theoretic statement makes a surprising but essential use of locally finite group theory. In fact the proof we give requires the classification of the finite simple groups. The relevant group-theoretic fact, Lemma 2.1, is used for certain ∞-definable groups in T^{eq}; thus in many contexts it can be proved using specific features of T, avoiding use of the classification. (A similar proof under additional geometric assumptions, sufficient for the use in [2], was sketched in [3].)

[1]E.H. was supported by Israel Science Foundation Grant no. 244/03

For properties of stable embeddedness, we refer to [2] or the appendix to [1]. We will work with imaginary elements; in particular $acl(B)$ denotes the algebraic closure of B in M^{eq}; see [8], [7], or [6].

We thank the referee for his or her careful reading.

1. Basic lemmas on orthogonality and stable embeddedness

Orthogonality over a set of parameters B is denoted "$(P \perp_B Q)$".

Lemma 1.1. *The following are equivalent:*

1. $(P \perp_B Q)$*; i.e. any B-definable subset of $P^l \times Q^m$ is a finite Boolean combination of rectangles $R \times R'$.*
2. *For any $l, m \in \mathbb{N}$, and $a \in P^l, b \in Q^m$, $tp(a/acl(B)) \implies tp(a/acl(B), b)$.*
3. *For any $l \in \mathbb{N}$ and $a \in P^l$, any Ba-definable relation on Q is $acl(B)$-definable.*

Proof. Assume (1). Then any B-definable $S \subset P^l \times Q^m$ is a finite union of rectangles $R' \times R''$; the maximal definable rectangles contained in S are finite in number, hence $acl(B)$-definable.[2] Thus R', R'' can be taken to be $acl(B)$-definable. Let $B' = acl(B) \cap dcl(P)$, $B'' = acl(B) \cap dcl(Q)$. Since R' is a relation on P, it can be distinguished from any finite number of other relations by points of P, so the canonical code for R' is B'-definable. Similarly R'' is B''-definable. It follows (symbolically) that $tp(P/B')$ implies $tp(P/BQ)$. Since $B' \subset dcl(BP)$, $tp(PB'/B')$ implies $tp(PB'/BQ)$, so $tp(P/B')$ implies $tp(P/B'Q)$. Since $B'' \subset dcl(Q)$, it follows that $tp(P/B'B'')$ implies $tp(P/B'B''Q)$. Let $B''' = acl(B) \cap dcl(P \cup Q)$. Any B-definable equivalence relation on $P^k \times Q^l$ with finite classes is a finite union of $B'B''$-definable rectangles (as is any relation), and so each class is $B'B''$-definable. Thus $B''' = dcl(B'B'')$, so

$$tp(P/B''') \text{ implies } tp(P/B'''Q)$$

But $tp(acl(B)/B''')$ implies $tp(acl(B)/P \cup Q) = tp(acl(B)/B''' \cup P \cup Q)$; so $tp(P/B'''Q)$ implies $tp(P/acl(B) \cup Q)$. In particular $tp(P/acl(B))$ implies $tp(P/acl(B), Q)$ so $tp(a/acl(B))$ implies $tp(a/acl(B), b)$.

Now (2) implies the dual (3') of (3), which implies (1) by a standard compactness argument. This closes the circle, showing (1),(3'),(2) are equivalent. Since (1) is self-dual, (3) and (2') are too. ☐

Lemma 1.2. *Let $f : P' \to P$ be B-definable with finite fibers. If $(P \perp_B Q)$ then $(P' \perp_B Q)$.*

Proof. We may assume $B = acl(B)$. Let $a \in P^l$, $c \in F_a$, F_a a finite Ba-definable set, $b \in Q^n$. We have to show that $tp(ac/B) \implies tp(ac/Bb)$; since $tp(a/B) \implies tp(a/Bb)$, it suffices to show that $tp(c/Ba) \implies tp(c/Bab)$. Otherwise, there is a Bac-definable set $R_c \subseteq Q^n$, not Ba-definable. Consider the equivalence relation E_a: $(\forall y \in F_a)(x \in R_y \iff x' \in R_y)$. Since F_a is finite, E_a has finitely many classes. By orthogonality, E_a is $acl(B) = B$-definable. So each class is B-definable. But R_c is a union of classes, so it is B- definable. A contradiction. ☐

Corollary 1.3. *If $(P \perp_B Q)$, and $a \in P$, $b \in Q$, then $tp(b/acl(B)) \implies tp(b/acl(Ba))$.*

Proof. It suffices to show that $tp(b/acl(B)) \implies tp(b/Ba')$ for any finite tuple $a' \in acl(Ba)$. For such an a' we have $a' \in P'$ for some P' admitting a B-definable map to some P^m with finite fibers. So $(P' \perp_B Q)$ by Lemma 1.2 . ☐

[2] The referee has pointed out a quick proof of this statement. Define $E_P(x, x') \iff (\forall y)(S(x, y) \iff S(x', y))$. As S is a finite union of rectangles, it is clear that E_P has finitely many classes $C_1, \ldots, C_r$. Similarly define E_q, with classes $C'_1, \ldots, C'_s$; then the C_i, C'_j are $acl(B)$-definable, and S is a union of rectangles $C_i \times C'_j$.

Lemma 1.4. *Let $f : P' \to P$ be B-definable. For $a = (a_1, \dots, a_l) \in P^l$, let $F_a = \cup f^{-1}(a_i)$. If $(P \perp_B Q)$, and $(F_a \perp_{Ba} Q)$ for each l and each $a \in P^l$, then $(P' \perp_B Q)$.*

Proof. Let $a \in P^l$, $c \in F_a^k$, and let R_c be a Bac-definable relation on Q. Since $(F_a \perp_{Ba} Q)$, $R_{c'}$ can take only finitely many values as c' runs over F_a. Thus the equivalence relation E_a defined in the proof of Lemma 1.2 has finitely many classes. The rest of the proof is identical. □

Lemma 1.5. *Let P, Q be orthogonal 0-definable sets in an $|L|^+$ -saturated structure M, each stably embedded. Then $P \cup Q$ is stably embedded iff for any (finite) $B \subseteq M$, $(P \perp_B Q)$.*

Proof. If $P \cup Q$ is stably embedded, then any b-definable relation on $P \cup Q$ is b'-definable for some b' from $P \cup Q$; so it is clearly a finite union of rectangles. Conversely, if $P \cup Q$ is not stably embedded, then some relation R_b on $P \cup Q$ is not $P \cup Q$-definable. Then R_b cannot be a finite Boolean combination of rectangles: otherwise by stable embeddedness of P and of Q, each side of each rectangle is P or Q-definable,hence R_b itself. Thus P, Q are not orthogonal over b, hence not over B. □

2. Stable embeddedness of a union of definable sets

The proof of the following lemma, and through it all results in this section except Theorem 2.3, requires the classification of the finite simple groups.

Lemma 2.1. *There is no infinite group G with the following property: for each n, the action of G on G^n by conjugation has finitely many orbits.*

Proof. If such a group G exists, say with $|G^n/ad_G| = c(n)$, where ad_G denotes the action, then every n-generated subgroup must have size $< c(n+1)$. (If $a, b \in \langle c_1, \dots, c_n \rangle$ and $(a, c_1, \dots, c_n)$, $(b, c_1, \dots, c_n)$ are G-conjugate, then $a = b$.) In particular, G is locally finite, with finitely many conjugacy classes.

However, no such group can be infinite. Suppose otherwise. G has only finitely many normal subgroups. Let G^0 be the minimal normal subgroup of G of finite index; G^0 still has finitely many conjugacy classes. Let N be a maximal proper normal subgroup of G^0; then G^0/N has the same properties, and is a simple group. We may thus take G to be simple. The elements of G have only finitely many orders. By [5], simple locally finite groups omitting even one order are linear. So G is a linear group; $G \leq GL_n(K)$ for some n and some algebraically closed field K. At this point, [9] applies, with a complete classification of the locally finite simple linear groups. A contradiction can also be reached more directly, using the boundedness of the exponent, as follows.

Let H be the Zariski closure of G. If m is the least common multiple of the orders of elements of G, then $x^m = 1$ for all $x \in G$, and hence for all $x \in H$. In characteristic 0, it follows that the connected component H^0 of H is trivial, so H is finite, a contradiction. In positive characteristic p, a Zariski generic element of H^0 can have order $m = p^l$; but in this case H^0 is unipotent, hence H is solvable-by-finite, contradicting the simplicity of G. □

Theorem 2.2. *Let P, Q be orthogonal 0-definable sets in a structure M, each stably embedded. Then for any $B \subseteq M$, $(P \perp_B Q)$.*

Proof. Let c be a canonical parameter for a relation ϕ_c on $P \cup Q$, not $P \cup Q$-definable. If c and c' have the same type over $P \cup Q$, then $c = c'$. We can work over a base set $B \subseteq P \cup Q$ such that the type $R = tp(c/B)$ implies $tp(c/B \cup P)$ and also $tp(c/B \cup Q)$. Equivalently, $dcl(Bc) \cap P^{eq} \subseteq dcl(B)$ and similarly for Q.

For $a \in P$, the relation $\phi_c(a, y)$ on Q is Q-definable, with some canonical parameter $f_c(a) \in Q^{eq}$; this uses the stable embeddedness of Q. By stable embeddedness of P, the equivalence relation: $f_c(x) = f_c(x')$ is B-definable. Thus we can view f_c as a definable bijection $U \to V$, with $U \subseteq P^{eq}, V \subseteq Q^{eq}$.

Let $S = U \cup V \cup R$. Then the restriction map is an isomorphism $Aut(S/P) \simeq Aut(V/P)$. Similarly restriction gives an isomorphism $Aut(S/Q) \simeq Aut(U/Q)$.

f_c shows that U is V-internal, and vice versa. By [4], Appendix B, $Aut(U/Q)$ and $Aut(V/P)$ are ∞-definable groups. Note that $Aut(U/Q) \subseteq dcl(P)$ and $Aut(V/P) \subseteq dcl(Q)$. It follows that

$G_P := Aut(S/P) \simeq Aut(V/P) \subseteq dcl(Q)$

$G_Q := Aut(S/Q) \simeq Aut(U/Q) \subseteq dcl(P)$.

But G_P, G_Q both act regularly on R. Their actions commute: If $g \in G_P, h \in G_Q$, then $[g,h] \in Aut(S/P \cup Q) = (1)$.

Thus a choice of $c \in R$ gives a definable isomorphism $\alpha_c : G_P \to G_Q$, mapping g to h if $g(c) = h^{-1}(c)$. α_c is c-definable. *But any two such isomorphisms differ by conjugation.* Thus the map induced by α_c on G_P-conjugacy classes in G_P does not depend on c. So there is a B-definable bijection between $(G_P)^n/ad_{G_P}$ and $(G_Q)^n/ad_{G_Q}$. By orthogonality, these sets are all finite. By Lemma 2.1, G_P is finite. So R is finite. But then f_c is $acl(B)$-definable; a contradiction. □

Theorem 2.3. *Assume T is a theory such that for any every ∞-interpretable (with parameters) permutation group (G, X), the intersection of a definable family of point stabilizers is a finite intersection.*

Let P, Q be stably embedded definable sets. Then $P \cup Q$ is stably embedded.

The condition holds if every such pair (G, X) is linear, or just embeddable into some stable permutation group.

Proof. Follow the proof of Theorem 2.2 to the point of obtaining G_P. For $v \in V$, let $Z_v = \{g \in G_P : gv = v\}$. Then $(1) = \cap_v Z_v$, so by (2) there exists a finite $F \subseteq V$ with $\cap_{v \in F} Z_v = (1)$. Thus f_c (from the proof of Theorem 2.2) is determined by the finitely many values: let $g = f_c^{-1}$. Suppose $c \neq c' \in R$. We have $tp(c/P) = tp(c'/P)$, so there exists $1 \neq \sigma \in G_P$ with $c' = \sigma(c)$. By choice of F, $\sigma(a) \neq a$ for some $a \in F$. and $g(a) = \sigma(g)(\sigma(a)) \neq \sigma(g)(a) = f_{c'}^{-1}(a)$. So the values of f_c^{-1} on F determine c, hence $c \in dcl(B, F, f_c^{-1}(F)) \subseteq dcl(P \cup Q)$. This contradicts the choice of c. □

Corollary 2.4. *Let P, Q, Q' be stably embedded. If $(P \perp_B Q)$ and $(P \perp_B Q')$ and $Q'' = Q \cup Q'$, then $(P \perp_B Q'')$.*

Proof. We may assume $B = acl(B)$. Let $a \in P^l, b \in Q^m, b' \in (Q')^{m'}$. Since $(Q \perp_B P)$, and by Corollary 1.2, $tp(a/B) \implies tp(a/acl(Bb))$. Since $(P \perp_{Bb} Q')$ (by Theorem 2.2), $tp(a/acl(Bb)) \implies tp(a/Bbb')$. Thus $tp(a/B) \implies tp(a/Bbb')$. □

Here is Lemma 2.4.8 of [2], with stable embeddedness added to the hypotheses.

Corollary 2.5. *Let $f : P' \to P$ be B-definable, $F_a = f^{-1}(a)$. Assume Q is stably embedded, and F_a is stably embedded over a for each a. If $(P \perp_B Q)$, and $(F_a \perp_{Ba} Q)$ for each $a \in P$, then $(P' \perp_B Q)$.*

Proof. The conclusion is given by Lemma 1.4; the hypothesis of Lemma 1.4 is provided by Corollary 2.4. □

Example 2.6. *The condition on (G, X) in Theorem 2.3 cannot be removed.*

Proof. Let A be an Abelian group, with a uniformly definable family of definable subgroups $(A_u : u \in U)$; say the family is closed under finite intersections, and has no smallest element. Let $B_u = A/A_u$, and let B be the disjoint union $\cup_{u \in U}(\{u\} \times B_u)$. There is a natural action of A on B, such that every stabilizer contains some A_u. Let B^1, B^2 be two copies of B made into disjoint sorts; do not put an isomorphism between them into the language, but do include the action of A on B^i. Let A' be another copy of A, again as a sort disjoint from the others. Add the relation $\cup_{u \in U} R_u$, where $R_u = \{(a', b_1, b_2) \in A' \times B_1 \times B_2 : (a'/A_u) + b_1 = b_2\}$. Let $P = (A \cup B_1), Q = (A \cup B_2), R = A'$. □

Example 2.7. *The stable embeddedness assumption in Corollary 2.4 or Corollary 2.5 cannot be removed .*

Proof. Let P, Q, Q' be unary predicates, and R a ternary relation symbol. Let K be the class of all finite structures A in this language such that P, Q, Q' partition the universe into three disjoint classes, and if $R(a, b, c)$ holds then no two of a, b, c belong to the same classs.

K is closed under substructures, has the joint embedding property and amalgamation property so the Fraissé limit M exists and eliminates quantifiers.

By elimination of quantifiers P is orthogonal to Q and to Q'. But by construction P is not orthogonal to $Q \cup Q'$. □

References

[1] Chatzidakis, Z., Hrushovski, E., Model Theory of difference fields, AMS Transactions v. 351, No. 8, pp. 2997-3071

[2] Gregory Cherlin & Ehud Hrushovski, *Finite Structures with Few Types*, Annals of Mathematics Studies 152, Princeton University Press, Princeton and Oxford 2003

[3] Hrushovski, E., Quasi-finite structures, in Proceedings of the NATO ASI "Finite and Infinite Combinatorics in Sets and Logic," Banff 1991, eds. N. Sauer, R. Woodrow, and B. Sands, NATO ASI Series= C , Volume 411, 117-124. Kluwer. Dordrecht 1993.

[4] Ehud Hrushovski, Computing the Galois group of a linear differential equation, in *Differential Galois Theory*, Banach Center Publications 58, Institute of Mathematics, Polish Academy of Sciences, Warszawa 2002

[5] Kegel, Otto and Wujie, Shi, On the orders of elements of a locally finite simple group. C. R. Math. Rep. Acad. Sci. Canada 13 (1991), no. 6, 253–254.

[6] Marker, David, *Model Theory: An Introduction*, Graduate Texts in Mathematics 217, Springer, 2002, New York. 342 pp. ISBN 0-387-98760-6

[7] B. Poizat: Une théorie de Galois imaginaire, *J. Symbolic Logic* **48**(1983) 1151-1170.

[8] Shelah, S., *Classification theory and the number of nonisomorphic models.* Second edition. Studies in Logic and the Foundations of Mathematics, 92. North-Holland Publishing Co., Amsterdam, 1990. xxxiv+705 pp. ISBN: 0-444-70260-1

[9] Thomas, Simon, The classification of the simple periodic linear groups. Arch. Math. (Basel) 41 (1983), no. 2, 103–116.

G.C.: Dept. of Mathematics, Rutgers, 110 Frelinghuysen Road, Piscataway NJ 08854;
M.D.: Dept. of Mathematics, Uppsala University, Box 480, 75106 Uppsala, Sweden;
E.H.: Einstein Institute of Mathematics, the Hebrew University of Jerusalem, Givat Ram, Jerusalem, 91904, Israel

E-mail address: cherlin@math.rutgers.edu; marko@math.uu.se; ehud@math.huji.ac.il